Kaedah-Kaedah Universiti Putra Malaysia
(Teknologi Maklumat Dan Komunikasi) 2014

Suatu Kaedah-Kaedah untuk mengadakan peruntukan bagi perkara-perkara yang berhubungan dengan teknologi maklumat dan komunikasi di Universiti Putra Malaysia termasuklah mengenai keselamatan dan pengurusan teknologi maklumat dan komunikasi dan bagi perkara-perkara lain yang berhubungan dengannya.

[tarikh kuat kuasa: 1 Januari 2014]

Pada menjalankan kuasa yang diberikan oleh subseksyen 37(1) Perlembagaan Universiti Putra Malaysia, Lembaga Pengarah membuat kaedah-kaedah berikut:-

Bahagian A - Permulaan

Nama dan Pemakaian

1. Kaedah-Kaedah ini bolehlah dinamakan Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2014 dan hendaklah mula berkuatkuasa mulai 1 Januari 2014.

Tafsiran

2. Dalam Kaedah-Kaedah ini, melainkan konteksnya menghendaki makna yang lain–

"Aset teknologi maklumat dan komunikasi" termasuklah perkakasan, perisian, aplikasi, dokumentasi berkaitan dengan teknologi maklumat dan komunikasi yang berada bawah tanggungjawab Universiti;

"Data dan maklumat" ertinya fakta atau koleksi fakta sama ada dalam bentuk kertas atau elektronik yang mengandungi maklumat yang disimpan atau digunakan oleh

Universiti termasuklah semua dokumentasi, piawaian operasi, rekod-rekod Universiti, rekod pelanggan, staf atau pelajar;

"Pelajar" ertinya pelajar Universiti mengikut tafsiran Akta Universiti dan Kolej Universiti 1971;

"Staf" ertinya pekerja Universiti mengikut tafsiran Perlembagaan Universiti.

Bahagian B - Dasar Teknologi Maklumat Dan Komunikasi

Keperluan Mengadakan Dasar

3. Lembaga Pengarah Universiti hendaklah menyediakan suatu dasar Universiti berkaitan dengan teknologi maklumat dan komunikasi di Universiti Putra Malaysia termasuklah mengenai keselamatan dan pengurusan teknologi maklumat dan komunikasi dan bagi perkara-perkara lain yang berhubungan dengannya.

Pelaksanaan dan Pindaan Dasar

4.(1) Dasar mengenai teknologi maklumat dan komunikasi Universiti yang dibuat oleh Lembaga Pengarah Universiti hendaklah dilaksanakan oleh Universiti dan hendaklah diurus-selia oleh pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat Universiti.

(2) Dasar mengenai teknologi maklumat dan komunikasi Universiti boleh dipinda dan dibuat baharu dari semasa ke semasa oleh Lembaga Pengarah Universiti.

Bahagian C – Penubuhan Jawatankuasa-Jawatankuasa

Penubuhan Jawatankuasa Teknologi Maklumat dan Komunikasi Universiti

5.(1) Jawatankuasa Teknologi Maklumat dan Komunikasi Universiti hendaklah terdiri daripada:–

(a) Timbalan Naib Canselor yang dipertanggungkan dengan tanggungjawab teknologi maklumat dan komunikasi sebagaimana yang ditetapkan oleh Naib Canselor, yang hendaklah menjadi Pengerusi;

(b) Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti, yang hendaklah menjadi Setiausaha;

(c) Pendaftar atau wakilnya;

(d) Bendahari atau wakilnya;

(e) Ketua Pustakawan atau wakilnya;

(f) Dekan Fakulti Sains Komputer dan Teknologi Maklumat;

(g) Dekan Fakulti Kejuruteraan atau wakilnya yang mempunyai kepakaran teknologi maklumat dan komunikasi;

(h) Ketua bagi pejabat yang dipertanggungkan dengan tanggungjawab mengenai laman sesawang Universiti;

(i) Mana-mana staf atau pelajar lain Universiti yang dilantik oleh Naib Canselor.

(2) Timbalan Ketua di pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi hendaklah menjadi ahli *ex-officio* Jawatankuasa tetapi tidak berhak untuk mengundi.

