POLISI KESELAMATAN SIBER

UNIVERSITI MALAYSIA TERENGGANU

Versi 1.0

POLISI KESELAMATAN SIBER

UNIVERSITI MALAYSIA TERENGGANU

Versi 1.0

POLISI KESELAMATAN SIBER

UNIVERSITI MALAYSIA TERENGGANU

Versi 1.0

Penerbit UMT
Universiti Malaysia Terengganu (UMT)
21030 Kuala Nerus
Terengganu
2022

Polisi Keselamatan Siber
Universiti Malaysia Terengganu

Diterbitkan oleh/*Published in Malaysia*
Penerbit UMT
Universiti Malaysia Terengganu
21030 Kuala Nerus
Terengganu, Malaysia

http://penerbit.umt.edu.my
E-mel: penerbitumt@umt.edu.my

Perpustakaan Negara Malaysia Data Pengkatalogan-dalam-Penerbitan

POLISI KESELAMATAN SIBER : UNIVERSITI MALAYSIA TERENGGANU. VERSI. 1.0.
eISBN 978-967-2793-46-5
1. Universiti Malaysia Terengganu--Security measures.
2. Universities and colleges--Security measures--Malaysia--Terengganu.
3. Computer security.
4. Security systems.
5. Government publications--Malaysia.
6. Electronic books.
005.809595122

Set in Optima

Reka bentuk: Penerbit UMT
Reka letak: Penerbit UMT

KANDUNGAN

PRAKATA

Assalamualaikum Warahmatullahi Wabarakatuh dan Salam Sejahtera.

Alhamdulillah, sebanyak-banyak syukur kepada Allah SWT dengan limpah dan izin-Nya, Polisi Keselamatan Siber UMT Versi 1.0 telah berjaya dihasilkan.

Pembangunan *Polisi Keselamatan Siber UMT Versi 1.0* ini bertujuan memberi panduan merangkumi semua komponen keselamatan yang perlu diambil kira oleh warga UMT iaitu pelajar dan staf serta semua pengguna untuk melindungi segala sumber data dan maklumat dalam ruang siber di UMT.

Polisi Keselamatan Siber UMT Versi 1.0 adalah berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) April 2016, Versi 1.0 dan mengikut format Polisi Keselamatan Siber MAMPU (Arahan Pentadbiran Ketua Pengarah MAMPU) Bilangan 4, Tahun 2020. Pembangunan Polisi Keselamatan Siber ini juga telah mengambil kira keperluan standard piawaian antarabangsa ISO/IEC 27001:2013 yang terkini di mana terdapat 14 kawalan yang perlu dipatuhi selaras dengan keperluan perkhidmatan teras bagi menjamin kesinambungan perkhidmatan ICT UMT dapat teruskan.

Besarlah harapan kami agar penerbitan buku *Polisi Keselamatan Siber UMT Versi 1.0* ini akan dimanfaatkan oleh semua warga UMT dalam usaha untuk meningkatkan lagi tahap keselamatan maklumat dan mengekalkan pematuhan amalan terbaik dalam Sistem Pengurusan Keselamatan Maklumat di UMT.

Ucapan setinggi penghargaan dan terima kasih kepada semua pihak yang telah terlibat menyumbangkan idea, masa dan tenaga dalam membangunkan polisi ini. Sekecil mana pun sumbangan kita, tetap sahaja akan diberi ganjaran oleh Allah SWT dengan sebaik-baik balasan.

Akhirnya, sama-samalah kita berdoa kepada Allah SWT supaya kita dimasukkan dalam kalangan orang-orang yang sentiasa ditambahkan ilmu pengetahuan, penuh manfaat kepada masyarakat, dan seterusnya mendapat kejayaan hidup di dunia dan di akhirat. Amin ya Rabbal Alamin.

PROFESOR Ts. DR. MUHAMMAD SUZURI HITAM
Ketua Pegawai Maklumat (CIO)
Pusat Ekosistem Digital (PED) UMT

PENGHARGAAN

Lembaga Pengarah Universiti (LPU)

Jawatankuasa Pengurusan Universiti (MPU)

Jawatankuasa Pengurusan ICT (JKICT)

Jawatankuasa Induk Kesihatan dan Keselamatan Pekerjaan (JKKP)

Jawatankuasa CERT UMT

Penasihat Undang-undang Universiti

Ketua dan Juru Audit Dalam ISMS UMT

Pusat Pembangunan dan Pengurusan Akademik (PPPA))

Pejabat Pendaftar

Pejabat Bendahari

Pusat Komunikasi Korporat

Pusat Transformasi, Perancangan Strategik dan Risiko (TSR)

Pejabat Pembangunan dan Harta (PPH)

Pejabat Undang-undang (PUU)

Bahagian Keselamatan

Pusat Perkhidmatan Penyelidikan dan Lapangan (PPPL)

Pusat Ekosistem Digital

Fakulti Teknologi Kejuruteraan Kelautan dan Informatik

Semua PTj dan pegawai yang terlibat secara langsung dan tidak langsung

Semoga Allah SWT mengurniakan kebaikan kepada semua.

PENGENALAN

Salah satu langkah dalam transformasi Universiti Malaysia Terengganu (UMT) adalah penggunaan teknologi maklumat dan komunikasi (ICT) untuk meningkatkan kecekapan dalam penyampaian perkhidmatan universiti. Ini bermakna maklumat atau data disimpan dan diproses dalam bentuk digital, atau dalam erti kata lain, dalam ruang siber.

Sehubungan itu, *Polisi Keselamatan Siber UMT* dibangunkan bertujuan memberi panduan merangkumi semua komponen keselamatan yang perlu diambil kira oleh semua pengguna untuk melindungi maklumat dalam ruang siber mereka.

Polisi Keselamatan Siber UMT juga merujuk kepada Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) dan Pelan Pengurusan Keselamatan Maklumat (PPKM). Agensi pengauditan boleh menggunakan polisi ini untuk memastikan PPKM bagi pelaksanaan sistem ICT adalah lengkap dan menentukan tahap keselamatan dan kematangan sistem.

LATAR BELAKANG

Polisi Keselamatan Siber UMT diwujudkan untuk menjamin kesinambungan urusan universiti dengan meminimumkan kesan insiden keselamatan ICT. Polisi ini juga bertujuan memastikan hala tuju pengurusan keselamatan universiti untuk melindungi aset ICT selaras dengan keperluan perundangan.

OBJEKTIF

Objektif utama Polisi Keselamatan Siber UMT adalah seperti yang berikut:

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

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

c. Memastikan kelancaran operasi dan meminimumkan kerosakan atau kemusnahan;

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

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

SKOP

Dalam konteks dokumen ini, ruang siber ditakrifkan sebagai sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manusia yang berinteraksi dengan sistem-sistem ini secara fizikal atau maya, serta persekitaran fizikal sistem-sistem tersebut disimpan.

Maklumat yang dipindahkan dari ruang siber ke ruang fizikal (melalui cetakan, salinan tulisan tangan, rakaman foto menggunakan peralatan fotografi) adalah di luar skop dokumen ini dan hendaklah ditangani dengan peraturan sedia ada.

TADBIR URUS

Bagi memastikan keberkesanan dan kejayaan pelaksanaan Polisi Keselamatan Siber UMT. Pihak Universiti mengguna pakai Struktur Governan Sistem Pengurusan Kualiti UMT sebagai struktur tadbir urus ISMS dan Pengurusan Kesinambungan Perkhidmatan UMT.

ASET ICT

Aset ICT universiti merangkumi Maklumat, Aliran Data, Platform Aplikasi dan Perisian, Peranti Fizikal dan Sistem, Sistem Luaran serta Sumber Luaran seperti:

a. Maklumat

i. Semua maklumat yang dijana atau dikumpulkan oleh universiti hendaklah diasingkan mengikut kategori Maklumat Rasmi, Maklumat Rahsia Rasmi, Maklumat Pengenalan Peribadi dan Data Terbuka.

ii. Maklumat Rahsia Rasmi

Maklumat Rahsia Rasmi mempunyai erti yang diberikan kepadanya di bawah Akta Rahsia Rasmi 1972 [Akta 88]. Apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 [Akta 88] dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantik di bawah Seksyen 2B Akta Rahsia Rasmi 1972.

iii. Maklumat Rasmi

Maklumat Rasmi adalah maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh mana-mana agensi kerajaan semasa menjalankan urusan rasmi. Maklumat Rasmi ini juga adalah merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

iv. Maklumat Pengenalan Peribadi

Maklumat Pengenalan Peribadi (PII atau Personally Identifiable Information) adalah maklumat yang boleh digunakan secara

tersendiri atau digunakan dengan maklumat lain untuk mengenal pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

v. Maklumat Universiti

Maklumat Universiti adalah maklumat yang dipunyai dan dijana oleh universiti termasuk maklumat pelajar, maklumat staf, maklumat kewangan dan perakaunan serta maklumat penyelidikan.

vi. Data Terbuka

Data Terbuka adalah maklumat yang bebas digunakan, dikongsi dan digunakan semula oleh orang awam, agensi kerajaan dan organisasi swasta untuk pelbagai tujuan. PII dikecualikan daripada data terbuka.

b. Aliran Data

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

i. Saluran komunikasi dan aliran data antara sistem dalam universiti;

ii. Saluran komunikasi dan aliran data ke ruang sistem luar; dan

iii. Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

c. Platform Aplikasi dan Perisian

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

d. Peranti Fizikal dan Sistem

Semua peranti fizikal yang digunakan dalam Jabatan hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Peranti fizikal termasuk:

i. Pelayan (Server);

ii. Peranti/Peralatan Rangkaian (Network Device/Equipment);

iii. Peralatan Makmal (Lab Equipment) dan penyelidikan yang boleh menghasilkan maklumat;

iv. Komputer Peribadi/ Komputer Riba (Personal Computer/ Notebook)

v. Telefon/Peranti Pintar (Smartphone/Smart Device);

vi. Media storan merupakan tempat penyimpanan maklumat seperti USB Drive, Disket, Compact Disc (CD), Digital Versatile Dics (DVD), Pita, External Hard Disk dan sebagainya;

vii. Pencetak dan Mesin Fotostat

viii. Peranti dengan sambungan ke Internet, contohnya pengimbas (scanner), sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);

ix. Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi kerajaan; dan

x. Peranti pengesahan (authentication device), contohnya token keselamatan, *dongle* dan alat pengimbas biometrik.

e. Sistem Luaran

Sistem luaran adalah sistem bukan milik universiti yang dihubungkan dengan sistem universiti. Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

f. Sumber Luaran

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 universiti. Contoh perkhidmatan sumber luaran ialah:

i. Perisian Sebagai Satu Perkhidmatan

ii. Platform sebagai Satu Perkhidmatan

iii. Infrastruktur sebagai Satu Perkhidmatan

iv. Storan Pengkomputeran Awan

v. Pemantauan Keselamatan

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

RISIKO

Universiti hendaklah mengenal pasti risiko yang berkaitan dengan aset yang telah dikenal pasti. Risiko adalah kebarangkalian universiti tidak dapat melaksanakan fungsi universiti dengan baik. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber universiti.
Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber universiti.

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

Universiti hendaklah mengenal pasti kedua-dua ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

c. Impak

Universiti hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi universiti. Impak teknikal melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti. Impak fungsi universiti melibatkan perkara-perkara daripada segi strategi, kewangan, reputasi, pematuhan, operasi dan manusia.

d. Tahap Risiko

Tahap risiko ditentukan daripada kebarangkalian dan impak risiko. Kaedah penentuan adalah berpandukan polisi pengurusan risiko yang sedang berkuat kuasa.

e. Rawatan Risiko

i. Rawatan risiko hendaklah dikenal pasti untuk menentukan sama ada ia boleh diterima, dipindah, dikurangkan, dihapus atau mengambil peluang dengan berpandukan skor risiko berdasarkan situasi semasa di universiti.

ii. Ancaman berkaitan nilai sisa risiko dan risiko yang diterima hendaklah dipantau secara berkala.

1. Teknologi

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

2. Proses

Universiti hendaklah sekiranya perlu untuk pemantauan tahap risiko, membangunkan atau menambah baik proses prosedur operasi standard dan polisi.

3. Manusia

Universiti hendaklah mengenal pasti sumber manusia berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pemantauan tahap risiko yang berkesan.

f. Pengurusan Risiko

i. Universiti hendaklah mengenal pasti struktur tadbir urus pengurusan risiko untuk:

1. Mengenal pasti kerentanan;
2. Mengenal pasti ancaman;
3. Menentukan skor risiko;
4. Menentukan pemantauan tahap risiko;
5. Memantau keberkesanan pemantauan tahap risiko; dan
6. Memantau ancaman yang berkaitan dengan nilai sisa dan risiko yang diterima.

ii. Laporan Penilaian Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya sekali setahun dalam mesyuarat Jawatankuasa Kerja Pengurusan Risiko UMT (JKPR).

PRINSIP-PRINSIP KESELAMATAN

Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan Siber UMT dan perlu dipatuhi adalah seperti berikut:

a. Akses atas prinsip "Perlu-Tahu"

Akses terhadap capaian maklumat dan penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas prinsip "Perlu-Tahu" sahaja. Ini bermakna akses

hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

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

b. Hak akses minimum

Hak akses pengguna hanya diberi pada tahap set 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. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

c. Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT universiti hendaklah menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

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;

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

ii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

d. Pengasingan

Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

e. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan (server), penghala (router), tembok api (firewall) dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail;

f. Pematuhan

Polisi Keselamatan Siber UMT hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

g. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan 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; dan

h. Saling bergantungan

Setiap prinsip di atas adalah saling melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

TEKNOLOGI

Teknologi untuk melindungi data hendaklah dikenal pasti di semua peringkat pemprosesan data dan pada setiap elemen pengkomputeran.

a. Peringkat Pemprosesan Data

i. Data-Dalam-Simpanan

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

2. Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi dari segi kerahsiaan dan integriti data. Data Terbuka perlu dilindungi daripada segi integriti data.

ii. Data-Dalam-Pergerakan

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

iii. Data-Dalam-Penggunaan

1. Universiti hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan

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

2. Teknologi yang bersesuaian boleh digunakan oleh universiti untuk memastikan asal data dan data/transaksi tanpa sangkal.

iv. Perlindungan Ketirisan Data

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

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

b. Elemen dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, universiti hendaklah menggunakan teknologi dan kawalan keselamatan yang dapat melindungi data di semua peringkat saluran pemprosesan dan bagi semua elemen dalam persekitaran pengkomputeran.

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

Setiap projek ICT yang dibangunkan di universiti hendaklah mempunyai Pelan Pengurusan Keselamatan Maklumat tersendiri yang mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

i. Peranti Pengkomputeran Peribadi

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

2. Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Rasmi hendaklah memohon kebenaran daripada universiti. Walau bagaimanapun, peranti pengkomputeran peribadi milik persendirian hendaklah dilarang daripada mencapai Maklumat Rahsia Rasmi dan dilarang sama sekali dibawa masuk ke kawasan terperingkat. Teknologi yang boleh menguruskan peranti pengkomputeran peribadi milik persendirian hendaklah dilaksanakan sebagai sebahagian daripada pelan pengolahan risiko.

ii. Peranti Rangkaian

1. Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti suis (switch), penghala (router), tembok api (firewall), peranti *Virtual Private Network* (VPN) dan sistem pengkabelan (unshielded twisted pair dan optical fiber).

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

iii. Aplikasi

1. Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi adalah pelayan sesawang (web server), pelayan aplikasi

(application server) dan sistem pengoperasian (operating system).

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

iv. Pelayan

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

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

v. Persekitaran Fizikal

1. Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem dan peralatan ICT.

2. Universiti hendaklah merujuk kepada CGSO untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.

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

4. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang

ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

PROSES

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

a. Konfigurasi Asas

   i. Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi pra-syarat pentauliahan sistem.

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

b. Kawalan Perubahan Konfigurasi

   i. Prosedur kawalan perubahan konfigurasi hendaklah diwujudkan dan dilaksanakan bagi perubahan kepada sistem, termasuk tampalan perisian (software patches), pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.

   ii. Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh personel/jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi. Hasil perubahan ini menjadi konfigurasi asas terkini.

   iii. Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan.

c. Sandaran

   i. Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.

   ii. Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

d. Kitaran Pengurusan Aset

i. Perolehan

Memastikan perolehan perkakasan dan perisian ICT mengikut peraturan dan perolehan ICT.

ii. Agih

Menguruskan pengagihan perkakasan dan perisian mengikut peraturan yang berkuat kuasa.

iii. Pindah

Pemindahan hak milik aset berlaku dalam keadaan berikut:

1. Warga UMT meninggalkan agensi disebabkan oleh persaraan, peletakan jawatan atau penugasan semula;
2. Aset yang dikongsi untuk kegunaan sementara;
3. Pemberian aset kepada agensi lain; dan
4. Aset dikembalikan setelah tamat tempoh sewaan.

Data dalam peranti tersebut hendaklah diuruskan mengikut pelupusan di perkara iv.

iv. Pelupusan

1. Semua pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya.
2. Berdasarkan keputusan CGSO, pelupusan hendaklah dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 (Akta 629) dan Warta Kerajaan P.U.(A)377. Peraturan-Peraturan Arkib Negara (Penetapan Borang-borang bagi Pelupusan Rekod Awam) 2008.

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

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

v. Kitaran Hayat

1. Kitaran hayat data hendaklah diuruskan mengikut Akta 629.

2. Akta 629 memberi mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

MANUSIA

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

Sistem penyampaian perkhidmatan kerajaan hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Warga UMT hendaklah dilatih dalam bidang pengkhususan yang diperlukan. Asas kecekapan pengguna perlu dibangunkan bagi semua pekerja dalam universiti.

a. Kompetensi Pengguna

i. Kompetensi pengguna termasuk:

1. Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT dan program kepentingan keselamatan siber.

2. Kemahiran menggunakan alat dengan menyediakan latihan yang mencukupi kepada warga UMT berhubung alat-alat keselamatan yang berkaitan bagi memastikan mereka mampu melaksanakan tugasan harian.

ii. Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian mendalam.

iii. Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeliling semasa adalah diharapkan.

b. Kompetensi Pelaksana

i. Warga UMT yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

ii. Pegawai keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

1. Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.
2. Memenuhi keperluan pembelajaran berterusan.
3. Menimba pengalaman yang mencukupi dalam bidang keselamatan siber.
4. Memperoleh tapisan keselamatan daripada agensi yang diberi kuasa.

iii. Pegawai Keselamatan ICT yang dilantik oleh universiti hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di universiti.

c. Peranan

i. Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.

ii. Setiap orang yang terlibat dengan Maklumat Rahsia Rasmi, hendaklah menandatangani perjanjian ketakdedahan seperti Arahan Keselamatan. Salinan asal perjanjian yang ditandatangani hendaklah disimpan dengan selamat dan menjadi rujukan masa hadapan.

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

iv. Warga UMT yang berperanan menguruskan aset hendaklah memastikan semua aset universiti dikembalikan sekiranya berlaku perubahan peranan.

v. Warga UMT yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset universiti yang berkaitan seperti yang tersenarai dalam senarai aset dalam Nota Serah Tugas.

vi. Warga UMT lain yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset jabatan dengan diselia oleh staf yang dipertanggungjawabkan oleh universiti.

PELAN PENGURUSAN KESELAMATAN

Setiap projek di universiti 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 Sektor Awam (RAKKSSA), Polisi Keselamatan Siber UMT dan surat pekeliling/arahan terkini untuk menangani isu-isu operasi projek.

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

PERNYATAAN POLISI

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

Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan 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 yang berikut:

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

b. Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

c. Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

d. Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan

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

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

Empat belas bidang keselamatan yang terlibat dalam Polisi Keselamatan Siber UMT diterangkan dengan jelas dan teratur dalam bahagian seterusnya.

BIDANG 1

POLISI KESELAMATAN MAKLUMAT

Rujukan: Standard ISO/IEC 27001:2013 (Annex 5)

1.1 Polisi Keselamatan Maklumat

Objektif

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan universiti dan perundangan yang berkaitan.

1.1.1. Pelaksanaan Polisi

Peranan/Pemilik/Pelaksana: Pej. Pendaftar, PED, PPP, PSNZ, PKK, Warga UMT

Pelaksanaan polisi ini akan dijalankan oleh Naib Canselor UMT yang dibantu oleh Pasukan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pengarah PED, Pegawai Keselamatan ICT (ICTSO) dan semua Ketua Pusat Tanggungjawab.

1.1.2 Penyebaran Polisi

Peranan/Pemilik/Pelaksana: PED

Polisi ini perlu disebarkan kepada semua pengguna universiti termasuk warga UMT, pembekal, pakar runding dan lain-lain.

1.1.3 Kajian Semula Polisi

Peranan/Pemilik/Pelaksana: PED

Polisi Keselamatan Siber UMT adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, Polisi Kerajaan dan kepentingan sosial.

Berikut adalah prosedur yang berhubung dengan penyelenggaraan Polisi Keselamatan Siber UMT:

1.1.3.1. Kemukakan cadangan pindaan secara bertulis kepada CIO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pengurusan ICT (JKICT) UMT;

1.1.3.2. Maklumkan kepada semua pengguna perubahan yang telah dipersetujui oleh JKICT; dan

1.1.3.3. Polisi ini hendaklah dikaji semula setiap LIMA (5) TAHUN SEKALI atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.

1.1.4 Pengecualian Polisi

Peranan/Pemilik/Pelaksana: PED, Warga UMT

Polisi Keselamatan Siber UMT adalah terpakai kepada semua pengguna ICT Universiti dan tiada pengecualian diberikan.

BIDANG 2

PERANCANGAN BAGI KESELAMATAN ORGANISASI

Rujukan: Standard ISO/IEC 27001:2013 (Annex 6)

2.1. Perancangan Dalaman

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Siber UMT.

2.1.1. Naib Canselor UMT (NC)

NC adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti yang berikut:

2.1.1.1. Menetapkan arah tuju dan strategi untuk pelaksanaan keselamatan siber universiti;

2.1.1.2. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Polisi Keselamatan Siber UMT;

2.1.1.3. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi;

2.1.1.4. Memastikan penilaian risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan dalam Polisi Keselamatan Siber UMT; dan

2.1.1.5. Mempengerusikan mesyuarat Jawatankuasa Pengurusan ICT (JKICT) UMT.

2.1.2. Ketua Pegawai Maklumat (CIO)

Peranan dan tanggungjawab CIO adalah seperti yang berikut:

2.1.2.1. Membantu NC dalam melaksanakan tugas-tugas berkaitan dengan keselamatan siber universiti;

2.1.2.2. Memastikan semua pengguna mematuhi Polisi Keselamatan Siber UMT;

2.1.2.3. Menentukan keperluan keselamatan siber;

2.1.2.4 Melaporkan sebarang perkara atau penemuan mengenai keselamatan siber kepada NC; dan

2.1.2.5. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan siber universiti.

2.1.3. Pengarah Pusat Ekosistem Digital (PED)

Pengarah PED adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti yang berikut:

2.1.3.1. Mengkaji semula dan melaksanakan kawalan keselamatan siber selaras dengan keperluan universiti;

2.1.3.2. Menentukan kawalan akses pengguna terhadap ruang siber dan aset ICT universiti;

2.1.3.3. Melaporkan sebarang perkara atau penemuan mengenai keselamatan siber kepada CIO;

2.1.3.4. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan siber universiti;

2.1.3.5. Memastikan pelaksanaan Polisi Keselamatan Siber UMT berjalan lancar;

2.1.3.6. Memastikan semua pengguna memahami dan mematuhi peruntukan-peruntukan di bawah Polisi Keselamatan Siber UMT;

2.1.3.7. Memantau pelan latihan dan program kesedaran keselamatan siber serta pengurusan risiko dan pengauditan;

2.1.3.8. Memastikan kawalan keselamatan maklumat dalam universiti diseragamkan dan diselaraskan dengan sebaiknya; dan

2.1.3.9. Memastikan penilaian risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan oleh pengurusan universiti.

2.1.4. Pegawai Keselamatan ICT (ICTSO)

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti yang berikut:

2.1.4.1. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber UMT;

2.1.4.2. Mengurus keseluruhan program-program keselamatan siber universiti;

2.1.4.3. Menguatkuasakan pelaksanaan Polisi Keselamatan Siber UMT;

2.1.4.4. Memberi penerangan dan pendedahan berkenaan Polisi Keselamatan Siber UMT kepada semua pengguna;

2.1.4.5 Merangka pengurusan risiko dan audit keselamatan siber;

2.1.4.6. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan universiti berdasarkan hasil penemuan dan menyediakan laporan mengenainya;

2.1.4.7. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;

2.4.7.8. Memaklumkan kepada Pengarah PED dan CIO dan melaporkan insiden keselamatan siber kepada The National Cyber Security Agency (NACSA);

2.4.7.9. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera;

2.1.4.8. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan siber;

2.1.4.9. Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur siber supaya insiden baru dapat dielakkan; dan

2.1.4.10. Koordinator Pengurusan Kesinambungan Perkhidmatan (Koordinator PKP) UMT.

2.1.5. Pentadbir ICT

Pentadbir ICT terdiri daripada seperti yang berikut:

2.1.5.1. Pentadbir Aplikasi;

2.1.5.2. Pentadbir Pusat Data;

2.1.5.3. Pentadbir Rangkaian ICT;

2.1.5.4. Pentadbir Pangkalan Data; dan

2.1.5.5. Pentadbir E-mel.

2.1.6. Pentadbir Aplikasi

Peranan dan tanggungjawab Pentadbir Aplikasi adalah seperti yang berikut:

2.1.6.1. Mengkaji cadangan pembangunan atau penyelarasan sistem atau modul di universiti;

2.1.6.2. Membuat kajian semula serta memperbaiki sistem atau modul sedia ada di universiti;

2.1.6.3. Membuat pertimbangan dan menyediakan cadangan pelaksanaan sistem atau modul di universiti;

2.1.6.4. Membuat pemantauan dan penyelenggaraan terhadap sistem atau modul dari semasa ke semasa;

2.1.6.5. Bertanggungjawab dalam aspek-aspek pelaksanaan keseluruhan sistem atau modul; dan

2.1.6.6. Menyediakan dokumentasi sistem atau modul dan manual pengguna.

2.1.7. Pentadbir Pusat Data

Pentadbir Pusat Data universiti adalah berperanan dan bertanggungjawab seperti yang berikut:

2.1.7.1. Memastikan persekitaran fizikal dan keselamatan Pusat Data berada dalam keadaan baik dan selamat;

2.1.7.2. Memastikan keselamatan data dan sistem aplikasi yang berada dalam Pusat Data;

2.1.7.3. Menjadual dan melaksanakan proses *backup* dan *restoration* ke atas pangkalan data dan sistem secara berkala;

2.1.7.4. Menyediakan perancangan bencana mengikut prinsip Pengurusan Kesinambungan Perkhidmatan (PKP) UMT;

2.1.7.5. Melaksanakan prinsip-prinsip Polisi Keselamatan Siber UMT;

2.1.7.6. Memastikan Pusat Data sentiasa beroperasi mengikut polisi yang telah ditetapkan;

2.1.7.7. Melaporkan sebarang pelanggaran keselamatan Pusat Data universiti kepada ICTSO; dan

2.1.7.8. Memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.

2.1.8. Pentadbir Rangkaian ICT

Pentadbir Rangkaian ICT adalah berperanan dan bertanggungjawab seperti yang berikut:

2.1.8.1. Memastikan rangkaian setempat (Local Area Network - LAN) dan rangkaian kawasan luas (Wide Area Network - WAN) di universiti beroperasi sepanjang masa;

2.1.8.2. Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna;

2.1.8.3. Merancang peningkatan infrastruktur,ciri-ciri keselamatan dan prestasi rangkaian sedia ada;

2.1.8.4. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil;

2.1.8.5. Melaksanakan penilaian tahap keselamatan sistem rangkaian dan penilaian risiko keselamatan maklumat;

2.1.8.6. Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian universiti secara tidak sah;

2.1.8.7. Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian;

2.1.8.8. Memantau penggunaan rangkaian dan melaporkan kepada ICTSO sekiranya berlaku penyalahgunaan sumber rangkaian; dan

2.1.8.9. Memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.

2.1.9. Pentadbir Pangkalan Data

Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti yang berikut:

2.1.9.1. Melaksanakan instalasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data;

2.1.9.2. Memastikan pangkalan data boleh digunakan pada setiap masa;

2.1.9.3. Melaksanakan pemantauan dan penyelenggaraan yang berterusan ke atas pangkalan data;

2.1.9.4. Melaksanakan data *masking* dalam menyediakan data latihan;

2.1.9.5. Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur;

2.1.9.6. Melaksanakan polisi pengguna pangkalan data berdasarkan kepada prinsip-prinsip Polisi Keselamatan Siber UMT;

2.1.9.7. Melaksanakan proses pengemaskinian data (housekeeping) di dalam pangkalan data; dan

2.1.9.8. Melaporkan sebarang insiden pelanggaran dasar keselamatan pangkalan data kepada ICTSO.

2.1.10. Pentadbir E-mel

Peranan dan tanggungjawab Pentadbir e-mel adalah seperti yang berikut:

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

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

2.1.10.3. Memastikan pengguna e-mel universiti berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel universiti dan Internet universiti serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan e-mel dan Internet) secara berterusan.

2.1.10.4 Memastikan kemudahan membuat capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi;

2.1.10.5. Mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan melalui saluran rasmi; dan

2.1.10.6 Memastikan maklumat perhubungan perlu dikemas kini dari semasa ke semasa.

2.1.11. Pegawai Aset

Peranan dan tanggungjawab Pegawai Aset adalah seperti berikut:

2.1.11.1. Memastikan pengurusan aset ICT Universiti dijalankan selaras dengan peraturan yang ditetapkan;

2.1.11.2. Memastikan semua aset universiti yang diterima didaftarkan menggunakan Sistem Pengurusan Aset universiti (SPA);

2.1.11.3. Bertanggungjawab urusan penggunaan, penyimpanan dan pemeriksaan. Aset yang rosak hendaklah dilaporkan kerosakan menggunakan Modul Rosak/Senggara melalui Sistem SPA,

2.1.11.4. Aset yang dibawa keluar dari pejabat hendaklah mendapat kebenaran bertulis daripada Ketua PTj atau pegawai bertanggungjawab yang telah dilantik oleh Ketua PTj. Aset berkenaan perlu dipulangkan semula sebaik selesai penggunaannya atau mengikut tempoh kelulusan mana yang lebih awal.

i. Setiap pegawai adalah bertanggungjawab terhadap sebarang kekurangan, kerosakan atau kehilangan aset di bawah tanggungjawabnya.

ii. Pengagihan Harta Modal/Inventori yang dibuat hendaklah dikemas kini dalam Modul Agihan Aset dan hendaklah ditandatangani oleh pegawai yang bertanggungjawab.

2.1.11.5. Bertanggungjawab di dalam urusan penyelenggaraan

i. Senarai aset yang memerlukan penyelenggaraan boleh dicetak melalui Modul Rosak/Selenggara

ii. Merancang penyelenggaraan

iii. Melaksanakan program penyelenggaraan

iv. Merekodkan penyelenggaraan

v. Menilai program penyelenggaraan

vi. Menyelia dan memantau penyelenggaraan oleh pihak swasta

2.1.11.6. Bertanggungjawab di dalam urusan pelupusan

i. Mengemukakan permohonan pelupusan kepada Seksyen Pengurusan Aset, Pejabat Bendahari, UMT.

2.1.12. Pengguna

Pengguna mempunyai peranan dan tanggungjawab seperti yang berikut:

2.1.12.1. Membaca, memahami dan mematuhi Polisi Keselamatan Siber UMT;

2.1.12.2 Mengetahui dan memahami implikasi keselamatan Siber kesan daripada tindakannya;

2.1.12.3. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;

2.1.12.4. Melaksanakan prinsip-prinsip Polisi Keselamatan Siber UMT dan menjaga kerahsiaan maklumat universiti;

2.1.12.5 Melaksanakan langkah-langkah perlindungan seperti berikut:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan maklumat;

v. Mematuhi dasar, piawaian dan garis panduan keselamatan siber yang ditetapkan;

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

vii. Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum.

2.1.12.6. Menghadiri program-program kesedaran mengenai keselamatan siber secara umum jika perlu;

2.1.12.7. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; dan

2.1.12.8. Bersetuju dengan terma dan syarat yang terkandung dalam polisi ini.

2.1.13. Jawatankuasa Pengurusan ICT (JKICT)

Tanggungjawab Jawatankuasa Pengurusan ICT (JKICT) adalah seperti yang berikut:

i. Memaklumkan / Memohon kelulusan kertas kerja untuk sebarang permohonan berkaitan ICT.

ii. Mesyuarat bersidang tiga (3) kali setahun.

iii. Melaporkan status semasa perkembangan dan perkhidmatan ICT oleh setiap PTj yang berkaitan.

iv. Korum mesyuarat adalah 2/3 daripada ahli mesyuarat.

Keahlian JKICT ialah seperti berikut:
Pengerusi: Naib Canselor, UMT

Setiausaha: Pengarah, PED
Ahli Tetap:

a. Semua Pegawai Utama Universiti

b. Semua Ketua Pusat Tanggungjawab

c. Pengarah PED

d. Semua Pegawai Gred 41 ke atas, PED

Pencatat: Pegawai Teknologi Maklumat Kanan, PED

(Seksyen Pentadbiran ICT & Kewangan)

2.1.14. Jawatankuasa Pengurusan Pembangunan Sistem Aplikasi (JPPSA)

Tanggungjawab Jawatankuasa Pengurusan Pembangunan Sistem Aplikasi (JPPSA) adalah seperti yang berikut:

i. Menyelaras dan menentukan hala tuju serta strategi pelaksanaan sistem aplikasi;

ii. Menyelesaikan isu-isu dasar yang timbul berkaitan dengan sistem aplikasi;

iii. Memantau dan memastikan pelaksanaan serta kemajuan pembangunan sistem aplikasi memenuhi skop dan jadual yang telah ditetapkan;

iv. Menyemak dan memastikan serahan projek pembangunan sistem aplikasi memenuhi keperluan yang ditetapkan;

v. Mesyuarat bersidang tiga (3) kali setahun dan pada bila-bila masa seperti yang diarahkan oleh Pengerusi;

vi. Korum mesyuarat adalah 2/3 daripada ahli mesyuarat. Keahlian JPPSA ialah seperti berikut:

Pengerusi: Ketua Pegawai Maklumat *(Chief Information Officer)*

Setiausaha: Ketua Bahagian (Bahagian Pembangunan Sistem Aplikasi, PED)

Ahli Tetap:

a. Pendaftar/Ahli ganti tetap (Kategori Sumber Manusia;)

b. Bendahari/Ahli ganti tetap (Kategori Kewangan);

c. Pengarah Jabatan Pengurusan Akademik/Ahli ganti tetap (Kategori Akademik);

d. Pengarah Pusat Pengurusan Penyelidikan dan Inovasi/Ahli ganti tetap (Kategori Penyelidikan);

e. Ketua Pentadbiran HEPA (Kategori HEPA);

f. Timbalan Pengarah, Bahagian Infostruktur PED;

g. Ahli yang dijemput mengikut keperluan (Kategori Tadbir Urus, Sokongan Universiti dan lain-lain)

Urus setia/Pencatat:

Penolong Pegawai Teknologi Maklumat, PED

(Bahagian Pembangunan Sistem Aplikasi, PED)

2.1.15. Jawatankuasa Teknikal Perolehan ICT (JKTPICT)

i. Mempertimbangkan permohonan perolehan ICT, UMT.

ii. Memastikan semua pembelian/perbelanjaan dibuat mengikut garis panduan dan prosedur yang ditetapkan sama ada oleh pihak Perbendaharaan, Kementerian atau Pejabat Bendahari;

iii. Memastikan pembelian/perbelanjaan mengikut keperluan dan terkawal;

iv. Memastikan pembelian/perbelanjaan mengikut perancangan dan berhemah;

v. Memastikan spesifikasi peralatan yang dimohon sesuai dengan keperluan teknologi semasa;

vi. Mesyuarat bersidang tiga (3) kali setahun dan turut bergantung kepada permohonan semasa;

vii. Korum mesyuarat adalah 2/3 daripada ahli mesyuarat.