(3) Jawatankuasa Teknologi Maklumat dan Komunikasi hendaklah mempunyai bidang kuasa berikut:-

(a) memperakukan Dasar Teknologi Maklumat dan Komunikasi Universiti kepada Jawatankuasa Pengurusan Universiti dan Lembaga Pengarah Universiti;

(b) membuat garis panduan, arahan kerja atau tatacara bagi pemakaian khusus teknologi maklumat dan komunikasi dalam Universiti mengikut keperluan Dasar Teknologi Maklumat dan Komunikasi Universiti dan Kaedah-Kaedah ini;

(c) membuat pemantauan mengenai pematuhan Dasar Teknologi Maklumat dan Komunikasi Universiti dan Kaedah-Kaedah ini oleh staf dan pelajar Universiti; dan

(d) menilai teknologi maklumat dan komunikasi yang terkini dan bersesuaian dengan Universiti dan mencadangkan penggunaannya mengikut keperluan yang wajar kepada Jawatankuasa Pengurusan Universiti;

Penubuhan Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi

6.(1) Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi hendaklah terdiri daripada:-

(a) Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal keselamatan teknologi maklumat dan komunikasi yang hendaklah menjadi Pengerusi;

(b) Timbalan Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi;

(c) Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab keselamatan Universiti;

(d) Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab pembangunan dan pengurusan aset Universiti;

(e) Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab pengurusan keselamatan dan kesihatan pekerjaan Universiti;

(f) Ketua Unit yang dipertanggungkan dengan tanggungjawab keselamatan teknologi maklumat dan komunikasi Universiti yang hendaklah menjadi Setiausaha;

(g) Mana-mana staf lain Universiti yang dilantik oleh Pengerusi.

(2) Ketua-Ketua Unit di pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi hendaklah menjadi ahli *ex-officio* Jawatankuasa tetapi tidak berhak untuk mengundi.

(3) Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi hendaklah mempunyai bidang kuasa berikut:–

(a) membuat garis panduan, arahan kerja atau tatacara bagi keselamatan teknologi maklumat dan komunikasi dalam Universiti mengikut keperluan Dasar Teknologi Maklumat dan Komunikasi Universiti dan Kaedah-Kaedah ini;

(b) menguatkuasakan garis panduan, arahan kerja atau tatacara bagi keselamatan teknologi maklumat dan komunikasi Universiti;

(c) menerima laporan keselamatan teknologi maklumat dan komunikasi, termasuk mengenai apa-apa insiden teknologi maklumat dan komunikasi dalam Universiti, dan mengambil tindakan yang wajar dan suaimanfaat mengenai laporan tersebut;

(d) membuat apa-apa cadangan kepada Jawatankuasa Pengurusan Universiti bagi mengelakkan insiden keselamatan teknologi maklumat dan komunikasi berlaku;

(e) menilai teknologi maklumat dan komunikasi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan teknologi maklumat dan komunikasi; dan

(f) menubuhkan pasukan pengendali insiden keselamatan teknologi maklumat dan komunikasi dan menetapkan terma rujukan bagi pasukan pengendali insiden keselamatan teknologi maklumat dan komunikasi tersebut.

Urus Setia

7. Pusat yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti hendaklah menjadi urus setia bagi Jawatankuasa Teknologi Maklumat dan Komunikasi Universiti dan Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi Universiti.

Bahagian D – Pengurusan Aset Teknologi Maklumat dan Komunikasi

Pengenalpastian Aset Teknologi Maklumat dan Komunikasi

8.(1) Ketua bagi sesuatu pusat tanggungjawab di Universiti hendaklah mengenalpasti dan merekodkan semua aset teknologi maklumat dan komunikasi sedia ada di pusat tanggungjawab masing-masing mengikut cara yang ditetapkan oleh Jawatankuasa Teknologi Maklumat dan Komunikasi Universiti dan Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi Universiti.

(2) Sekiranya terdapat apa-apa penambahan atau pelupusan aset teknologi maklumat dan komunikasi di pusat tanggungjawab, ketua pusat tanggungjawab itu hendaklah mengemaskini maklumat penambahan atau pelupusan itu.