Keahlian JKTPICT ialah seperti berikut:

Pengerusi: Ketua Pegawai Maklumat *(Chief Information Officer)*

Setiausaha: Pegawai Teknologi Maklumat Kanan, PED (Seksyen Pentadbiran ICT & Kewangan)

Ahli Tetap:

a. Ketua Pegawai Maklumat

b. Pengarah, PED

c. Wakil Tetap Bendahari - Timbalan Bendahari

d. Wakil Tetap Pejabat Pembangunan dan Harta - Timbalan Pengarah/Ketua Bahagian

e. 3 orang wakil Pensyarah/Pentadbir bidang ICT

2.1.16. *Computer Emergency Response Team* (CERT) UMT
Peranan/Pemilik/Pelaksana: CERT UMT

CERT adalah jawatankuasa yang bertanggungjawab dalam keselamatan siber dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan siber universiti.

2.1.16.1. Keahlian CERT adalah seperti berikut:

i. Pengarah PED sebagai Pengarah CERT;

ii. ICTSO sebagai Pengurus CERT; dan

iii. 5 orang ahli yang terdiri daripada

a. Pentadbir Pangkalan Data;

b. Pentadbir Rangkaian ICT;

c. Pentadbir Server;

d. Pentadbir Aplikasi; dan

e. Pentadbir Laman Web Universiti

2.1.16.2. Tanggungjawab CERT UMT meliputi semua bidang tugas pengurusan pengendalian insiden keselamatan siber universiti seperti berikut:

i. Pentadbiran (Administration)

Bidang pentadbiran merangkumi tugas-tugas merekodkan aduan, mengemas kini maklumat insiden dan menyelenggarakan fail data insiden untuk membantu kelancaran operasi CERT agensi.

ii. Pengendalian Insiden (Incident Response Handling (IRH))

Tugas-tugas pengendalian insiden dijalankan apabila aduan diterima dari agensi di bawah kawalan sehingga kes insiden selesai dikendalikan. Bidang tugas

ini meliputi proses-proses penerimaan laporan insiden, penyiasatan kes, penyediaan laporan selepas pengendalian serta khidmat nasihat kepada agensi terlibat.

iii. Penyebaran Maklumat

Setiap CERT agensi mestilah menyebarkan maklumat berkaitan insiden keselamatan siber dari semasa ke semasa kepada agensi-agensi di bawah kawalannya dan GCERT MAMPU bagi berkongsi maklumat untuk meningkatkan tahap keselamatan siber agensi dan membendung insiden keselamatan siber sektor awam. Penyebaran maklumat ini dilaksanakan secara reaktif dan proaktif. Penyebaran maklumat dilakukan secara reaktif bagi insiden yang telah berlaku dan secara proaktif mengenai kelemahan (vulnerabilities) dan ancaman yang bakal melanda agensi supaya tindakan pengukuhan dilakukan untuk mengelakkan kejadian insiden ke atas agensi di bawah kawalannya.

iv. Penyelarasan Pengurusan Pengendalian Insiden

CERT agensi berperanan menyelaraskan mesyuarat pengurusan pengendalian insiden keselamatan siber di antara agensi-agensi di bawah kawalannya dan pihak-pihak lain yang terlibat dalam pengendalian insiden keselamatan siber. Agenda utama mesyuarat adalah untuk berkongsi maklumat bagi meningkatkan tahap keselamatan siber dan

membendung kejadian insiden keselamatan siber di antara agensi-agensi di bawah kawalannya dan sektor awam amnya.

2.2. Pihak Ketiga

Objektif:

Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).

2.2.1. Keperluan Keselamatan Kontrak dengan Pihak Ketiga

Peranan/Pemilik/Pelaksana: Semua PTj

Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal.

Perkara yang perlu dipatuhi oleh termasuk yang berikut:

2.2.1.1. Membaca, memahami dan mematuhi Polisi Keselamatan Siber UMT;

2.2.1.2. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian;

2.2.1.3. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga;

2.3.1.4. Akses kepada aset ICT Universiti perlu berlandaskan kepada perjanjian kontrak;

2.2.1.5. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga; dan

2.2.1.6. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber UMT sebagaimana Lampiran 1 - A.

2.3. Pengasingan Tugas

Peranan/Pemilik/Pelaksana: Ketua PTj

Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau tidak sengaja menggubal atau menyalah guna aset.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

2.3.1.1. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT;

2.3.1.2. 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 di manipulasi;

2.3.1.3. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyelenggarakan dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan

2.3.1.4. Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak di atas kuasa tunggalnya.

2.4. Hubungan dengan Pihak Berkuasa

Peranan/Pemilik/Pelaksana: PUU, Unit Integriti, Bahagian Keselamatan, CERT UMT, JKKP

Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi:

2.4.1. Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab universiti;

2.4.2. Mewujudkan dan mengemas kini prosedur atau senarai pihak berkuasa perundangan atau pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia (PDRM) dan Suruhanjaya Komunikasi dan Multimedia (SKMM). Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan

2.4.3. Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.

2.5. Hubungan dengan Pihak Berkepentingan yang Khusus

Peranan/Pemilik/Pelaksana: Warga UMT, Semua PTj (Mengikut Bidang Kepakaran)

Hubungan yang baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau forum bagi:

2.5.1. Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;

2.5.2. Menerima amaran awal dan nasihat berhubungan kerentanan dan ancaman keselamatan maklumat terkini;

2.5.3. Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan

2.5.4. Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.

2.6. Keselamatan Maklumat dalam Pengurusan Projek

Peranan/Pemilik/Pelaksana: PED, PPP, Pejabat Pendaftar, Pejabat Bendahari, Warga UMT, Semua PTj (Pasukan Projek)

Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

2.6.1. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek universiti;

2.6.2. Objektif keselamatan maklumat hendaklah di ambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;

2.6.3. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan; dan

2.6.4. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi ini.

2.7. Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh. Polisi ini juga mendefinisikan standard, prosedur dan sekatan kepada pengguna yang mengguna pakai sumber aplikasi dan perkakasan melalui peranti mudah alih. Melindungi integriti dan privasi data yang berkaitan ataupun yang disediakan daripada sumber infrastruktur ICT Universiti.

2.7.1. Peralatan Mudah Alih

2.7.1.1. Polisi ini terpakai kepada semua klasifikasi peranti mudah alih berikut:

i. Mana-mana peranti mudah alih yang mempunyai keupayaan untuk membuat sambungan ke rangkaian universiti seperti:

a. Komputer Riba (Notebook);

b. Komputer *Tablet*;

c. Telefon Pintar; dan

d. Mana-mana peranti pintar yang bersambung ke rangkaian universiti.

2.7.1.2. Kawalan Akses Peranti Mudah Alih

i. Peranti mudah alih yang diguna pakai dalam persekitaran infrastruktur ICT Universiti perlu mendapat pengesahan identiti untuk menggunakan rangkaian universiti;

ii. Peranti mudah alih yang diguna pakai dalam persekitaran infrastruktur ICT Universiti hendaklah sentiasa dikemas kini;

iii. PED berhak menolak, menghalang capaian dan sambungan daripada peranti mudah alih pengguna;

iv. Semua peranti mudah alih adalah tertakluk kepada keperluan keselamatan PED daripada semasa ke semasa;

v. PED mempunyai hak untuk menolak dan menghalang capaian dilakukan daripada peranti mudah alih pengguna kepada mana-mana peranti/ peralatan/perisian yang berkaitan dengan infrastruktur ICT Universiti sekiranya proses berkenaan didapati akan memberikan impak yang bertentangan dengan konsep capaian murni oleh pengguna lain; dan

vi. Peranti mudah alih yang tidak disahkan penggunaan dengan internet universiti akan diklasifikasikan sebagai *Unmanaged Mobile Devices*, PED akan membuat pemantauan secara menyeluruh dan sekiranya didapati melanggar peraturan capaian dan penggunaan sumber dalaman, PED berhak untuk menghalang capaian daripada peranti berkenaan.

2.7.2. Kerja Jarak Jauh

Peranan/Pemilik/Pelaksana: PED, Pejabat Pendaftar, Warga UMT

Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan di samping memastikan keselamatan maklumat apabila maklumat dicapai, diproses dan disimpan di lokasi luar. Perkara yang perlu dipatuhi adalah seperti berikut:

2.7.2.1. Memastikan proses pengesahan pengguna remote digunakan untuk mengawal capaian *logical* ke atas kemudahan port diagnostik dan konfigurasi jarak jauh;

2.7.2.2. Sebarang capaian ke dalam komputer pelayan daripada luar hanya dibenarkan dengan akses melalui *Virtual Private Network* (VPN) rasmi universiti atau peralatan ataupun perisian yang telah mendapat kelulusan daripada Pengarah PED;

2.7.2.3. Dasar dan langkah-langkah keselamatan sokongan perlu dilaksanakan untuk melindungi maklumat yang dicapai, diproses atau disimpan di lokasi luar;

2.7.2.4. Kawalan perlindungan dan keselamatan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan; dan

2.7.2.5. Mematuhi Garis Panduan Pengurusan Rahsia Rasmi UMT bagi melindungi maklumat yang diakses, diproses atau tersimpan di lokasi luar.

BIDANG 3

KESELAMATAN SUMBER MANUSIA

Rujukan: Standard ISO/IEC 27001:2013 (Annex 7)

3.1. Sebelum Perkhidmatan

Objektif:

Memastikan semua sumber manusia yang terlibat termasuk pegawai dan warga UMT, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga UMT hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa. Perkara-perkara yang mesti dipatuhi adalah seperti berikut:

i. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga UMT serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;

ii. Menjalankan tapisan keselamatan untuk warga UMT serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan

iii. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

3.1.1. Tapisan Keselamatan

Peranan/Pemilik/Pelaksana: Pejabat Pendaftar, Warga UMT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti

Tapisan keselamatan hendaklah dijalankan terhadap warga UMT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

3.1.1.1. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga UMT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan

3.1.1.2 Menjalankan tapisan keselamatan untuk warga UMT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti yang terlibat berasaskan keperluan garis panduan pelantikan ditetapkan, keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.

3.1.2. Terma dan Syarat Perkhidmatan

Peranan/Pemilik/Pelaksana: Pejabat Pendaftar, Pejabat Bendahari, PPP, Semua PTj, Warga UMT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti

Persetujuan berkontrak dengan warga UMT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:

3.1.2.1. Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga UMT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti yang terlibat dalam menjamin keselamatan aset ICT; dan

3.1.2.2. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

3.2. Dalam Perkhidmatan

Objektif: Memastikan warga UMT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

3.2.1. Tanggungjawab Pengurusan

Peranan/Pemilik/Pelaksana: Pejabat Pendaftar, PPP, Semua PTj, Warga UMT

3.2.2. Program Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat

Peranan/Pemilik/Pelaksana: PPBI, PPPA, PED

Semua pengguna yang berkepentingan perlu diberikan program kesedaran keselamatan siber yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Warga UMT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

3.2.2.1. Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber UMT, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produksi/fungsi/aplikasi/ sistem keselamatan secara berterusan dan melaksanakan tugas-tugas dan tanggungjawab mereka;

3.2.2.2. Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber UMT perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan

3.2.2.3. Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.

3.2.3. Proses Tatatertib

Peranan/Pemilik/Pelaksana: PUU, Unit Integriti

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

3.2.3.1. Memastikan warga UMT serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh universiti;

3.2.3.3. Memastikan adanya proses tindakan tatatertib dan/atau undang-undang ke atas warga UMT serta pihak ketiga yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan ditetapkan oleh universiti; dan

3.2.3.3. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan siber.

3.3. Bertukar atau Tamat Perkhidmatan

Peranan/Pemilik/Pelaksana: Pejabat Pendaftar, Bahagian Keselamatan, PED, Semua PTj, Warga UMT

3.3.1. Bertukar

Warga UMT yang telah bertukar perkhidmatan hendaklah:

3.3.2.1. Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada universiti mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

3.3.1.2. Menyedia dan menyerahkan nota serah tugas kepada penyelia yang berkaitan.

3.3.2. Tamat Perkhidmatan

Warga UMT yang telah tamat perkhidmatan perlu mematuhi perkara-perkara yang berikut:

3.3.1.1. Memastikan semua aset ICT dikembalikan kepada universiti mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

3.3.2.2. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh universiti dan/atau terma perkhidmatan.

BIDANG 4

PENGURUSAN ASET

Rujukan: Standard ISO/IEC 27001:2013 (Annex 8)

4.1. Akauntabiliti Aset

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Universiti.

4.1.1. Inventori Aset ICT

Peranan/Pemilik/Pelaksana: Pejabat Bendahari, Pegawai Aset, Warga UMT

Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.

Perkara yang perlu dipatuhi adalah seperti yang berikut:

4.1.1.1. Memastikan semua aset ICT dikenal pasti dan maklumat aset dikemas kini, direkodkan dalam Sistem Pengurusan Aset (SPA) serta borang daftar harta modal dan inventori sentiasa dikemas kini;

4.1.1.2. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;

4.1.1.3. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di universiti;

4.1.1.4. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan

4.1.1.5. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan

4.1.1.6. Semua pengurusan aset di universiti adalah tertakluk kepada pekeliling dan tatacara yang berkuat kuasa.

4.1.2. Pemilikan Aset

Peranan/Pemilik/Pelaksana: Pejabat Bendahari, Pegawai Aset, PTj, Warga UMT

Aset yang diselenggarakan hendaklah hak milik universiti. Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut:

4.1.2.1. Memastikan aset di bawah tanggungjawabnya telah dimasukkan dalam senarai aset;

4.1.2.2 Memastikan aset telah dikelaskan dan dilindungi;

4.1.2.3. Kenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan;

4.1.2.4. Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapuskan atau dilupuskan;dan

4.1.2.5. Memastikan semua aset dipelihara dengan baik.

4.1.3. Penggunaan Aset yang Dibenarkan

Peranan/Pemilik/Pelaksana: Pejabat Bendahari, PUU, Pegawai Aset, Warga UMT

Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.

4.1.4. Pengendalian Aset

Peranan/Pemilik/Pelaksana: Pejabat Pendaftar, PSNZ, Semua PTj

Aktiviti pengendalian aset seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan seperti yang berikut:

4.1.4.1. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

4.1.4.3. Menentukan maklumat sedia untuk digunakan;

4.1.4.4. Menjaga kerahsiaan kata laluan;

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

4.1.4.6. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

4.1.4.7. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

4.1.5. Pemulangan Aset

Peranan/Pemilik/Pelaksana: Pejabat Bendahari, Pejabat Pendaftar, Warga UMT

Warga UMT hendaklah memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.

4.2. Pengelasan Maklumat

Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

4.2.1. Pengelasan Maklumat

Peranan/Pemilik/Pelaksana: Pejabat Pendaftar, PSNZ, Semua PTj

Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan dan Garis Panduan Pengurusan Rahsia Rasmi UMT serta dasar arkib yang diguna pakai.

Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan dalam dokumen Arahan Keselamatan seperti berikut:

4.2.1.1. Rahsia Besar;

4.2.1.2. Rahsia;

4.2.1.3. Sulit; atau

4.2.1.4. Terhad.

4.2.2. Pelabelan Maklumat

Peranan/Pemilik/Pelaksana: Pejabat Pendaftar, PSNZ, Semua PTj

Prosedur penandaan peringkat keselamatan pada maklumat hendaklah dipatuhi berdasarkan arahan keselamatan.

4.3. Pengendalian Media

Objektif: Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

4.3.1. Pengurusan Media Mudah Alih

Peranan/Pemilik/Pelaksana: PED, Pejabat Pendaftar Semua PTj

Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut:

4.3.1.1. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;

4.3.1.2. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;

4.3.1.3. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;

4.3.1.4. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan;

4.3.1.5. Menyimpan semua media di tempat yang selamat seperti kabinet berkunci;

4.3.1.6. Elakkan media daripada debu atau habuk, sinaran matahari, suhu panas dan cecair bendalir;

4.3.1.7. Media storan yang digunakan hendaklah bebas daripada serangan virus yang boleh mengganggu ketidakstabilan sistem komputer dan rangkaian. Gunakan perisian antivirus untuk mengimbas media storan sebelum menggunakannya; dan

4.3.1.8. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.

4.3.2. Pelupusan Media

Peranan/Pemilik/Pelaksana: PED, Pejabat Pendaftar, PPPA, Pejabat Bendahari, Semua PTj

4.3.2.1. Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh kerajaan;

4.3.2.2. Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan pendua (backup);

4.3.2.3. Media yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan kandungan dalam media telah dihapuskan dengan cara yang selamat;

4.3.2.4. Media yang hendak dilupus perlu disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

4.3.2.5. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa merujuk Garis Panduan Pengurusan Rahsia Rasmi UMT; dan

4.3.2.6. Pengguna adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti yang berikut:

i. Menyimpan mana-mana media yang akan dilupuskan untuk keperluan peribadi; dan

ii. Memindah keluar dari UMT mana-mana media yang akan dilupuskan;

4.3.3. Pemindahan Media Fizikal

Peranan/Pemilik/Pelaksana: PED, Pejabat Pendaftar, PPPA, Semua PTj

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.

BIDANG 5

KAWALAN AKSES

Rujukan: Standard ISO/IEC 27001:2013 (Annex 9)

5.1. Polisi Kawalan Akses

Objektif: Mengehadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian.

5.1.1. Polisi Kawalan Akses

Peranan/Pemilik/Pelaksana: PED, Pemilik Sistem, Pentadbir ICT

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong polisi kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

5.1.1.1. Keperluan keselamatan peralatan dan aplikasi;

5.1.1.2. Hak akses dan dasar klasifikasi maklumat sistem aplikasi dan rangkaian;

5.1.1.3. Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa;

5.1.1.4. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;

5.1.1.5. Pengasingan peranan kawalan capaian;

5.1.1.6. Kebenaran rasmi permintaan akses;

5.1.1.7. Keperluan semakan hak akses berkala;

5.1.1.8. Pembatalan hak akses;

5.1.1.9. Hak akses pentadbir ICT dilantik mempunyai kuasa untuk mencapai, merekodkan atau memantau maklumat atau kegiatan dari semasa ke semasa sebagai rutin pemantauan untuk tujuan keselamatan ICT;

5.1.1.10. Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan

5.1.1.11. Capaian *privilege*.

5.1.2. Capaian kepada Rangkaian dan Perkhidmatan Rangkaian Peranan/Pemilik/Pelaksana: PED, Pentadbir Rangkaian ICT

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:

5.1.2.1. Menempatkan atau memasang antara muka yang bersesuaian antara rangkaian universiti, rangkaian agensi lain dan rangkaian awam;

5.1.2.2. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;

5.1.2.3. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT;

5.1.2.4. Penggunaan Internet di universiti hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian ICT bagi memastikan penggunaannya untuk tujuan capaian yang

dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian universiti;

5.1.2.5. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;

5.1.2.6. Penggunaan teknologi seperti *Network Traffic Packet Shaping* boleh digunakan untuk mengawal aktiviti (video conferencing, video streaming, chat, downloading) di samping membantu pengurusan penggunaan lebar jalur (bandwidth) yang maksimum dan lebih berkesan;

5.1.27. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. PED berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;

5.1.2.8. Laman web yang dilayari hendaklah hanya yang berkaitan dengan semua bidang kerja dan terhad untuk tujuan yang dibenarkan oleh PED/pegawai yang diberi kuasa;

5.1.2.9. Laman web yang berbentuk keganasan, lucah, hasutan, perkauman dan yang boleh menimbulkan atau mendorong kepada keganasan, keruntuhan akhlak dan kebencian serta dikenal pasti tidak sesuai adalah tidak dibenarkan sama sekali, kecuali mendapat kebenaran;

5.1.2.10. PED berhak menyekat capaian kepada laman web tertentu mengikut keperluan dan arahan dari semasa ke semasa;

5.1.2.11. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;

5.1.2.12. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada pegawai yang bertanggungjawab sebelum dimuat naik ke Internet;

5.1.2.13. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

5.1.2.14. Sebarang bahan yang dimuat turun daripada Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh universiti;

5.1.2.15. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada polisi dan peraturan yang telah ditetapkan;

5.1.2.16. Pemberian alamat protokol Internet (Internet Protocol - IP Address) adalah tertakluk kepada syarat-syarat yang ditetapkan oleh PED dari semasa ke semasa.

5.1.2.17. Penggunaan *personal modem* dan *personal router* untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali;

5.1.2.18. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti yang berikut:

i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan

ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.

5.1.2.19. Penggunaan perisian seperti penganalisis rangkaian atau penghidu rangkaian (network sniffer) adalah dilarang sama sekali kecuali untuk tujuan penyelidikan setelah mendapat kelulusan PED ; dan

5.1.2.20. Pengguna dilarang mencapai sumber ICT yang menyalahi undang-undang negara.

5.2. Pengurusan Akses Pengguna

Objektif: Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.

5.2.1. Pendaftaran dan Pembatalan Akaun Pengguna

Peranan/Pemilik/Pelaksana: Pejabat Pendaftar, PED, Pemilik Sistem, Semua Pengguna dan Warga UMT

Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:

5.2.1.1. Akaun yang diperuntukkan dan diperakukan oleh universiti sahaja boleh digunakan;

5.2.1.2. Akaun pengguna mestilah unik;

5.2.1.3. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

5.2.1.4. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada Polisi Keselamatan Siber UMT. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;dan

5.2.1.5. Menentukan setiap akaun pengguna yang diwujudkan atau dibatalkan telah mendapat kelulusan pihak berwajib di universiti.

5.2.2. Peruntukan Akses Pengguna

Peranan/Pemilik/Pelaksana: PED, Pemilik Sistem

Proses formal peruntukan akses pengguna hendaklah dilaksanakan dalam pemberian atau pembatalan hak akses kepada semua jenis pengguna untuk semua sistem dan perkhidmatan.

5.2.3. Pengurusan Hak Akses Istimewa

Peranan/Pemilik/Pelaksana: ICTSO, PED, Pentadbir ICT dan Pemilik Sistem

Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak akses perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas dan kelulusan Ketua Pusat Tanggungjawab (PTj).

5.2.4. Pengurusan Maklumat Pengesahan Rahsia Pengguna

Peranan/Pemilik/Pelaksana: PED, Pentadbir ICT dan Pemilik Sistem

Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan.

5.2.5. Kajian Semula Hak Akses Pengguna

Peranan/Pemilik/Pelaksana: PED, ICTSO, Pentadbir ICT dan Pemilik Sistem

Pemilik aset dan sistem hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan. Pentadbir ICT dan Pemilik Sistem perlu mewujudkan Prosedur Pendaftaran dan Penamatan Pengguna sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan.

5.2.6. Pembatalan atau Pelarasan Hak Akses

Peranan/Pemilik/Pelaksana: PED, ICTSO, Pentadbir ICT dan Pemilik Sistem

Hak akses warga UMT 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 universiti.

5.3. Tanggungjawab Pengguna

Objektif: Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.

5.3.1. Penggunaan Maklumat Pengesahan Rahsia
Peranan/Pemilik/Pelaksana: PED, Warga UMT

Peranan dan tanggungjawab pengguna adalah seperti yang berikut:

5.3.1.1. Membaca, memahami dan mematuhi Polisi Keselamatan Siber UMT;

5.3.1.2. Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya;

5.3.1.3. Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat universiti;

5.3.1.4. Pengemaskinian data dalam sistem hanya boleh dilakukan oleh pemilik data sahaja.

5.3.15. 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 langkah-langkah keselamatan siber daripada diketahui umum.

5.3.1.6. Melaporkan kerosakan maklumat yang berada di luar had capaian sebagai pemilik data kepada ICTSO;

5.3.1.7. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; dan

5.3.1.8. Menghadiri program-program kesedaran mengenai keselamatan siber.

5.4. Kawalan Akses Sistem dan Aplikasi

Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat dalam sistem dan aplikasi.

5.4.1 Sekatan Akses Maklumat

Peranan/Pemilik/Pelaksana: PED, Pemilik Sistem

Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut para 5.1.1.

5.4.2. Prosedur Log Masuk yang Selamat

Peranan/Pemilik/Pelaksana: PED, Pemilik Sistem

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 adalah seperti berikut:

5.4.2.1. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan universiti;

5.4.2.2. Menjana amaran (alert) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem;

5.4.2.3. Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin;

5.4.2.4. Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; dan

5.4.2.5. Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.

5.4.3. Pengurusan Kata Laluan

Peranan/Pemilik/Pelaksana: PED, ICTSO, Pentadbir ICT, Pengguna

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh PED seperti berikut:

5.4.3.1. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;

5.4.3.2. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;

5.4.3.3. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan huruf, nombor dan simbol;

5.4.3.4. Kata laluan hendaklah diingat dan TIDAK BOLEH didedahkan dengan apa cara sekalipun;

5.4.3.5. Kata laluan sistem pengoperasian komputer (Microsoft Windows, Apple MacOS, Linux OS) dan *screen saver* hendaklah diaktifkan;

5.4.3.6. Kawalan had masa bagi *lock screen saver* adalah 15 minit.

5.4.3.7. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;

5.4.3.8. Kuatkuasakan pertukaran kata laluan semasa log masuk kali pertama atau selepas log masuk kali pertama atau selepas kata laluan ditetapkan semula;

5.4.3.9. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;

5.4.3.10. Kata laluan digalakkan ditukar secara berkala atau ditukar dalam tempoh 90 hari;

5.4.3.11. Mengelakkan penggunaan semula kata laluan yang baharu digunakan; dan

5.4.3.12. Kata laluan baharu yang dicipta sebaik-baiknya belum digunakan pada mana-mana perkhidmatan Internet yang lain.

5.4.4. Penggunaan Program Utiliti yang Mempunyai Hak Istimewa

Peranan/Pemilik/Pelaksana: PED, Pentadbir ICT

Penggunaan program utiliti yang boleh memberi gangguan kepada sistem adalah dilarang sama sekali.

5.4.5. Kawalan Akses kepada Kod Sumber Program Peranan/ Pemilik/Pelaksana: PED, Pengurus Projek dan Pentadbir ICT, Pentadbir Aplikasi

Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut:

5.4.5.1. Log audit perlu dikekalkan kepada semua akses kod sumber;

5.4.5.2. Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan;

5.4.5.3. Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik universiti; dan

5.4.5.4. Semua perisian sistem aplikasi hak milik UMT boleh dijual, disewa, dilesenkan semula, dipinjam, disebar atau diberi kepada sesiapa atau entiti bagi tujuan pengkomersialan dan perundingan tertakluk kepada polisi, peraturan dan garis panduan UMT yang berkuat kuasa.

BIDANG 6

KAWALAN KRIPTOGRAFI

Rujukan: Standard ISO/IEC 27001:2013 (Annex 10)

6.1. Kawalan Kriptografi

Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan dan/atau keutuhan maklumat.

6.1.1. Polisi Penggunaan Kawalan Kriptografi

Peranan/Pemilik/Pelaksana: PED, Warga UMT

Kriptografi merangkumi kaedah-kaedah seperti yang berikut:

6.1.1.1. Enkripsi

Pengguna hendaklah membuat enkripsi (encryption) ke atas maklumat yang berkaitan dengan dokumen rahsia rasmi pada setiap masa.

6.1.1.2. Tandatangan Digital

Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan Garis Panduan Pengurusan Rahsia Rasmi.

6.1.1.3. *Secure Protocol https*

Aplikasi maklumat yang berada dalam pelayan universiti perlu dilengkapi dengan fasiliti protokol keselamatan *https*.

6.1.2. Pengurusan Infrastruktur Kunci Awam/*Public Key Infrastructure* (PKI)

Peranan/Pemilik/Pelaksana: PED

Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.

BIDANG 7

KESELAMATAN FIZIKAL DAN PERSEKITARAN

Rujukan: Standard ISO/IEC 27001:2013 (Annex 11)

7.1. Keselamatan Kawasan

Objektif: Menghalang akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat dan kemudahan pemprosesan maklumat universiti.

7.1.1. Perimeter Keselamatan Fizikal

Peranan/Pemilik/Pelaksana: Pejabat Pendaftar, Bahagian Keselamatan, PPH, PED, PPPA

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat universiti. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

7.1.1.1. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;

7.1.1.2. Melindungi kawasan larangan melalui kawalan pintu masuk yang bersesuaian bagi memastikan staf yang diberi kebenaran sahaja boleh melalui pintu masuk ini;

7.1.1.3. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;

7.1.1.4. Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-

bilau dan sebarang bencana alam atau perbuatan manusia;

7.1.1.5. Melaksanakan perlindungan fizikal; dan menyediakan garis panduan untuk staf yang bekerja di dalam kawasan larangan;

7.1.1.6. Memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya; dan

7.1.1.7. Memasang alat kawalan keselamatan seperti alat penggera atau sistem kamera keselamatan litar tertutup (CCTV) dan *door access* di kawasan yang diperlukan.

7.1.2. Kawalan Kemasukan Fizikal

Peranan/Pemilik/Pelaksana: Bahagian Keselamatan, PED, Semua PTj, Pengguna

Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke Universiti. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

7.1.2.1. Setiap warga UMT hendaklah mempamerkan kad identiti sepanjang waktu bertugas. Semua kad identiti hendaklah dikembalikan kepada universiti apabila pengguna tamat perkhidmatan atau bersara;

7.1.2.2. Setiap pelawat hendaklah mendaftar dan mendapatkan pas pelawat di pintu kawalan utama. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan

7.1.2.3. Kehilangan kad identiti/pas pelawat mestilah dilaporkan dengan segera kepada pihak yang bertanggungjawab.

7.1.3. Kawalan Kawasan Pusat Data

Kawasan Pusat Data ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Pengguna luar adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu (seperti memberi perkhidmatan sokongan atau bantuan teknikal) serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

7.1.3.1. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;

7.1.3.2. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;

7.1.3.3. Memasang *door access thumbprint* dan sistem kamera keselamatan litar tertutup (CCTV);

7.1.3.4. Mengehadkan jalan keluar masuk;

7.1.3.5. Menyediakan tempat atau bilik khas untuk pelawat-pelawat;

7.1.3.6. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan staf yang diberi kebenaran sahaja boleh melalui pintu masuk ini;

7.1.3.7. Melaksanakan dan mematuhi perlindungan fizikal daripada kebakaran,banjir, letupan, kacau-bilau, bencana dan lain-lain; dan

7.1.3.8. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya.

7.1.4. Keselamatan Pejabat, Bilik dan Kemudahan

Peranan/Pemilik/Pelaksana: Bahagian Keselamatan, Semua PTj

Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

7.1.4.1. Kawasan tempat bekerja, bilik mesyuarat, bilik gerakan, bilik perbincangan, bilik fail, bilik cetakan, bilik kebal, stor, bilik kawalan sistem kamera keselamatan litar tertutup (CCTV) dan pusat data perlu dihadkan daripada diakses tanpa kebenaran;

7.1.4.2. Kawasan tempat bekerja, bilik mesyuarat, bilik gerakan, bilik perbincangan, bilik fail, bilik cetakan, bilik kebal, stor, bilik kawalan sistem kamera keselamatan litar tertutup (CCTV) dan pusat data perlu dihadkan daripada diakses oleh bukan warga; dan

7.1.4.3. Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi Arahan Keselamatan.

7.1.5. Perlindungan daripada Ancaman Luar dan Persekitaran

Peranan/Pemilik/Pelaksana: JKKP, Bahagian Keselamatan, PPH

Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. Universiti perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.

7.1.6. Bekerja di Kawasan Larangan

Peranan/Pemilik/Pelaksana: JKKP, Bahagian Keselamatan, PPH, Semua PTj

Prosedur bekerja di kawasan larangan hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrif sebagai kawasan yang dihadkan kemasukan bagi warga UMT yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis universiti termasuk Pusat Data.

Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut:

7.1.6.1. Sumber data atau pelayan, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik pelayan atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran;

7.1.6.2. Akses adalah terhad kepada warga UMT yang telah diberi kuasa sahaja dan dipantau pada setiap masa;

7.1.6.3. Pemantauan dibuat menggunakan sistem kamera keselamatan litar tertutup (CCTV) atau lain-lain peralatan yang sesuai;

7.1.6.4. Alat kawalan keselamatan seperti alat penggera atau sistem kamera keselamatan litar tertutup (CCTV) dan *door access* perlu diperiksa secara berjadual;

7.1.6.5. Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan;

7.1.6.6. Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab sepanjang tempoh di lokasi berkaitan;

7.1.6.7. Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam;

7.1.6.8. Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; dan

7.1.6.9. Memperkukuh dinding, siling dan mengehadkan jalan keluar masuk.

7.1.7. Kawasan Penyerahan dan Pemunggahan

Peranan/Pemilik/Pelaksana: PPH, Semua PTj, Pengguna

Kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan.

Universiti hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.

7.2. Peralatan

Objektif: Melindungi peralatan universiti termasuk peralatan ICT dan peralatan yang memproses maklumat untuk mengelakkan kehilangan, kerosakan, kecurian atau penjejasan aset dan gangguan terhadap operasi organisasi.

7.2.1. Penempatan dan Perlindungan Peralatan

Peranan/Pemilik/Pelaksana: PED, Semua PTj, Warga UMT, Pembekal, Pakar Runding, Pihak yang mempunyai urusan dengan perkhidmatan ICT di universiti

Peralatan hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman, bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

7.2.1.1. Semua peralatan dan perisian yang dibekalkan kepada pengguna untuk tujuan pengajaran dan pembelajaran, penyelidikan dan pentadbiran adalah menjadi hak milik universiti dan tidak boleh dijual, dipinjam atau disalin semula tanpa kebenaran universiti.