Kawalan Keselamatan Aset dan Kawasan

9. Ketua bagi sesuatu pusat tanggungjawab di Universiti hendaklah melindungi aset teknologi maklumat dan komunikasi, dan kawasan persekitaran aset itu, daripada pencerobohan, ancaman, kerosakan dan akses yang tidak dibenarkan, dan hendaklah:—

(a) mengenalpasti aset teknologi maklumat dan komunikasi yang ada di pusat tanggungjawabnya dan memastikan keselamatan aset itu dengan mengadakan pengawalan kebolehaksesan aset itu; dan

(b) mengenalpasti kawasan keselamatan fizikal aset teknologi maklumat dan komunikasi dan menggunakan keselamatan perimeter termasuklah mengadakan halangan seperti dinding, kamera litar tertutup, pagar kawalan, pengawal keselamatan, pintu keselamatan, kawalan akses biometrik, kad pintar dan akses dengan kebenaran sahaja, untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat.

Penyelenggaraan Aset Teknologi Maklumat dan Komunikasi

10. Ketua bagi sesuatu pusat tanggungjawab di Universiti hendaklah memastikan:–

(a) penyelenggaraan bagi sesuatu aset teknologi maklumat dan komunikasi dibuat dari semasa ke semasa mengikut:

(i) spesifikasi yang ditetapkan oleh pengeluar aset teknologi maklumat dan komunikasi itu; atau

(ii) garis panduan, arahan kerja atau tatacara seperti yang ditetapkan oleh Jawatankuasa Teknologi Maklumat dan Komunikasi Universiti atau Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi Universiti;

(b) aset teknologi maklumat dan komunikasi diselenggara oleh staf atau pihak ketiga yang berkelayakan dan diberi akses kepada aset itu oleh ketua pusat tanggungjawab;

*(c)*penyelenggaraan berkala bagi aset teknologi maklumat dan komunikasi dilaksanakan mengikut jadual yang ditetapkan dari semasa ke semasa; dan

(d) penyelenggaraan yang dilakukan ke atas aset teknologi maklumat dan komunikasi dilakukan dalam pengetahuan pegawai teknologi maklumat dan komunikasi yang dipertanggungkan dengan tanggungjawab teknologi maklumat dan komunikasi di pusat tanggungjawab itu.

Infrastruktur Rangkaian Komputer

11.(1) Universiti hendaklah membangunkan infrastuktur rangkaian komputer bagi penggunaan kampus utama Universiti dan kampus cawangan Universiti.

(2) Ketua bagi sesuatu pusat tanggungjawab di Universiti hendaklah mengenalpasti dan merekodkan infrastruktur rangkaian komputer yang terdapat di pusat tanggungjawab masing-masing mengikut cara yang ditetapkan oleh Jawatankuasa Teknologi Maklumat dan Komunikasi Universiti dan Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi Universiti.

(3) Ketua bagi sesuatu pusat tanggungjawab di Universiti hendaklah mengambil langkah-langkah keselamatan bagi mengelakkan pencerobohan atau kerosakan ke atas infrastruktur rangkaian komputer seperti yang dicadangkan atau diarahkan oleh Ketua yang dipertanggungkan dengan tanggungjawab bagi hal ehwal teknologi maklumat dan komunikasi Universiti atau oleh Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi.

(4) Sekiranya terdapat apa-apa penambahan atau pelupusan bagi infrastruktur rangkaian komputer, ketua pusat tanggungjawab itu hendaklah mengemaskini maklumat penambahan atau pelupusan itu.

5) Ketua yang dipertanggungkan dengan tanggungjawab bagi hal ehwal teknologi maklumat dan komunikasi Universiti hendaklah memasang sistem pencegah ancaman dan pencerobohan pada infrastruktur rangkaian komputer bagi mengelakkan aktiviti-aktiviti pencerobohan kepada sistem rangkaian komputer dan capaian internet Universiti.

Bahagian E – Pengurusan Perisian

Pelindungan Hakcipta dan Pelesenan

12.(1) Staf atau pelajar hendaklah hanya menggunakan perisian atau aplikasi yang dilesenkan secara sah daripada pemunya perisian atau aplikasi yang berkenaan.