7.2.1.2. Pengguna hendaklah menyemak dan memastikan semua peralatan di bawah kawalannya berfungsi dengan sempurna;

7.2.1.3. Pengguna bertanggungjawab sepenuhnya ke atas peralatan masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

7.2.1.4. Pengguna dilarang sama sekali menambah, menanggalkan atau mengganti sebarang peralatan ICT yang telah ditetapkan oleh PED;

7.2.1.5. Pengguna bertanggungjawab ke atas perisian tambahan yang dipasang kepada peralatan ICT di bawah kawalannya;

7.2.1.6. Pengguna bertanggungjawab di atas kerosakan atau kehilangan peralatan di bawah kawalannya;

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;

7.2.1.7. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

7.2.1.8. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;

7.2.1.9. Peralatan-peralatan khas dan kritikal perlu dilengkapi dengan pemasangan *Automatic Voltage Regulator* (AVR), *Uninterruptable Power Supply* (UPS), Generator Set (Gen-Set) atau peralatan khas yang diperakui oleh PTj berkaitan ;

7.2.1.10. Semua peralatan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;

7.2.1.11. Peralatan rangkaian seperti *switches*, *router* dan aksesori berkaitan rangkaian perlu diletakkan di dalam rak khas dan berkunci;

7.2.1.12. Semua peralatan yang digunakan secara berterusan (24 jam) mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai;

7.2.1.13. Peralatan yang hendak dibawa keluar dari premis universiti, perlulah mendapat kelulusan dan direkodkan bagi tujuan pemantauan;

7.2.1.14. Peralatan ICT yang hilang di luar waktu pejabat hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;

7.2.1.15. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

7.2.1.16. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran;

7.2.1.17. Sebarang kerosakan peralatan hendaklah dilaporkan untuk dibaik pulih;

7.2.1.18. 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 dalam keadaan baik;

7.2.1.19. Konfigurasi alamat protokol Internet (IP Address) tidak dibenarkan diubah daripada alamat protokol Internet (IP Address) yang asal;

7.2.1.20. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (administrator password) yang telah ditetapkan oleh Pentadbir ICT;

7.2.1.21. Pengguna dilarang sama sekali melakukan pemasangan perisian komputer yang boleh menggugat sistem dan rangkaian universiti.

7.2.1.22. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;

7.2.1.23. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan *OFF* apabila meninggalkan pejabat;

7.2.1.24. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO;

7.2.1.25. Memastikan palam kuasa dicabut daripada suis utama elektrik bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir kilat dan sebagainya;

7.2.1.26. Semua staf diperuntukkan sebuah komputer berdasarkan keperluan kerja;

7.2.1.27. Pengguna boleh merujuk kepada PED bagi menilai spesifikasi perkakasan dan perisian ICT serta mendapatkan khidmat nasihat teknikal untuk memastikan piawaian dan keseragaman dari segi teknologi dan keperluan semasa;

7.2.1.28. Staf yang tamat perkhidmatan atau bercuti melebihi tempoh tiga bulan atau bersara atau meletak jawatan, bercuti sabatikal luar negara atau melanjutkan pengajian, perlu memaklumkan dan memulangkan semula kemudahan ICT yang telah diperuntukkan di bawah tanggungjawabnya kepada pihak berwajib selewat-lewatnya satu minggu sebelum tarikh berkenaan; dan

7.2.1.29. Tindakan surcaj tatatertib boleh dikenakan ke atas peminjam sekiranya berlaku kehilangan peralatan mengikut Tatacara Pengurusan Aset Alih.

7.2.2. Utiliti Sokongan

Peranan/Pemilik/Pelaksana: PED, PPH

Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggarakan dari semasa ke semasa (sekurang-kurangnya setahun sekali).

7.2.3. Keselamatan Kabel

Peranan/Pemilik/Pelaksana: PED

Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada 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 adalah seperti yang berikut:

7.2.3.1. Menggunakan kabel yang mengikut spesifikasi merujuk kepada badan berkuasa yang telah ditetapkan;

7.2.3.2. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;

7.2.3.3. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan atau *wire tapping*; dan

7.2.3.4. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui kaedah pemasangan mengikut standard yang ditetapkan bagi memastikan keselamatan kabel daripada kerosakan bencana dan kecurian maklumat.

7.2.4. Penyelenggaraan Peralatan

Peranan/Pemilik/Pelaksana: PED, PPH, Semua PTj

Peralatan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

7.2.4.1. Bertanggungjawab terhadap penyelenggaraan setiap peralatan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;

7.2.4.2. Mematuhi spesifikasi yang ditetapkan oleh pengeluaran bagi semua peralatan yang diselenggarakan;

7.2.4.3. Memastikan peralatan hanya boleh diselenggarakan oleh staf atau pihak yang dibenarkan sahaja;

7.2.4.4. Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan;

7.2.4.5. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan

7.2.4.6. Penyelengaraan dan pembaikan aset ICT perlulah melalui Sistem CustCare PED.

7.2.5. Pengalihan Aset

Peranan/Pemilik/Pelaksana: PED, Pegawai Aset, Warga UMT

Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:

7.2.5.1. Peralatan yang dibawa keluar dari premis universiti untuk tujuan rasmi,

perlulah mendapat kelulusan Ketua Pusat Tanggungjawab (PTJ) atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan;

7.2.5.2. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan; dan

7.2.5.3. Semua aktiviti pengalihan aset adalah tertakluk kepada pekeliling dan peraturan yang berkuat kuasa.

7.2.6. Keselamatan Peralatan dan Aset di Luar Premis

Peranan/Pemilik/Pelaksana: PED, Pejabat Bendahari, Warga UMT, Pembekal, Pakar Runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di universiti

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-perkara yang perlu dipatuhi adalah seperti yang berikut:

7.2.6.1. Peralatan perlu dilindungi dan dikawal sepanjang masa;

7.2.6.2. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan

7.2.6.3. Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.

7.2.7. Pelupusan yang Selamat atau Penggunaan Semula Perkakasan

Peranan/Pemilik/Pelaksana: Pejabat Bendahari, PED, Semua PTj

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 yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh universiti dan ditempatkan di universiti.

Peralatan yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan universiti. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

7.2.7.1 Bagi peralatan ICT yang akan dilupuskan sebelum dipindah milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat;

7.2.7.2. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran;

7.2.7.3. Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal. Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat penduaan;

7.2.7.4. Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;

7.2.7.5. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

7.2.7.6. Peralatan yang hendak dilupus perlu disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

7.2.7.7. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam inventori Sistem Pengurusan Aset;

7.2.7.8. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan

7.2.7.9. Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti yang berikut:

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman *CPU* seperti *RAM, harddisk, motherboard* dan sebagainya;

ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti *Automatic Voltage Regulator* (AVR), speaker dan mana-mana

peralatan yang berkaitan ke mana-mana bahagian di universiti;

iii. Memindah keluar dari universiti mana-mana peralatan ICT yang hendak dilupuskan; dan

iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab universiti.

7.2.7.10. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan;

7.2.7.11 Maklumat lanjut berhubung pelupusan boleh dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Universiti (TPA) yang berkuat kuasa; dan

7.2.7.12. Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan.

7.2.8. Peralatan Pengguna Tanpa Kawalan

Peranan/Pemilik/Pelaksana: PED, Semua PTj, Pengguna

Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:

7.2.8.1. Tamatkan sesi aktif apabila selesai tugas;

7.2.8.2. *Log-off* komputer peribadi, komputer riba dan pelayan yang berkaitan apabila sesi bertugas selesai; dan

7.2.8.3. Komputer peribadi, komputer riba atau terminal selamat daripada perkara yang tidak dibenarkan.

7.2.9. Meja Bersih (Clear Desk) dan Skrin Kosong (Clear Screen)
Peranan/Pemilik/Pelaksana: PED, Pengguna

Dasar meja bersih untuk kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan.

Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

7.2.9.1. Panduan Meja Bersih (Clear Desk)

i. Kata laluan mestilah tidak disimpan berhampiran komputer atau mana-mana lokasi lain yang mudah diakses;

ii. Salinan dokumen yang mengandungi maklumat terperingkat perlu dikeluarkan dari mesin pencetak/ faks;

iii. Dokumen atau pita magnetik atau media mudah alih seperti *Compact Disc* (CD), *Digital Versatile Disc* (DVD) dan lain-lain perlu disimpan dengan selamat;

iv. Maklumat sulit tidak harus ditinggalkan tanpa kawalan sekitar kawasan kerja;

v. Maklumat sulit hendaklah dikunci dengan selamat di laci, kabinet atau bilik fail pada setiap masa kecuali ketika digunakan; dan

vi. Meja mesti dibersihkan pada setiap akhir waktu kerja.

7.2.9.2. Panduan Skrin Kosong (Clear Screen)

i. *Shutdown* komputer pada akhir kerja;

ii. *Lock screen* dan aktifkan kata laluan bila tidak digunakan;

iii. Pengguna perlu log masuk ke Portal MyNemo setiap kali kawalan sesi tamat secara automatik sekiranya *idle time*;

iv. Tutup semua aplikasi dan log keluar pada akhir kerja;

v. Skrin komputer hendaklah berada dalam keadaan yang sukar dilihat oleh orang lain; dan

vi. Komputer riba mesti disimpan dalam laci berkunci atau kabel kunci dan disimpan di tempat yang selamat.

BIDANG 8

KESELAMATAN OPERASI

Rujukan: Standard ISO/IEC 27001:2013 (Annex 12)

8.1. Prosedur dan Tanggungjawab Operasi

Objektif: Memastikan operasi kemudahan pemprosesan maklumat yang betul dan selamat.

8.1.1. Prosedur Operasi yang Didokumenkan

Peranan/Pemilik/Pelaksana: PED

Penyedia dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut:

8.1.1.1. Semua prosedur keselamatan siber yang diwujudkan, dikenal pasti dan diguna pakai hendaklah didokumenkan, disimpan dan dikawal;

8.1.1.2. 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

8.1.1.3. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.

8.1.2. Pengurusan Perubahan

Peranan/Pemilik/Pelaksana: PED, Pentadbir ICT, Semua PTj

Perubahan dalam organisasi, proses *bisnes*, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

8.1.2.1. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;

8.1.2.2. Aktiviti-aktiviti seperti memasang, menyelenggarakan, 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;

8.1.2.3. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan

8.1.2.4. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

8.1.3. Pengurusan Kapasiti

Peranan/Pemilik/Pelaksana: PED

Penggunaan sumber hendaklah dipantau dan disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi

sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

8.1.3.1. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan

8.1.3.2. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.

8.1.4. Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi

Peranan/Pemilik/Pelaksana: PED

Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

8.1.4.1. Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggarakan dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (production);

8.1.4.2. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan

8.1.4.3. Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.

8.2. Perlindungan daripada Perisian Hasad

Objektif: Memastikan maklumat dan kemudahan pemprosesan maklumat dilindungi daripada perisian hasad (malware).

8.2.1. Kawalan daripada Perisian Hasad

Peranan/Pemilik/Pelaksana: PED, Pentadbir ICT

Kawalan pengesanan, pencegahan dan pemulihan untuk memberi perlindungan daripada sebarang *malware* hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

8.2.1.1. Memasang sistem keselamatan untuk mengesan perisian atau program *malware* seperti antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;

8.2.1.2. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;

8.2.1.3. Mengimbas semua perisian atau sistem dengan antivirus yang dikemas kini sebelum menggunakannya;

8.2.1.4. Mengemas kini antivirus dengan *signature*/*pattern* antivirus yang terkini;

8.2.1.5. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;

8.2.1.6. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;

8.2.1.7. Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;

8.2.1.8. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan

8.2.1.9. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus dan ancaman-ancaman terkini.

8.3. Sandaran/Salinan (Backup)

Objektif: Memastikan segala data diselenggarakan agar penyimpanan data diuruskan dengan sempurna.

8.3.1. Sandaran Maklumat

Peranan/Pemilik/Pelaksana: PED, PPP , Semua PTj

Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *off-site*. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

8.3.1.1. Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;

8.3.1.2. Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi;

8.3.1.3. Menguji sistem sandaran dan prosedur *restore* sedia ada bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan

8.3.1.4. Sandaran hendaklah dilakukan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya satu tahun.

8.4. Log dan Pemantauan

Objektif: Merekodkan kejadian dan menghasilkan bukti.

8.4.1. Log Kejadian

Peranan/Pemilik/Pelaksana: PED, Pentadbir ICT

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.

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 seperti yang berikut:

8.4.1.1. Fail log sistem pengoperasian;

8.4.1.2. Fail log servis (contoh: web, e-mel);

8.4.1.3. Fail log aplikasi (audit trail);

8.4.1.4. Fail log rangkaian (contoh: switch, firewall, IPS).

Pentadbir Aplikasi hendaklah melaksanakan perkara-perkara berikut:

8.4.1.5. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;

8.4.1.6. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan

8.4.1.7. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Aplikasi hendaklah melaporkan kepada pasukan CERT UMT.

8.4.2. Perlindungan Maklumat Log

Peranan/Pemilik/Pelaksana: PED, Pentadbir ICT

Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin.

8.4.3. Log Pentadbir dan Pengendalian

Peranan/Pemilik/Pelaksana: PED, Pentadbir ICT, Pentadbir Pangkalan Data

Aktiviti pentadbir aplikasi dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara tetap. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

8.4.3.1. Memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala;

8.4.3.2. Aktiviti pentadbiran dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu;

8.4.3.3. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;

8.4.3.4. Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian;

8.4.3.5. Kemudahan merekodkan dan maklumat log perlu dilindungi daripada diubah suai dan sebarang capaian yang tidak dibenarkan; dan

8.4.3.6. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Aplikasi hendaklah melaporkan kepada pasukan CERT UMT.

8.4.4. Penyeragaman Jam

Peranan/Pemilik/Pelaksana: PED, Pentadbir Pusat Data

Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain

keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal.

Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam universiti atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh *National Metrology Institute of Malaysia* (NMIM).

8.5. Kawalan Perisian yang Beroperasi

Objektif: Menghalang capaian yang tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

8.5.1. Pemasangan Perisian pada Sistem yang Beroperasi

Peranan/Pemilik/Pelaksana: PED, Pentadbir Pusat Data

Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa meluluskan adalah seperti yang berikut:

8.5.1.1. Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi sistem dan perisian;

8.5.1.2. Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperakui berjaya; dan

8.5.1.3. Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.

8.6. Pengurusan Kerentanan Teknikal

Objektif: Memastikan kawalan kerentanan teknikal adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.

8.6.1. Pengurusan Kerentanan Teknikal

Peranan/Pemilik/Pelaksana: PED, Pentadbir Pusat Data

Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai perlu diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

8.6.1.1. Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;

8.6.1.2. Menganalisis tahap risiko kerentanan; dan

8.6.1.3. Mengambil tindakan pengolahan dan kawalan risiko.

8.6.2. Sekatan ke Atas Pemasangan Perisian

Peranan/Pemilik/Pelaksana: PED, Pentadbir Pusat Data

Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan.

Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:

8.6.2.1. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan warga UMT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Universiti;

8.6.2.2. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah

mana-mana undang-undang bertulis yang berkuat kuasa;

8.6.2.3. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya;

8.6.2.4. Pengguna tidak dibenarkan membuat salinan ataupun apa jua kaedah yang bertujuan memindah, menyalin, menyebarkan dan membuat instalasi mana-mana perisian yang diberikan oleh universiti;

8.6.2.5. Universiti tidak akan bertanggungjawab terhadap sebarang penyalahgunaan perisian termasuk penggunaan perisian tanpa lesen yang diguna pakai oleh pengguna;

8.6.2.6. Perisian berlesen untuk sekali pemasangan (one time installation) adalah tidak digalakkan bagi pengguna komputer sewaan; dan

8.6.2.7. Universiti menggalakkan penggunaan dan pembangunan aplikasi berasaskan perisian sumber terbuka.

8.7. Pertimbangan Tentang Audit Sistem Maklumat

Objektif: Meminimumkan kesan aktiviti audit terhadap sistem yang beroperasi.

8.7.1. Kawalan Audit Sistem Maklumat

Peranan/Pemilik/Pelaksana: PED, ICTSO, Pentadbir Pusat Data dan Pentadbir Aplikasi

Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perniagaan.

BIDANG 9

KESELAMATAN KOMUNIKASI

Rujukan: Standard ISO/IEC 27001:2013 (Annex 13)

9.1. Pengurusan Keselamatan Rangkaian

Objektif: Memastikan perlindungan maklumat dalam rangkaian dan dalam kemudahan sokongan pemprosesan maklumat dalam rangkaian.

9.1.1. Kawalan Rangkaian

Peranan/Pemilik/Pelaksana: PED, Pentadbir Rangkaian ICT, Warga UMT

Sistem dan aplikasi hendaklah dikawal dan diurus sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

9.1.1.1. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;

9.1.1.2. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas daripada risiko seperti banjir, gegaran dan habuk;

9.1.1.3. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;

9.1.1.4. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;

9.1.1.5. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir ICT;

9.1.1.6. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan PED;

9.1.1.7. Semua perisian *sniffing* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;

9.1.1.8. Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat PED;

9.1.1.9. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;

9.1.1.10. Sebarang penyambungan rangkaian yang bukan di bawah kawalan PED adalah tidak dibenarkan;

9.1.1.11. Semua pengguna hanya dibenarkan menggunakan rangkaian universiti sahaja dan penggunaan *modem* dan *router* peribadi adalah dilarang sama sekali;

9.1.1.12. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan;

9.1.1.13. Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan;

9.1.1.14. Menempatkan atau memasang antara muka (interface) yang bersesuaian di antara rangkaian universiti, rangkaian agensi lain dan rangkaian awam;

9.1.1.15. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;

9.1.1.16. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang digunakan sahaja;

9.1.1.17. Mengawal capaian fizikal dan logikal ke atas kemudahan *port diagnostik* dan konfigurasi jarak jauh;

9.1.1.18. Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan universiti; dan

9.1.1.19. Mewujud dan melaksanakan kawalan pengalihan tumpuan bagi memastikan pematuhan terhadap peraturan universiti.

9.1.2. Keselamatan Perkhidmatan Rangkaian

Peranan/Pemilik/Pelaksana: PED, ICTSO, Pentadbir Rangkaian ICT, Pembekal

Pengurusan bagi semua perkhidmatan rangkaian (inhouse or outsource) yang merangkumi mekanisme keselamatan rangkaian dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan ke dalam perjanjian perkhidmatan rangkaian.

9.1.3. Pengasingan dalam Rangkaian

Peranan/Pemilik/Pelaksana: PED, ICTSO, Pentadbir Rangkaian ICT

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

9.2. Pemindahan Data dan Maklumat

Objektif: Memastikan keselamatan pemindahan/pertukaran data atau maklumat antara universiti dan agensi luar terjamin.

9.2.1. Polisi dan Prosedur Pemindahan Data dan Maklumat

Peranan/Pemilik/Pelaksana: PED, Pejabat Pendaftar, Semua PTj

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

9.2.1.1. Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi;

9.2.1.2. Terma pemindahan data, maklumat dan perisian antara universiti dengan pihak luar hendaklah dimasukkan di dalam perjanjian;

9.2.1.3. Media yang mengandungi maklumat perlu dilindungi; dan

9.2.1.4. Memastikan maklumat yang terdapat di dalam e-mel elektronik hendaklah dilindungi sebaiknya.

9.2.2. Maklumat dalam Talian (Online)

Peranan/Pemilik/Pelaksana: PED, PKK, Semua PTj

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti yang berikut:

9.2.2.1. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian;

9.2.2.2. Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu;

9.2.2.3. Memastikan segala maklumat yang hendak dipaparkan telah disahkan dan diluluskan berdasarkan SOP yang disediakan sebelum dimuat naik ke laman web;

9.2.2.4. Maklumat yang terlibat dalam talian perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan;

9.2.2.5. Maklumat yang terlibat dalam transaksi dalam talian (online) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan

9.2.2.6. Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.

9.2.3. Media Sosial

Peranan/Pemilik/Pelaksana: PED, PKK, Semua PTj, Warga UMT

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan dan kawalan penyebaran maklumat yang dikongsi dan

disebarkan melalui media sosial adalah seperti yang berikut:

9.2.3.1. Tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara;

9.2.3.2. Tidak melibatkan penyebaran maklumat dan dokumen terperingkat;

9.2.3.3. Tidak memaparkan kenyataan yang boleh menjejaskan imej kerajaan dan universiti;

9.2.3.4. Tidak menyentuh isu sensitif seperti agama, politik atau perkauman;

9.2.3.5. Tidak memaparkan kenyataan yang berunsur fitnah atau hasutan; dan

9.2.3.6. Mematuhi garis panduan, prosedur dan polisi yang sedang berkuat kuasa.

9.2.4. Keselamatan Media Sosial

Peranan/Pemilik/Pelaksana: PED, PKK, Semua PTj

Pegawai yang bertanggungjawab mengendalikan laman web media sosial rasmi Universiti dan PTJ perlulah memastikan keselamatan media sosial dengan melaporkan masalah *spam,* dicerobohi atau digodam kepada pasukan CERT UMT.

9.2.5. Perjanjian Mengenai Pemindahan Data dan Maklumat

Peranan/Pemilik/Pelaksana: PED, Pemilik Data, Semua PTj

Universiti 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:

9.2.5.1 Ketua PTj hendaklah mengawal penghantaran dan penerimaan maklumat universiti;

9.2.5.2. Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat universiti;

9.2.5.3. Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan

9.2.5.4. Universiti hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.

9.2.6. Pesanan Elektronik (E-mel)

Peranan/Pemilik/Pelaksana: PED, Pentadbir E-mel, Warga UMT

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 di LAMPIRAN 2:

Penggunaan e-mel di universiti hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet.

Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti yang berikut:

9.2.6.1. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh universiti sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

9.2.6.2. Setiap warga UMT hendaklah diperuntukkan satu akaun e-mel sahaja. Setiap lantikan pentadbiran Ahli Lembaga Pengarah Universiti (LPU),PTj dan persatuan berdaftar di universiti boleh diperuntukkan satu akaun e-mel rasmi.

9.2.6.3. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh universiti;

9.2.6.4. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;

9.2.6.5. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;

9.2.6.6. Pengguna dinasihatkan menggunakan fail kepilan (attachment), sekiranya perlu, tidak melebihi 25 Megabait (25Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz dan perkongsian fail awan (cloud file sharing) adalah disarankan;

9.2.6.7. Pengguna hendaklah mengelak daripada membuka e-mel penghantar yang tidak diketahui atau diragui;

9.2.6.8. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

9.2.6.9. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara

pengurusan sistem fail elektronik yang telah ditetapkan;

9.2.6.10. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi boleh dihapuskan;

9.2.6.11. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;

9.2.6.12. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;

9.2.6.13. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, unifi.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi;

9.2.6.14. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing;

9.2.6.15. Universiti boleh menamatkan kemudahan akuan e-mel yang telah diberikan kepada warga UMT atas sebab-sebab berikut:

i. Tamat perkhidmatan/tamat pengajian

ii. Persatuan dibubarkan

9.2.6.16. Akaun e-mel akan dihapuskan selepas tiga bulan tamat perkhidmatan;

9.2.6.17. Pengurusan tertinggi universiti boleh mengarahkan PED secara bertulis memeriksa dan melihat isi kandungan e-mel dan ruang storan pengguna atas faktor keselamatan; dan

9.2.6.18. Permohonan akaun e-mel bagi individu boleh dibuat menggunakan sistem pendaftaran

atas talian melalui portal aplikasi MyNemo. Permohonan bagi akaun e-mel atas kapasiti jawatan lantikan pentadbiran dan program rasmi universiti boleh dikemukakan surat permohonan rasmi kepada PED;

9.2.6.19. Pengguna adalah dilarang daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan e-mel atau mana-mana undang-undang bertulis yang berkuat kuasa seperti yang berikut:

i. Berkongsi atau memberi akaun e-mel kepada orang lain;

ii. Menyebar luas e-mel berantai (chain email), iklan atau yang seumpamanya;

iii. Menghantar dan melibatkan diri dalam e-mel yang berunsur hasutan, perkauman, kutukan, *broadcast mail* atau *mass* (spamming), fitnah atau aktiviti-aktiviti lain yang dilarang;

iv. Memalsukan atau menyembunyikan identiti sebenar pengirim e-mel (spoofing);

v. Menghantar atau memiliki bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian dan jenayah;

vi. Menghantar bahan-bahan yang boleh menyebabkan kerosakan atau ancaman keselamatan kepada komputer dan maklumat seperti virus, *worm, trojan horse, trap door* dan seumpamanya;

vii. Menggunakan e-mel untuk tujuan komersial atau politik yang berkepentingan peribadi;

viii. Menghantar maklumat peribadi orang lain, teks, imej atau dokumen di bawah akta hak cipta tanpa kebenaran pihak berkenaan; dan

ix. Universiti tidak bertanggungjawab terhadap pengguna yang menjadi penghantar (sender) atau penerima (receiver) kepada sebarang e-mel yang berunsur *spamming* atau penyebaran e-mel dengan kandungan tidak beretika.

9.2.7. Perjanjian Kerahsiaan atau Ketakdedahan

Peranan/Pemilik/Pelaksana: PUU, Pejabat Pendaftar, Pejabat Bendahari, Semua PTj

Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan.

Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.

BIDANG 10

PEMEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

Rujukan: Standard ISO/IEC 27001:2013 (Annex 14)

10.1. Keperluan Keselamatan Sistem Maklumat

Objektif: Memastikan keselamatan maklumat dijadikan bahagian penting dalam sistem maklumat sepanjang kitar hayat. Ini juga termasuk keperluan untuk sistem maklumat yang menyediakan perkhidmatan melalui rangkaian awam.

10.1.1. Analisis dan Spesifikasi Keperluan Keselamatan Maklumat

Peranan/Pemilik/Pelaksana: PED, Semua PTj

Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem sedia ada. Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara seperti yang berikut:

10.1.1.1. Aspek keselamatan hendaklah dimasukkan ke dalam kitar hayat pembangunan sistem termasuk konsep perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan;

10.1.1.2. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan

pengguna dan selaras dengan Polisi Keselamatan Siber UMT;

10.1.1.3. Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan;

10.1.1.4. Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data; dan

10.1.1.5. Pembangunan sistem perlulah melalui Jawatankuasa Pengurusan Pembangunan Sistem Aplikasi.

10.1.2. Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam

Peranan/Pemilik/Pelaksana: PED

Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

10.1.2.1. Semua perkhidmatan sumber luar hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi universiti. Contoh perkhidmatan sumber luaran ialah:

i. Perisian sebagai Satu Perkhidmatan;

ii. Platform sebagai Satu Perkhidmatan;

iii. Infrastruktur sebagai Satu Perkhidmatan;

iv. Storan Pengkomputeran Awam; dan

v. Pemantauan Keselamatan.

10.1.2.2. Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala;

10.1.2.3. Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (authentication);

10.1.2.4. Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi;

10.1.2.5. Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan

10.1.2.6. Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.

10.1.3. Melindungi Transaksi Perkhidmatan Aplikasi
Peranan/Pemilik/Pelaksana: PED

Maklumat 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-perkara yang perlu dipertimbangkan adalah seperti yang berikut:

10.1.3.1. Penggunaan tandatangan elektronik/ kaedah pengesahan yang dipersetujui oleh setiap pihak yang terlibat dalam transaksi;

10.1.3.2. 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.

10.2. Keselamatan dalam Proses Pembangunan dan Sokongan

Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan siber yang bersesuaian bagi menghalang kesilapan, kehilangan, kecurian, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.

10.2.1. Dasar Pembangunan Selamat

Peranan/Pemilik/Pelaksana: PED, Pentadbir Aplikasi

10.2.1.1. Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

i. Keselamatan persekitaran pembangunan;

ii. Keselamatan pangkalan data;

iii. Keperluan keselamatan dalam fasa reka bentuk;

iv. Keperluan *check point* keselamatan dalam carta perbatuan projek;

v. Keperluan pengetahuan ke atas keselamatan aplikasi;

vi. Keselamatan dalam kawalan versi; dan

vii. Bagi pembangunan secara penyumberluaran (outsource), pembekal yang dilantik mesti berkebolehan untuk mengenal pasti dan menambah baik keselamatan dalam pembangunan sistem.

10.2.1.2. Pembangunan Sistem perlulah mengikuti Tatacara Pembangunan Sistem seperti yang berikut:

i. Pemilik sistem perlu menyediakan kertas cadangan yang lengkap dan terperinci dengan menyatakan skop keperluan yang jelas. JPPSA akan meneliti dan menentukan kelulusan kertas cadangan tersebut;

ii. PED akan menilai sistem-sistem yang dibekalkan oleh pihak luar dari segi keserasian dan keselamatan data, pelaksanaan melalui rangkaian universiti serta keupayaan integrasi sistem berkenaan;

iii. Pemilik sistem perlu menghantar permohonan dan Sistem CustCare (PED) bagi penambahbaikan, penyelenggaraan atau perubahan sistem yang diperlukan. Ia bertujuan

untuk perekodan, pemantauan dan pengurusan dapat dikawal dengan lebih berkesan;

iv. PED akan meneliti dan membuat kajian yang sewajarnya bagi penambahbaikan sistem aplikasi yang dipohon;

v. PTj boleh memohon pembangunan sistem dengan khidmat nasihat daripada PED menggunakan peruntukan kewangan masing-masing sekiranya berlaku kekangan staf dan kewangan di PED;

vi Sebarang perolehan atau pembangunan sistem aplikasi daripada pihak lain selain PED adalah tidak digalakkan. Sekiranya ia berlaku, PTj bertanggungjawab sepenuhnya terhadap proses pembangunan dan penyelenggaraan sistem tersebut; dan

vii. Permohonan pembangunan sistem yang baru perlu mendapat kelulusan daripada JPPSA;

10.2.1.3 Semua penyelenggaraan sistem adalah tertakluk kepada Garis Panduan Penambahbaikan dan Penyelenggaraan Sistem Aplikasi UMT; dan

10.2.1.4. Pembangunan sistem perlulah mengikuti siri-ciri berikut:

i. Integrasi

Sistem aplikasi yang dibangunkan dan ditambah baik akan diintegrasikan sepenuhnya di antara satu sistem dengan sistem yang lain agar kemasukan data berlaku secara berpusat dan data tersebut akan disalurkan kepada sistem-sistem aplikasi yang lain.

ii. Mesra Pengguna

Sistem aplikasi yang dibangunkan dan ditambah baik perlu menitikberatkan dan mengambil kira berkenaan dengan reka bentuk antara muka yang lebih mesra pengguna dan mudah difahami.

iii. Dinamik

Sistem aplikasi yang dibangunkan dan ditambah baik akan direka cipta bersifat dinamik supaya mudah diubah suai mengikut keperluan semasa.

iv. Kebolehcapaian

Sistem aplikasi yang dibangunkan mestilah mudah diakses pada bila-bila masa melalui Internet dan Intranet.

v. Kawalan Capaian Menu

Kawalan capaian menu adalah mengikut tahap atau kumpulan pengguna yang telah ditetapkan oleh pemilik sistem. Keadaan ini akan dapat mengawal sebarang aktiviti yang tidak diingini atau penyalahgunaan sistem.

vi. Maklumat Terkini, Tepat dan Kebolehpercayaan yang Tinggi

Sistem aplikasi yang dibangunkan dan ditambah baik adalah sangat membantu untuk mendapatkan sebarang maklumat yang diperlukan. Pihak pemilik data perlu mengetahui peranannya supaya data-data dan maklumat yang diperlukan adalah terkini, tepat dan mempunyai kebolehpercayaan yang tinggi.

vii. Automasi

Sistem aplikasi yang dibangunkan dan ditambah baik adalah bertujuan untuk mengautomasikan dan mengurangkan proses manual di mana ia merangkumi proses-proses secara atas talian. Ia juga merangkumi penggunaan peralatan seperti kad pintar (smartcard), pengimbas barkod (barcode reader) dan sebagainya.

viii. Kepintaran

Sistem yang dibangunkan hendaklah menggunakan kaedah dan pendekatan terbaik dalam pembangunan dan penyelenggaraan sistem. Sistem-sistem yang dibangunkan akan menjurus ke arah kecekapan dan keberkesanan pentadbiran, pengajaran dan pembelajaran, penyelidikan dan perundingan serta memberi ilmu

pengetahuan agar ia dapat memberi manfaat kepada organisasi.

ix. Penggunaan kertas secara minimum

Capaian maklumat secara atas talian adalah sangat penting bagi memastikan data-data yang dicapai adalah yang terkini dan dicapai dengan cepat. Komunikasi seperti memo, mesyuarat, pekeliling, pengumuman dan sebagainya boleh dijalankan secara atas talian.

10.2.2. Prosedur Kawalan Perubahan Sistem

Peranan/Pemilik/Pelaksana: PED, Pentadbir Aplikasi

Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Setiap perubahan hendaklah dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

10.2.2.1 Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;

10.2.2.2 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;

10.2.2.3. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja melalui jawatan kuasa berkaitan;

10.2.2.4. Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan;

10.2.2.5. Menghalang sebarang peluang untuk membocorkan maklumat.

10.2.2.6. Versi baru perisian aplikasi dan sistem pengoperasian sentiasa dikeluarkan secara berkala bagi mengatasi masalah pepijat dan ancaman serta meningkatkan fungsinya; dan

10.2.2.7. PED bertanggungjawab mengawal versi perisian aplikasi apabila perubahan atau peningkatan dibuat.

10.2.3. Kajian Semula Teknikal bagi Aplikasi Selepas Perubahan Platform Operasi

Peranan/Pemilik/Pelaksana: PED, Pentadbir Aplikasi

Apabila platform operasi berubah, aplikasi penting perniagaan hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi. Perkara yang perlu dipatuhi adalah seperti yang berikut:

10.2.3.1. Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform;

10.2.3.2. Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan

ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan

10.2.3.3. Memastikan perubahan yang sesuai dibuat kepada Pelan Kesinambungan Perkhidmatan UMT dan Pelan Pemulihan Bencana UMT.

10.2.4. Sekatan ke Atas Perubahan dalam Pakej Perisian
Peranan/Pemilik/Pelaksana: PED, Pentadbir Aplikasi

Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.

10.2.5 Prinsip Kejuruteraan Sistem Yang selamat
Peranan/Pemilik/Pelaksana: PED, Pentadbir Aplikasi

Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggarakan 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 berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam yang terkini.

10.2.5.1. Kawalan keselamatan perisian aplikasi dilaksanakan untuk mengelakkan berlakunya capaian oleh pengguna yang tidak sah, pengubahsuaian, pendedahan atau penghapusan maklumat. PED bertanggungjawab menyediakan kawalan seperti berikut:

i. Pelaksanaan satu (1) ID untuk setiap pengguna;

ii. Mengehadkan tahap capaian maklumat serta fungsi berdasarkan tanggungjawab pengguna; dan

iii. Mengadakan sistem log bagi setiap transaksi maklumat kritikal untuk tujuan jejak audit yang menentukan akauntabiliti kepada semua pengguna;

10.2.6. Persekitaran Pembangunan Selamat

Peranan/Pemilik/Pelaksana: PED, Pentadbir Aplikasi

Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.