(2) Mana-mana staf atau pelajar yang menggunakan perisian atau aplikasi atau media elektronik atau selainnya yang ada hakcipta tanpa lesen yang sah hendaklah

bertanggungjawab secara bersendirian terhadap apa-apa liabiliti atau gantirugi yang dituntut oleh pemunya perisian atau aplikasi tersebut dan hendaklah pada sepanjang masa menggantirugikan Universiti terhadap apa-apa kerugian yang ditanggung oleh Universiti yang berbangkit daripada tuntutan pemunya perisian atau aplikasi atau media elektronik atau selainnya yang ada hakcipta tersebut kepada Universiti.

Perlindungan Daripada Perisian Berbahaya

13.(1) Staf di sesuatu pusat tanggungjawab hendaklah menahan diri daripada memuat turun atau memuat naik atau memasang apa-apa perisian yang berbahaya, atau yang telah dinasihatkan oleh Ketua yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi bagi Universiti atau oleh pegawai teknologi maklumat yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi di pusat tanggungjawab itu sebagai berbahaya, ke dalam perkakasan teknologi maklumat dan komunikasi.

(2) Pelajar di sesuatu pusat tanggungjawab hendaklah menahan diri daripada memuat turun atau memuat naik atau memasang apa-apa perisian yang berbahaya, atau yang telah dinasihatkan oleh ketua yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi bagi Universiti atau oleh pegawai teknologi maklumat yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi di pusat tanggungjawab itu sebagai berbahaya, ke dalam perkakasan teknologi maklumat dan komunikasi.

(3) Mana-mana staf atau pelajar yang melanggar peruntukan ini adalah melakukan suatu perbuatan pelanggaran tatatertib dan boleh diambil tindakan mengikut prosedur tatatertib yang berkenaan dengan staf atau pelajar itu.

Bahagian F – Pengurusan Data dan Maklumat

Tanggungjawab Mengurus dan Mengawal Data dan Maklumat

14.(1) Staf dan pelajar yang diberi akses dan dibenarkan menggunakan aset teknologi maklumat dan komunikasi Universiti hendaklah bertanggungjawab melindungi data dan maklumat dan memastikan data dan maklumat yang disimpan dalam storan aset teknologi maklumat dan komunikasi itu dapat digunakan semula.

(2) Mana-mana staf atau pelajar yang melanggar peruntukan ini adalah melakukan suatu perbuatan pelanggaran tatatertib dan boleh diambil tindakan mengikut prosedur tatatertib yang berkenaan dengan staf atau pelajar itu.

Penyelenggaraan Data dan Maklumat

15. Ketua bagi sesuatu pusat tanggungjawab di Universiti hendaklah memastikan—

(a) data dan maklumat, yang disimpan dalam storan yang menggunakan aset teknologi maklumat dan komunikasi, diselenggara dari semasa ke semasa mengikut spesifikasi yang ditetapkan oleh garis panduan, arahan kerja atau tatacara yang ditetapkan oleh Jawatankuasa Teknologi Maklumat dan Komunikasi Universiti dan Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi Universiti;

(b) penyelenggaraan berkala bagi data dan maklumat dilaksanakan mengikut jadual yang ditetapkan dari semasa ke semasa;

(c) penyelenggaraan data dan maklumat hendaklah dibuat oleh staf atau pihak ketiga yang berkelayakan dan diberi akses kepada data dan maklumat itu oleh ketua pusat tanggungjawab itu;

(d) penyelenggaraan data dan maklumat itu dilakukan dalam pengetahuan pegawai teknologi maklumat yang dipertanggungkan dengan tanggungjawab teknologi maklumat dan komunikasi di pusat tanggungjawab itu.

Perkongsian Data dan Maklumat

16. Data dan maklumat dalam rangkaian komputer Universiti, atau dalam apa-apa media storan digital milik Universiti, boleh dikongsi antara sesama staf, sesama pelajar, sesama staf dan pelajar atau dengan pihak ketiga yang lain tertakluk kepada Arahan Keselamatan dan apa-apa peruntukan kerahsiaan maklumat lain yang berkuatkuasa dari semasa ke semasa di Universiti, dan tertakluk selanjutnya kepada—

(a) prinsip perlu mengetahui iaitu perkongsian tersebut dihadkan kepada staf, pelajar atau pihak ketiga tertentu yang fungsi atau peranan staf, pelajar atau pihak ketiga itu memerlukannya mendapatkan data dan maklumat tersebut dan hak untuk mengakses data dan maklumat itu diberikan pada tahap minimum iaitu akses untuk membaca atau melihat sahaja;

(b) seseorang staf, pelajar atau pihak ketiga yang diberikan akses kepada data dan maklumat itu hendaklah bertanggungjawab mengenai kerahsiaan data dan maklumat itu termasuklah tidak mendedahkan data dan maklumat itu kepada pihak yang tidak dibenarkan;

(c) staf, pelajar atau pihak ketiga itu bersetuju menandatangani apa-apa instrumen kerahsiaan yang disediakan oleh Universiti sebelum data dan maklumat Universiti itu dikongsikan.

Membuat Pernyataan Awam Menggunakan Media Sosial

17.(1) Staf atau pelajar dilarang membuat pernyataan awam dengan menggunakan media sosial yang boleh memudaratkan, memalukan, atau memburukkan nama baik dan reputasi Universiti atau staf atau pelajar lain.

(2) Mana-mana staf atau pelajar yang melanggar peruntukan ini adalah melakukan suatu perbuatan pelanggaran tatatertib dan boleh diambil tindakan mengikut prosedur tatatertib yang berkenaan dengan staf atau pelajar itu.

Mel Elektronik

18.(1) Universiti hendaklah menyediakan kemudahan mel elektronik bagi stafnya dan pelajarnya.

(2) Staf dan pelajar yang mendapat kemudahan mel elektronik Universiti hendaklah mematuhi apa-apa garis panduan, arahan kerja atau tatacara bagi penggunaan mel elektronik Universiti itu yang dibuat oleh Jawatankuasa Teknologi Maklumat dan Komunikasi Universiti atau ketua yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti.

(3) Staf dan pelajar yang mendapat kemudahan mel elektronik Universiti hendaklah menggunakan kemudahan mel elektronik tersebut dengan bertanggungjawab dan akan bertanggungan secara bersendirian terhadap apa-apa liabiliti atau gantirugi yang disebabkan oleh penggunaan secara salah mel elektronik Universiti itu dan hendaklah pada sepanjang masa menggantirugikan Universiti terhadap apa-apa kerugian yang ditanggung oleh Universiti yang berbangkit daripada penggunaan secara salah mel elektronik itu.

(4) Mana-mana staf atau pelajar yang tidak mematuhi apa-apa garis panduan, arahan kerja atau tatacara bagi penggunaan mel elektronik Universiti itu yang dibuat oleh Jawatankuasa Teknologi Maklumat dan Komunikasi Universiti atau ketua yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti adalah melakukan suatu perbuatan pelanggaran tatatertib dan boleh diambil tindakan mengikut prosedur tatatertib yang berkenaan dengan staf atau pelajar itu.

Transaksi dalam Talian

19.(1) Ketua yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti hendaklah memastikan keselamatan keseluruhan rangkaian komputer Universiti agar transaksi dalam talian yang melibatkan Universiti dapat dijalankan dengan selamat.

(2) Ketua bagi sesuatu pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab untuk mengendalikan apa-apa transaksi dalam talian yang melibatkan Universiti hendaklah mematuhi apa-apa garis panduan, arahan kerja atau tatacara bagi penggunaan transaksi dalam talian Universiti yang dibuat oleh Jawatankuasa Teknologi Maklumat dan Komunikasi Universiti dan Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi Universiti atau ketua yang dipertanggungkan dengan hal ehwal tanggungjawab teknologi maklumat dan komunikasi Universiti.