Universiti perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambi kira:

10.2.6.1. Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem.

10.2.6.2. Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran;

10.2.6.3. Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;

10.2.6.4. Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem;

10.2.6.5. Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai;

10.2.6.6. Kawalan ke atas capaian kepada persekitaran pembangunan sistem dan

10.2.6.7. Pihak berwajib bertanggungjawab mengurus dan melaksanakan kawalan penyimpanan kod sumber bagi perisian aplikasi yang dibangunkan secara dalaman (inhouse) atau luaran (outsourcing) untuk tujuan penyenggaraan dan penambahbaikan melalui:

i. Mewujudkan prosedur penyelenggaraan versi terkini;

ii. Mendokumenkan prosedur salinan (backup) kod sumber bagi penyelenggaraan versi terkini; dan

iii. Menyimpan salinan kod sumber di dua lokasi yang berasingan.

10.2.7. Pembangunan oleh Khidmat Luaran

Peranan/Pemilik/Pelaksana: PED, Pentadbir Aplikasi, Pembekal

Universiti hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara *outsource* oleh pihak luar. Kod sumber (source code) adalah menjadi hak milik universiti. Perkara yang perlu dipatuhi adalah seperti yang berikut:

10.2.7.1. Bagi pembangunan perisian aplikasi secara *outsource* seperti perkiraan perlesenan, kod sumber dan harta intelek sistem yang berkaitan adalah Hak Milik Universiti;

10.2.7.2. Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan

yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori "Pembekal hendaklah memberikan hak kepada universiti untuk mencapai kod sumber dan melaksanakan penambahbaikan risiko";

10.2.7.3. Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik;

10.2.7.4. Penerimaan pengujian berdasarkan kepada kualiti dan ketetapan serahan sistem;

10.2.7.5. Mengguna pakai prinsip dan tatacara *escrow*;

10.2.7.6. Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian; dan

10.2.7.7. Mematuhi standard, prosedur, langkah dan garis panduan yang sedang berkuat kuasa.

10.2.8. Pengujian Keselamatan Sistem

Peranan/Pemilik/Pelaksana: PED, Pentadbir Aplikasi

Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

10.2.8.1. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat;

10.2.8.2. Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat;

10.2.8.3. Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan;

10.2.8.4. Pengujian perlu bagi memastikan sistem berfungsi mengikut spesifikasi yang ditetapkan; dan

10.2.8.5. Pengujian sistem aplikasi perlu dilaksanakan pada beberapa peringkat iaitu:

i. Pengekodan atur cara sistem aplikasi;

ii. Integrasi sistem aplikasi;

iii. Pengujian pengguna;

iv. Pemindahan daripada perkakasan lama kepada baru;

v. Persekitaran yang berbeza; dan

vi. Melaksanakan ujian simulasi dengan semua pihak berkepentingan bagi memastikan sistem beroperasi mengikut keperluan yang ditetapkan oleh pemilik sistem.

10.2.9. Pengujian Penerimaan Sistem

Peranan/Pemilik/Pelaksana: PED, Pentadbir Aplikasi, Pemilik Sistem

Program pengujian penerimaan sistem 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:

10.2.9.1. Pengujian penerimaan sistem hendaklah merangkumi keperluan Keselamatan Sistem Maklumat (rujuk 10.1.1 dan 10.1.2) dan kepatuhan kepada Dasar Pembangunan Selamat (rujuk 10.2.1);

10.2.9.2. Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem diguna pakai;

10.2.9.3. Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian kerentanan (vulnerability scanner); dan

10.2.9.4. Maklumat lanjut berkaitan boleh merujuk kepada dokumen ISO/IEC/IEEE 29119 *Software Testing Standard*.

10.3. Data Ujian

Objektif: Untuk memastikan perlindungan ke atas data yang digunakan untuk pengujian.

10.3.1. Perlindungan Data Ujian

Peranan/Pemilik/Pelaksana: PED, Pentadbir Aplikasi, Pemilik Projek

Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

10.3.1.1. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian;

10.3.1.2. Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian;

10.3.1.3. Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai;

10.3.1.4. Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar; dan

10.3.1.5. Menguji atur cara, modul, sistem aplikasi dan integrasi perisian aplikasi bagi memastikan sistem berfungsi mengikut spesifikasi yang ditetapkan. Langkah berikut diambil semasa pengujian dijalankan:

i. Menggunakan data ujian (dummy) atau data lapuk (historical);

ii. Mengawal penggunaan data terpilih (classified);

iii. Mengehadkan capaian kepada staf yang terlibat sahaja;

iv. Mengadakan kaedah pemberitahuan (flag system) sekiranya capaian dan pengemaskinian maklumat dilakukan; dan

v. Menghapuskan maklumat yang digunakan setelah selesai pengujian (terutamanya apabila menggunakan data lapuk).

10.4. Pembangunan Laman Web

Objektif: Menerangkan perkara-perkara yang perlu dipatuhi dalam membangunkan laman web di universiti

10.4.1. Prosedur Pembangunan Laman Web

Peranan/Pemilik/Pelaksana: PED, Pentadbir Laman Web

Perkara perkara yang perlu dipatuhi adalah seperti yang berikut:

10.4.1.1. Semua maklumat yang hendak dimuatkan ke dalam laman web mestilah mendapat kelulusan mengikut prosedur yang telah ditetapkan;

10.4.1.2. Maklumat di laman web hendaklah dikemas kini dari semasa ke semasa;

10.4.1.3. Pembangunan laman web hendaklah mempunyai ciri-ciri keselamatan bagi mengelak diceroboh dan digodam; dan

10.4.1.4. Pembangunan laman web perlu mematuhi Pekeliling Pengurusan Laman Web Agensi Sektor Awam.

10.5. Pembangunan Aplikasi Mudah Alih

Objektif: Menerangkan perkara yang perlu dipatuhi dalam membangunkan aplikasi mudah alih

10.5.1. Prosedur Integrasi Pembangunan Aplikasi Mudah Alih

Peranan/Pemilik/Pelaksana: PED, Pentadbir Aplikasi

Pembangunan aplikasi mudah alih yang melibatkan integrasi dengan sistem induk hendaklah menggunakan *Application Programming Interface* (API) atau lain-lain kaedah yang bersesuaian yang tidak memberi risiko ancaman keselamatan.

BIDANG 11

HUBUNGAN PEMBEKAL

Rujukan: Standard ISO/IEC 27001:2013 (Annex 15)

11.1. Keselamatan Maklumat dalam Hubungan dengan Pembekal

Objektif: Memastikan pelindungan aset ICT Universiti yang diakses oleh pembekal.

11.1.1. Polisi Keselamatan Maklumat untuk Hubungan Pembekal

Peranan/Pemilik/Pelaksana: PED, Pejabat Bendahari, Pemilik Projek, Pembekal

Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset universiti. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:

11.1.1.1. Mengenal pasti dan mendokumentasikan jenis pembekal mengikut kategori;

11.1.1.2. Proses kitaran hayat yang seragam untuk menguruskan pembekal;

11.1.1.3. Mengawal dan memantau akses pembekal;

11.1.1.4. Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian;

11.1.1.5. Jenis-jenis obligasi kepada pembekal;

11.1.1.6. Pelan kontingensi bagi memastikan ketersediaan kemudahan pemprosesan maklumat;

11.1.1.7. Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber UMT kepada pembekal;

11.1.1.8. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber UMT (LAMPIRAN) 1-A; dan

11.1.1.9. Pembekal perlu mematuhi arahan keselamatan yang berkuat kuasa.

11.1.2. Menangani Keselamatan dalam Perjanjian Pembekal.

Peranan/Pemilik/Pelaksana: PED, Pejabat Bendahari, Pembekal, Semua PTj

Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua staf mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak universiti selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.

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:

11.1.2.1. Memilih syarikat pembekal yang mempunyai pendaftaran sah dengan

Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan;

11.1.2.2. Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan;

11.1.2.3. Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan;

11.1.2.4. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;

11.1.2.5. Jawatankuasa penilaian teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal;

11.1.2.6. Pembekal hendaklah mematuhi semua proses dan prosedur yang ditetapkan semasa menjalankan tugas;

11.1.2.7. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan universiti; dan

11.1.2.8. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh universiti.

11.1.3. Rantaian Bekalan Teknologi Maklumat dan Komunikasi

Peranan/Pemilik/Pelaksana: PED, Pejabat Bendahari, PPH, Pemilik Projek, Pembekal

Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut:

11.1.3.1. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan;

11.1.3.2. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan dan pembekalan produk; dan

11.1.3.3. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.

11.2. Pengurusan Penyampaian Perkhidmatan Pembekal

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

11.2.1. Memantau dan Mengkaji Semula Perkhidmatan Pembekal

Peranan/Pemilik/Pelaksana: PED, Pejabat Bendahari, Pemilik Projek, Pembekal, Semua PTj,

Universiti hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

11.2.1.1. Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan;

11.2.1.2. Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan

11.2.1.3 Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.

11.2.2. Mengurus Perubahan kepada Perkhidmatan Pembekal Peranan/Pemilik/Pelaksana: PED, Pejabat Bendahari, Pemilik Projek, Pembekal, Semua PTj

Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semua risiko. Perkara perkara yang perlu diambil kira adalah seperti yang berikut:

11.2.2.1. Perubahan dalam perjanjian dengan pembekal;

11.2.2.2. Perubahan yang dilakukan oleh universiti bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem pengubahsuaian dasar dan prosedur; dan

11.2.2.3. Perubahan dalam perkhidmatan pembekal hendaklah selaras dengan perubahan rangkaian teknologi baharu, produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.

BIDANG 12

PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

Rujukan: Standard ISO/IEC 27001:2013 (Annex 16)

12.1. Pengurusan Insiden Keselamatan Maklumat dan Penambahbaikan

Objektif: Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kelemahan keselamatan.

12.1.1. Tanggungjawab dan Prosedur

Peranan/Pemilik/Pelaksana: JKKP, PED, Bahagian Keselamatan, PPH, Semua PTj

Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat.

Perkara yang perlu dipatuhi adalah seperti yang berikut:

12.1.1.1. Memberi kesedaran berkaitan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan Siber UMT dan hebahan kepada warga UMT sekiranya ada perubahan; dan

12.1.1.2. Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.

12.1.2. Pelaporan Kejadian Keselamatan Maklumat

Peranan/Pemilik/Pelaksana: JKKP, PED, PPH, Bahagian Keselamatan, Semua PTj

Insiden keselamatan ICT bermaksud musibah (adverse event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar Polisi Keselamatan Siber sama ada yang ditetapkan secara tersurat atau tersirat.

Jenis insiden dapat dikenal pasti seperti yang berikut:

12.1.2.1. Pelanggaran Dasar (Violation of Policy)

Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar Polisi Keselamatan Siber.

12.1.2.2. Penghalangan Penyampaian Perkhidmatan (Denial of Service)

Ancaman ke atas keselamatan sistem komputer di mana perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal. Termasuk *denial of service* (DoS), *distributed denial of service* (DDoS) dan sabotaj.

12.1.2.3. Pencerobohan (Intrusion)

Mengguna dan mengubah suai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan

mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem (system tampering), pindaan data (modification of data) dan pindaan kepada konfigurasi sistem.

12.1.2.4. Pemalsuan (Forgery)

Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/ espionage) dan penipuan (hoax).

12.1.2.5. *Spam*

Spam adalah e-mel yang dihantar ke akaun e-mel orang lain yang tidak dikenali penghantar dalam satu masa dan secara berulang kali (kandungan e-mel yang sama). Ini menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan.

12.1.2.6. Kod Hasad (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.

12.1.2.7. Gangguan/Ancaman (Harrassment/Threats)

Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.

12.1.2.8. Cubaan/Godam (Attempts/Hack)

Percubaan (sama ada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran. Termasuk *spoofing, phishing, probing, war driving dan network scanning*.

12.1.2.9. Kehilangan Fizikal (Physical Loss)

Kehilangan capaian dan kegunaan disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT berpunca dari ancaman pencerobohan.

12.1.3. Aras-aras Kritikal

Peranan/Pemilik/Pelaksana: JKKP, PED, PPH, Semua PTj

Aras-aras kritikal insiden keselamatan adalah merujuk kepada tahap risiko di dalam Polisi Pengurusan Risiko UMT dan diberi keutamaan seperti yang berikut:

12.1.3.1. **Keutamaan 1**

Aktiviti yang boleh mengancam nyawa, keamanan dan keselamatan negara perlu dilaporkan,

12.1.3.2 **Keutamaan 2**

Insiden keselamatan ICT seperti yang berikut:

i. Maklumat didapati hilang atau disyaki hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa;

ii. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;

iii. Kata laluan atau mekanisme kawalan dicuri atau didedahkan;

iv. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan

v. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.

12.1.3.3. **Keutamaan 3**

Insiden hanya menjejaskan sebahagian infrastruktur ICT dan tidak ada tanda-tanda insiden seterusnya. Sebagai contoh, jangkitan virus terhadap beberapa komputer.

12.1.4. Prosedur Pelaporan Insiden Keselamatan Siber berdasarkan:

12.1.4.1. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi;

12.1.4.2. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; dan

12.1.4.3. Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan Siber ICT UMT.

12.1.5. Prosedur Operasi Standard Pengurusan Pengendalian Insiden Keselamatan Siber UMT

Peranan/Pemilik/Pelaksana: JKKP, PED, PPH

Melaporkan Insiden Keselamatan:

12.1.5.1. Semua insiden keselamatan mestilah disahkan oleh Pentadbir Keselamatan ICT sebaik sahaja insiden itu dikenal pasti;

12.1.5.2. Memaklumkan kepada Pengarah CERT/ CIO dan ketua jabatan selepas insiden disahkan;

12.1.5.3. Bergantung kepada keutamaan (rujuk 12.1.3. Aras-Aras Kritikal), insiden mestilah dilaporkan kepada Pengurusan Tertinggi Universiti;

12.1.5.4. Melaporkan kepada entiti luar (NACSA, Pihak Berkuasa) hanya sekiranya ada keperluan;

12.1.5.5. Semua insiden e-mel akan dilaporkan kepada pihak sokongan pembekal perkhidmatan e-mel; dan

12.1.5.6. Sila rujuk Lampiran 4 - Maklumat Pihak Bertanggungjawab bagi Pengendalian Insiden.

12.1.6. Agihan tindakan (Escalation Procedures)

Aras Kritikal Insiden	Prosedur Agihan Tindakan
Keutamaan 1	• Mengesahkan insiden. • Memaklumkan kepada Pengurusan Tertinggi Universiti melalui NACSA/CIO dan ICTSO. • Merekodkan pada Borang Insiden.

	• Mengesahkan insiden. • Memaklumkan kepada NACSA/CIO atau ICTSO. • Merekodkan pada Borang Insiden.
Keutamaan 3	• Mengesahkan insiden. • Memaklumkan kepada CERT UMT. • Merekodkan pada Borang Insiden.

12.1.7. Pelaporan Kelemahan Keselamatan Maklumat

Peranan/Pemilik/Pelaksana: JKKP, PED, CERT UMT, Bahagian Keselamatan, Pengguna

Warga UMT dan bukan Warga UMT yang menggunakan sistem dan perkhidmatan maklumat universiti dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan ICT.

12.1.8. Penilaian dan Keputusan Mengenai Kejadian Keselamatan Maklumat

Peranan/Pemilik/Pelaksana: JKKP, PED, CERT UMT, Bahagian Keselamatan

Kejadian keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.

12.1.9. Tindak Balas Terhadap Insiden Keselamatan Maklumat

Peranan/Pemilik/Pelaksana: JKKP, PED, CERT UMT, Bahagian Keselamatan, Pentadbir ICT

Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan Siber UMT.

Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut:

12.1.9.1. Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku;

12.1.9.2. Menjalankan kajian forensik sekiranya perlu;

12.1.9.3. Menghubungi pihak yang berkenaan dengan secepat mungkin;

12.1.9.4. Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti;

12.1.9.5. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;

12.1.9.6. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;

12.1.9.7. Menyediakan tindakan pemulihan segera; dan

12.1.9.8. Memaklumkan atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.

12.1.10. Pembelajaran daripada Insiden Keselamatan Maklumat (Learning from Information Security Incidents)

Peranan/Pemilik/Pelaksana: JKKP, PED, CERT UMT, Bahagian Keselamatan, Pentadbir ICT

Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan

kemungkinan berlakunya kejadian pada masa hadapan 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.

12.1.11. Pengumpulan Bahan Bukti

Peranan/Pemilik/Pelaksana: JKKP, PED, ICTSO, CERT UMT, Bahagian Keselamatan, Pentadbir Keselamatan ICT

Pentadbir Keselamatan ICT hendaklah merekodkan semua insiden keselamatan yang dikesan. Sekurang-kurangnya, maklumat berikut hendaklah direkodkan:

12.1.11.1. Tarikh dan masa insiden;

12.1.11.2. Menyenaraikan sistem yang terjejas akibat insiden atau kejadian tersebut;

12.1.11.3. Ringkasan insiden;

12.1.11.4. Tindakan yang diambil untuk membetulkan insiden;

12.1.11.5. Senarai bukti yang diperoleh semasa siasatan; dan

12.1.11.6. Pengajaran yang diperoleh.

BIDANG 13

ASPEK KESELAMATAN MAKLUMAT BAGI PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Rujukan: Standard ISO/IEC 27001:2013 (Annex 17)

13.1. Kesinambungan Keselamatan Maklumat

Objektif: Kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan *bisnes* universiti.