(3) Ketua bagi sesuatu pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab untuk mengendalikan apa-apa transaksi dalam talian yang melibatkan Universiti hendaklah memastikan bahawa transaksi dalam talian yang melibatkan Universiti dapat dilakukan dengan selamat dan semua data dan maklumat yang diperoleh daripada staf, pelajar atau orang awam dilindungi mengikut apa-apa peruntukan undang-undang yang berkaitan dengan perlindungan atau kerahsiaan data dan maklumat itu.

(4) Ketua bagi sesuatu pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab untuk mengendalikan apa-apa transaksi dalam talian yang melibatkan Universiti hendaklah memastikan data dan maklumat dalam talian yang diperoleh oleh Universiti dikemaskini dari semasa ke semasa.

Bahagian G – Kawalan Keselamatan Teknologi Maklumat dan Komunikasi

Keselamatan Sistem Teknologi Maklumat dan Komunikasi

20.(1) Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti hendaklah memastikan keselamatan keseluruhan sistem teknologi maklumat dan komunikasi Universiti merangkumi peralatan, perkakasan, data, media storan, peralatan rangkaian komputer, capaian rangkaian komputer, perisian dan aplikasi, pangkalan data dan dokumentasi, dan kawasan fizikal aset teknologi maklumat dan komunikasi.

(2) Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti boleh dari semasa ke semasa mengeluarkan apa-apa arahan berkaitan dengan keselamatan bagi sistem teknologi maklumat dan komunikasi.

(3) Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti, atas pertimbangan memelihara keselamatan sistem teknologi maklumat dan komunikasi Universiti, boleh memantau, menapis, menghalang, atau menghentikan sebarang aktiviti dalam rangkaian komputer Universiti.

Kawalan Kriptografi

21. Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti hendaklah mengadakan kawalan terhadap sistem teknologi maklumat dan komunikasi Universiti dengan cara mengadakan sama ada satu atau lebih kawalan kriptografi berikut:—

(a) menggunakan kaedah enkripsi bagi data dan maklumat yang sensitif dan terperingkat, yang melalui rangkaian komputer Universiti seperti data dan maklumat dalam sistem kewangan atau pangkalan data pelajar atau staf;

(b) menentusahkan pengiriman transaksi secara elektronik antara staf atau pelajar dengan Universiti atau antara Universiti dengan pihak ketiga atau apa-apa perhubungan elektronik oleh Universiti dengan mana-mana pihak melalui tandatangan digital mengikut Akta Tandatangan Digital 1997 (Akta 562); atau

(c) menggunakan kaedah pengurusan infrastruktur kunci awam bagi mengenalpasti identiti sijil digital yang mengikat individu seperti yang diberikan oleh Pihak Berkuasa Pendaftaran yang tidak boleh diubah, dimusnah atau didedahkan sepanjang tempoh sahnya.

Kawalan Sistem Fail

22.(1) Ketua bagi sesuatu pusat tanggungjawab hendaklah mengadakan dan mentadbir suatu sistem kawalan fail dan storan data elektronik yang boleh dicapai dalam talian rangkaian komputer Universiti tertakluk kepada kawalan kriptografi dalam Kaedah 21, Kaedah-Kaedah ini.

(2) Penyelenggaraan bagi sistem kawalan fail dan storan data elektronik hendaklah dibuat dari semasa ke semasa dengan mematuhi Kaedah 15 dan 16 Kaedah-Kaedah ini.

Proses Pembangunan Perisian atau Aplikasi

23.(1) Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti hendaklah memastikan keselamatan keseluruhan sistem teknologi maklumat dan komunikasi Universiti semasa membangunkan apa-apa perisian atau aplikasi yang akan digunakan oleh Universiti dan boleh membuat keputusan sama ada membangunkan perisian atau aplikasi itu secara dalaman atau membangunkan perisian atau aplikasi itu dengan menggunakan khidmat pihak ketiga lain.