13.1.1 Perancangan Kesinambungan Keselamatan Maklumat

Peranan/Pemilik/Pelaksana: JKKP, Semua PTj

Universiti hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, universiti perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi universiti.

Universiti juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara-perkara yang perlu dipertimbangkan adalah seperti berikut:

13.1.1.1. Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP)

13.1.1.2. Merangka dan menetapkan PKP;

13.1.1.3. Mengenal pasti perkhidmatan kritikal;

13.1.1.4. Melaksanakan Kajian Impak Perkhidmatan (Business Impact Analysis - BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal;

13.1.1.5. Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Garis Panduan Pengurusan Media dan Pelan Pemulihan Bencana ICT;

13.1.1.6. Melaksanakan program kesedaran dan latihan pasukan PKP dan warga UMT;

13.1.1.7. Melaksanakan simulasi ke atas dokumen di para (13.1.1.3) ; dan

13.1.1.8. Melaksanakan penyelenggaraan ke atas pelan di para (13.1.1.3).

13.1.2. Pelaksanaan Kesinambungan Keselamatan Maklumat
Peranan/Pemilik/Pelaksana: JKKP, Semua PTj

Universiti hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggarakan proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut:

13.1.2.1. Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal universiti yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Garis Panduan Pengurusan Media dan Pelan Pemulihan Bencana ICT terkini;

13.1.2.2. Melaksanakan post-mortem dan mengemas kini pelan-pelan PKP;

13.1.2.3. Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal universiti;

13.1.2.4. Mengemas kini struktur tadbir urus PKP UMT jika berlaku pertukaran; dan

13.1.2.5. Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.

13.1.3. Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat

Peranan/Pemilik/Pelaksana: JKKP, Semua PTj

Universiti hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.

13.2. Lewahan (Redundancy)

Objektif: Untuk memastikan ketersediaan kemudahan pemprosesan maklumat dengan mewujudkan lewahan.

13.2.1. Ketersediaan Kemudahan Pemprosesan Maklumat

Peranan/Pemilik/Pelaksana: PED

Kemudahan pemprosesan maklumat universiti perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (failover test) keberkesanannya dari semasa ke semasa.

BIDANG 14

PEMATUHAN

Rujukan: Standard ISO/IEC 27001:2013 (Annex 18)

14.1. Pematuhan dan Keperluan Perundangan dan Kontrak

Objektif: Mengelakkan pelanggaran obligasi undang-undang, statutori, kawal selia atau kontrak yang berkaitan dengan keselamatan maklumat dan sebarang keperluan keselamatan

14.1.1. Pengenalpastian Keperluan Undang-undang dan Kontrak yang Terpakai

Peranan/Pemilik/Pelaksana: PUU, PED, Semua PTj, Warga UMT, Pihak Ketiga,

Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga UMT, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan universiti. Senarai perundangan dan peraturan serta garis panduan yang berkuat kuasa di universiti perlu dipatuhi oleh semua pengguna seperti di Lampiran 2.

14.1.2. Hak Harta Intelek

Peranan/Pemilik/Pelaksana: PPP, Semua PTj

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.

14.1.3. Perlindungan Rekod

Peranan/Pemilik/Pelaksana: Pejabat Pendaftar, PPPA, PSNZ, Semua PTj

Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung dalam keperluan perundangan, peraturan dan perjanjian kontrak.

14.1.4. Privasi dan Perlindungan Maklumat Peribadi

Peranan/Pemilik/Pelaksana: Pejabat Pendaftar, PED, Semua PTj

Universiti hendaklah melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.

14.1.5. Peraturan Kawalan Kriptografi

Peranan/Pemilik/Pelaksana: PED, Semua PTj

Kawalan kriptografi hendaklah digunakan bagi mematuhi semua perjanjian, undang-undang dan peraturan yang relevan.

14.2. Kajian Semula Keselamatan Maklumat

Objektif: memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur universiti.

14.2.1. Kajian Semula Keselamatan dan Maklumat Secara Berkecuali

Peranan/Pemilik/Pelaksana: PED, PPPA

Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.

14.2.2. Pematuhan Polisi dan Standard Keselamatan

Peranan/Pemilik/Pelaksana: PED, Pejabat NC, PPPA, Semua PTj, Pengguna

Setiap pengguna di universiti hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber UMT dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.

Universiti 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.

14.2.3. Kajian Semula Pematuhan Teknikal

Peranan/Pemilik/Pelaksana: PED, PPPA

Universiti hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.

14.2.4 Pelanggaran Polisi

Peranan/Pemilik/Pelaksana: PED, PUU, Unit Integriti, Bahagian Keselamatan, Semua PTj, Warga UMT, Pengguna

(a) Pelanggaran polisi ini boleh mengakibatkan tindakan undang-undang diambil terhadap pengguna;

(b) Pelanggaran polisi oleh mana-mana staf universiti sama ada staf tetap, staf kontrak atau sambilan boleh dikenakan tindakan tatatertib di bawah Akta Badan-Badan Berkanun (Tatatertib dan Surcaj) 2000 (Akta 605), Akta Rahsia Rasmi 1972

atau mana-mana peruntukan undang-undang yang berkaitan; dan

(c) Pelanggaran polisi oleh mana-mana pelajar boleh mengakibatkan tindakan tatatertib di bawah Kaedah-kaedah Universiti Malaysia Terengganu (Tatatertib Pelajar-Pelajar) 2009.

GLOSARI

Terma	Keterangan
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CD-ROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Inventori Aset ICT	Senarai terperinci Aset ICT
Backup	Proses sandar/salinan sesuatu dokumen atau maklumat.
Bandwidth	Jaur Lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
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.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan Pencurian identiti, pencurian maklumat (information theft/espionage), penipuan (hoaxes).

NACSA	Pasukan tindakan kecemasan komputer negara / *National Cyber Security Agency* (NACSA), Malaysia. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (hub) 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.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
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.
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.

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.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Logout* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
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.
MODEM	*MOdulator DEModulator* 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.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi- fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *Spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.

Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ia tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Switches	Sejenis peranti yang menghubungkan beberapa segmen rangkaian komputer
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
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.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.
Warga UMT	Staf UMT dan Pelajar UMT
Pengguna	Pengguna ialah orang yang menggunakan peralatan ICT dan persekitaran Siber Universiti iaitu Warga UMT, pembantu penyelidik, profesor pelawat
Pihak ketiga	Pembekal, Pakar Runding
Universiti	Universiti Malaysia Terengganu
PTj	Pusat Tanggungjawab
Sistem	Input output proses

Program Utiliti	Program atau perisian sokongan yang membantu kelancaran perkakasan komputer, sistem pengendalian dan perisian aplikasi.
FTKKI	Fakulti Teknologi Kejuruteraan Kelautan dan Informatik
FSSM	Fakulti Sains dan Sekitaran Marin
FPSM	Fakulti Perikanan dan Sains Makanan
FPEPS	Fakulti Perniagaan, Ekonomi dan Pembangunan Sosial
FPM	Fakulti Pengajian Maritim
PPAL	Pusat Pendidikan Asas dan Lanjutan
AKUATROP	Institut Akuakultur Tropika dan Penyelidikan Perikanan
IMB	Institut Bioteknologi Marin
INOS	Institut Oseanografi dan Sekitaran
IBTPL	Institut Biodiversiti Tropika dan Pembangunan Lestari
PNC	Pejabat Naib Canselor
BEND	Pejabat Bendahari
PPH	Pejabat Pembangunan dan Harta
PPPA	Pusat Pembangunan dan Pengurusan Akademik
PPP	Pejabat Pengurusan Penyelidikan
PED	Pusat Ekosistem Digital
PPBI	Pusat Pembangunan Bakat dan Inovasi
Penerbit UMT	Penerbit UMT
PKU	Pusat Kesihatan Universiti
PASTEM	Pusat Asasi STEM
PPIJI	Pusat Pemindahan Ilmu dan Jaringan Industri
IC	Pusat Antarabangsa
PPPL	Pusat Perkhidmatan Penyelidikan dan Lapangan
TSR	Pusat Transformasi Perancangan Strategik dan Risiko

PISM	Pusat Islam Sultan Mahmud
PSNZ	Perpustakaan Sultanah Nur Zahirah
Pejabat Pendaftar	Pejabat Pendaftar
HEPA	Pejabat Hal Ehwal Pelajar dan Alumni
Bahagian Keselamatan	Bahagian Keselamatan
PKK	Pejabat Komunikasi Korporat
Bahagian Audit Dalam	Bahagian Audit Dalam
PPUU	Pejabat Penasihat Undang-undang
Unit Integriti	Unit Integriti UMT
JKKP	Jawatankuasa Keselamatan dan Kesihatan Pekerjaan
Pemilik Data	Individu atau PTj yang bertanggungjawab untuk semua data di dalam sistem yang berkaitan.
Pemilik Sistem	PTj yang bertanggungjawab sepenuhnya untuk merancang dan menyelaras keperluan sistem aplikasi PTj masing-masing.

RUJUKAN

Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Jabatan Perdana Menteri. (2020). *Arahan Pentadbiran Ketua Pengarah MAMPU Bil 4- Polisi Keselamatan Siber MAMPU* .

Bahagian Pengurusan Maklumat, Kementerian Pendidikan Malaysia (KPM). (2019). *Polisi Keselamatan Siber* Versi 1.0.

MIMOS, Pejabat Ketua Pegawai Kerajaan Keselamatan Malaysia, MAMPU, Cyber Security Malaysia. (2016). *Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)* Versi 1.0.

ISO/IEC 27001:2013 – Information technologies – Security techniques – Information Security Management Systems– Requirement. (2013).

LAMPIRAN

Lampiran 1

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER
UNIVERSITI MALAYSIA TERENGGANU (UMT)

Nama (Huruf Besar): .....

No. Kad Pengenalan: .....

Jawatan: .....

Pusat Tanggungjawab: .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber UMT; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : .....

Tarikh : .....

Pengesahan Ketua Jabatan

.....
( )

Tarikh: .....

Lampiran 1-A

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER
UNIVERSITI MALAYSIA TERENGGANU (UMT)

Nama (Huruf Besar): .....

No. Kad Pengenalan: .....

Jawatan: .....

Syarikat: .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber UMT;
2. Saya juga berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub dalam Polisi Keselamatan Siber UMT; dan
3. Sekiranya saya atau mana-mana individu yang mewakili syarikat ini didapati melanggar polisi yang telah ditetapkan, maka saya sebagai wakil syarikat bersetuju tindakan undang-undang boleh diambil ke atas sesiapa yang terlibat mengikut peruntukan-peruntukan undang-undang sedia ada yang sedang berkuat kuasa.

Tandatangan : .....

Tarikh : .....

Pengesahan Ketua Jabatan

.....

( )

Tarikh: .....

Lampiran 2

SENARAI PERUNDANGAN DAN PERATURAN

[1] Arahan Keselamatan (Semakan dan Pindaan 2015).

[2] Arahan 20 (Semakan Semula) – Dasar dan Mekanisme Pengurusan Bencana Negara.

[3] Arahan 24 - Dasar dan Mekanisme Pengurusan Krisis Siber Negara.

[4] Pekeliling Am Bil. 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam.

[5] Rancangan Malaysia ke-11.

[6] Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam.

[7] Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital *Document Management System* (DDMS) Sektor Awam 25 Januari 2015.

[8] Dasar Kriptografi Negara 12 Julai 2013

[9] Surat Pekeliling Perbendaharaan – Garis Panduan Mengenai Pengurusan Perolehan *Information Telecommunication Technology* ICT Kerajaan SPP 3/2013.

[10] Pekeliling Perbendaharaan Malaysia PK 2/2013 – Kaedah Perolehan Kerajaan.

[11] Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013.

[12] Arahan Ketua Pegawai Keselamatan Kerajaan 5 Jun 2012 – Langkah-langkah Keselamatan Perlindungan bagi Mencegah Kehilangan Komputer Riba dan Peranti Mudah Alih di Sektor Awam

[13] PK3.2 - Manual Perolehan Perkhidmatan Perunding Edisi 2011 (Pindaan Kedua).

[14] Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat 24 Nov 2010.

[15] Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam, 22 Jan 2010.

[16] Akta 709 – Akta Perlindungan Data Peribadi 2010.

[17] Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam.

[18] Surat Arahan Ketua Pengarah MAMPU - Langkah-langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agensi Kerajaan, 23 Nov 2007.

[19] Surat Arahan Ketua Pengarah MAMPU - Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan, 1 Jun 2007.

[20] Arahan Teknologi Maklumat, MAMPU, 2007.

[21] Akta 680 – Aktiviti Kerajaan Elektronik 2007.

[22] Arahan Ketua Setiausaha Negara Bil. 1 Tahun 2007 – Langkah-langkah Keselamatan Perlindungan untuk Larangan Penggunaan Telefon Bimbit atau Lain-lain Peralatan Komunikasi ICT Tanpa Kebenaran atau Kuasa sang Sah di Agensi-Agensi Kerajaan

[23] Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan, 20 Oktober 2006.

[24] Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam.

[25] Garis Panduan IT Outsourcing Agensi-Agensi Sektor Awam 04/2006.

[26] Akta 658 – Akta Perdagangan Elektronik 2006.

[27] Surat Pekeliling Am Bil. 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam

[28] Akta 629 – Akta Arkib Negara 2003.

[29] Akta 606 – Akta Cakera Optik 2000.

[30] Akta 588 – Akta Komunikasi dan Multimedia 1998. (in revision)

[31] Akta 562 - Akta Tandatangan Digital 1997.

[32] Akta 563 – Akta Jenayah Komputer 1997.

[33] Akta 564 - Telemedicine Act 1997. (not enforced)

[34] Akta 88 – Akta Rahsia Rasmi 1972.

[35] Akta 332 – Akta Hak Cipta 1987.

[36] Surat Pekeliling Am Bilangan 2/1987 – Peraturan Pengurusan Rahsia Rasmi Selaras dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987).

[37] Akta 298 – Kawasan Larangan Tempat Larangan 1959 Akta 56 – Akta Keterangan 1950.

[38] National Cyber Security Policy (NCSP)

[39] Guideline to Determine Information Security Professionals Requirement for the CNII Agencies/Organisations.

[40] Arahan Tetap Sasaran Penting.

[41] Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara.

[42] Garis Panduan Kontrak ICT bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi.

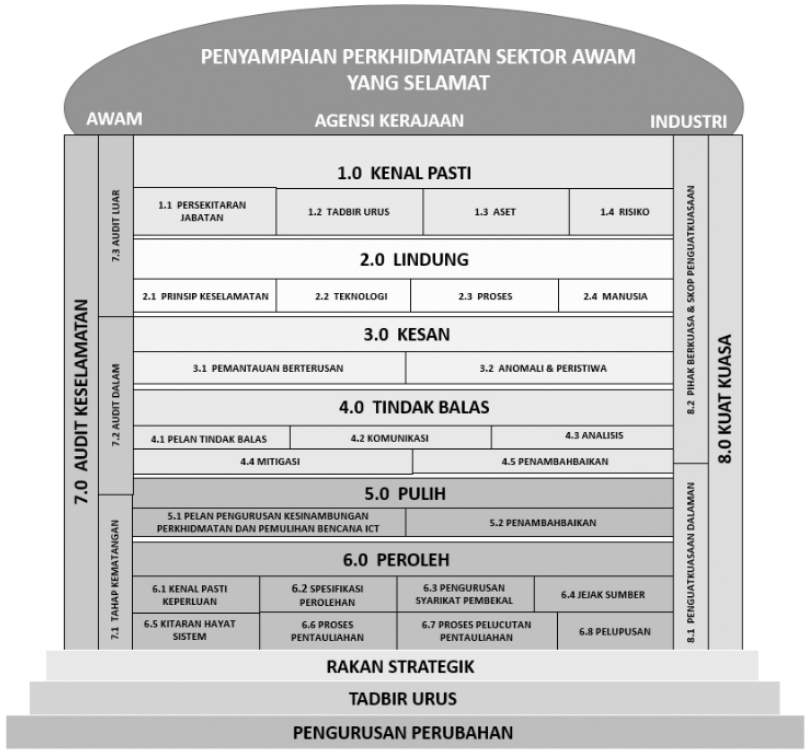
[43] Perintah Am Bab D.

[44] Surat Arahan Ketua Pengarah MAMPU 2015: Pelaksanaan Rasionalisasi Laman Web Sektor Awam.

[45] Pekeliling Kemajuan Pentadbiran Awan Bil. 1 Tahun 2021:Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam.

Lampiran 3

Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)



Lampiran 4

Meja Bantuan

Kaunter ICT Aras Bawah, Pusat Pengurusan Pengetahuan dan Teknologi Komunikasi , Universiti Malaysia Terengganu

No Telefon: 09-668 4490/sistem *CustCare* PED

GCERT

Agensi Keselamatan Siber Negara (NACSA)

Majlis Keselamatan Negara, Aras LG & G, Blok Barat, Bangunan Perdana Putra, Pusat Pentadbiran Kerajaan Persekutuan. 62502 PUTRAJAYA

Melaporkan Insiden Keselamatan di Luar Waktu Pejabat

Sebarang laporan insiden keselamatan ICT boleh dimajukan terus kepada:

Pengarah CERT Universiti Malaysia Terengganu

No Telefon: 09-668 3505 / e-mel: cert@umt.edu.my

Atau

Pegawai Keselamatan ICT

No Telefon : 09-668 4210/ e-mel: ictso@umt.edu.my

Penerbit UMT
Menjana Khazanah Ilmuwan
https://penerbit.umt.edu.my

eISBN 978-967-2793-46-5