(2) Sekiranya perisian atau aplikasi itu dibangunkan secara dalaman, perkara berikut hendaklah diberikan perhatian oleh Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti:—

(a) kemahiran dan kepakaran staf teknologi maklumat dan komunikasi membangunkan sesuatu perisian atau aplikasi;

(b) perisian dan aplikasi disesuaikan mengikut dan memenuhi keperluan khusus Universiti dan pusat tanggungjawab;

(c) perisian dan aplikasi mudah disesuaikan jika terdapat keperluan penukaran yang kerap;

(d) tempoh pembangunan perisian dan aplikasi; dan

(e) kos pembangunan sesuatu perisian atau aplikasi.

(3) Sekiranya perisian atau aplikasi itu dibangunkan dengan menggunakan khidmat pihak ketiga, perkara berikut hendaklah diberikan perhatian oleh Ketua bagi pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti:—

(a) ketiadaan kemahiran dan kepakaran staf teknologi maklumat dan komunikasi membangunkan sesuatu perisian atau aplikasi;

(b) kos dan sumber manusia bagi pembangunan sesuatu perisian atau aplikasi lebih rendah daripada dibangunkan secara dalaman;

(c) perisian dan aplikasi boleh disesuaikan mengikut dan memenuhi keperluan khusus Universiti dan pusat tanggungjawab;

(d) perisian dan aplikasi mudah disesuaikan jika terdapat keperluan penukaran yang kerap tanpa koordinasi kerap daripada pihak ketiga lain;

(e) kod sumber dan hak cipta bagi apa-apa perisian dan aplikasi yang dibangunkan khusus untuk Universiti hendaklah menjadi kepunyaan Universiti; dan

(f) proses pembangunan perisian dan aplikasi itu perlu diselia dan dipantau secara berterusan oleh pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti.

Bahagian H – Pengurusan Insiden Keselamatan Teknologi Maklumat dan Komunikasi

Melaporkan Insiden Keselamatan Teknologi Maklumat dan Komunikasi

24. Semua staf dan pelajar hendaklah bertanggungjawab membuat laporan berkaitan insiden keselamatan kepada Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi Universiti apabila staf atau pelajar itu mengetahui berlakunya insiden keselamatan teknologi maklumat dan komunikasi.

Huraian

Insiden keselamatan teknologi maklumat dan komunikasi termasuklah pencerobohan, ancaman, melumpuhkan sistem dan akses yang tidak dibenarkan terhadap perkhidmatan teknologi maklumat dan komunikasi Universiti.

Misalan-Misalan

(a) A, seorang staf Universiti menggunakan aset teknologi maklumat dan komunikasi bagi membocorkan maklumat mengenai keputusan pelantikan perjawatan sebelum keputusan tersebut diumumkan oleh Pendaftar. A melanggar Dasar Teknologi Maklumat dan Komunikasi.

(b) *A, seorang pelajar Universiti mencapai modul pemarkahan sistem maklumat pelajar tanpa kebenaran Universiti dan melakukan pindaan data. Perbuatan A itu merupakan satu perbuatan pencerobohan terhadap perkhidmatan teknologi maklumat dan komunikasi Universiti.*

(c) *A, seorang staf Universiti menggunakan perisian penghalang perkhidmatan kepada sistem sumber manusia sehingga menyebabkan sistem itu tidak boleh diakses oleh semua staf. Perbuatan A itu merupakan satu perbuatan penghalangan penyampaian perkhidmatan terhadap staf Universiti dan ancaman.*

(d) *A, seorang staf Universiti yang diberikan kebenaran menggunakan aset teknologi komunikasi dan maklumat telah mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan Universiti. Perbuatan A itu merupakan satu perbuatan sabotaj terhadap perkhidmatan teknologi maklumat dan komunikasi Universiti.*

(e) *A, seorang staf Universiti memalsukan maklumat gajinya yang diperoleh daripada sistem gaji Pejabat Bendahari bagi membuat pinjaman peribadi dari institusi kewangan. Perbuatan A itu merupakan satu pemalsuan maklumat Universiti.*

(f) *A, seorang staf Universiti menghantar mel elektronik menggunakan aset teknologi komunikasi dan maklumat Universiti mengenai jualan langsung yang dikendalikannya kepada sebilangan alamat mel elektronik individu lain dalam satu masa dan secara berulang-kali melakukannya dan mungkin menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan. Perbuatan A itu merupakan satu perbuatan spam terhadap kemudahan mel elektronik Universiti.*

(g) *A, seorang staf Universiti memasukkan perisian virus ke dalam sistem teknologi maklumat dan komunikasi Universiti dan menyebabkan serangan virus kepada sistem itu. Perbuatan A itu merupakan satu perbuatan meletakkan kod berbahaya terhadap sistem teknologi maklumat dan komunikasi Universiti.*

(h) *A, seorang staf Universiti menghantar mel elektronik yang mengandungi unsur gangguan atau ancaman peribadi terhadap B. Perbuatan A itu merupakan satu perbuatan gangguan atau ancaman terhadap B.*

(i) *A, seorang staf Universiti mencuri suis rangkaian komputer yang menghubungkan pusat tanggungjawab X ke pusat tanggungjawab Y. Perbuatan A itu merupakan satu perbuatan melumpuhkan sistem rangkaian komputer Universiti.*

Tindakan Atas Laporan

25.(1) Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi Universiti hendaklah mengambil tindakan yang sewajarnya mengenai laporan yang dikemukakan oleh mana-mana orang terhadap insiden keselamatan sistem teknologi maklumat dan komunikasi universiti dan sekiranya perlu, membuat apa-apa cadangan kepada Jawatankuasa Pengurusan Universiti bagi mengelakkan insiden yang sama berulang.

(2) Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi Universiti hendaklah menyedia dan menyenggara suatu daftar mengenai insiden keselamatan sistem teknologi maklumat dan komunikasi universiti yang dilaporkan kepadanya dan hendaklah dari semasa ke semasa melaporkankepada Jawatankuasa Pengurusan Universiti mengenai daftar tersebut.

Bahagian I - Am

Pengecualian

26. Naib Canselor boleh memberikan pengecualian kepada mana-mana staf atau pelajar daripada mematuhi mana-mana peruntukan Kaedah-kaedah ini atau garis panduan, arahan kerja atau tatacara yang ditetapkan oleh Jawatankuasa Teknologi Maklumat dan Komunikasi Universiti atau Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi Universiti atas sebab kepentingan keselamatan negara.

Dengan syarat pengecualian itu tidak boleh menyentuh mana-mana undang-undang lain yang berkuatkuasa dari semasa ke semasa atau mana-mana obligasi dan terma yang terkandung dalam kontrak antara Universiti dengan pihak ketiga lain.

Menanggung Rugi Universiti

27. Mana-mana staf atau pelajar Universiti yang gagal mematuhi peruntukan Kaedah-kaedah ini dan menyebabkan kerugian kepada Universiti, hendaklah menanggung rugi, mengganti bayar dan melepaskan Universiti daripada semua tuntutan, tindakan, kerugian, perbelanjaan, kos guaman, ganti rugi serta tanggungan yang diambil atau dituntut terhadap atau ditanggung oleh Universiti berkaitan atau disebabkan oleh kecuaian, ketinggalan, pengabaian atau tindakan staf atau pelajar yang gagal mematuhi Kaedah-kaedah ini.

Penasihatan Umum dan Bantuan

28. Pusat tanggungjawab yang dipertanggungkan dengan tanggungjawab hal ehwal teknologi maklumat dan komunikasi Universiti boleh dihubungi untuk mendapatkan nasihat dan bantuan mengenai persoalan yang timbul di bawah atau berkaitan Kaedah-kaedah ini.

Tafsiran Am

29. Kaedah-Kaedah ini hendaklah dibaca dan ditafsirkan bersama Kaedah-Kaedah lain Universiti yang berkuatkuasa dari semasa ke semasa.

Dibuat 10 Disember 2013

[Minit Mesyuarat LPU 99/04]

[UPM/PPUU/100/1/1/3/ICT ; UPM:IDEC/100/1/5/KAEDAH-KAEDAH UNIVERSITI PUTRA MALAYSIA (TEKNOLOGI MAKLUMAT & KOMUNIKASI) 2014]

PROF. EMERITUS TAN SRI DATO' DR. SYED JALALUDIN SYED SALIM

Pengerusi

Lembaga Pengarah

Universiti Putra Malaysia