Kaedah-Kaedah Universiti Putra Malaysia
(Teknologi Maklumat Dan Komunikasi) 2013

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) 2013 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 2013
[Minit Mesyuarat LPU]
[UPM/PPUU/100/1/1/3/ICT UPM/IDEC]

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

Pengerusi Lembaga Pengarah
Universiti Putra Malaysia

Universiti Putra Malaysia
(Information and Communication Technology) Rules 2013

A Rules to provide for matters relating to information and communication technology in Universiti Putra Malaysia including security and management of information and communication technology and for other matters incidental thereto.

[Date in force]

In exercise of the power conferred by subsection 37(1) of the Constitution of the Universiti Putra Malaysia, the Board of Director makes the following Rules:-

Part A - Preliminary

Name and Application

1. These Rules maybe cited as the Universiti Putra Malaysia (Information and Communication Technology) Rules 2013 and shall come into force on 1st January 2014.

Interpretation

2. In these Rules, unless the context otherwise required−

"Assets of information and communication technology" includes hardwares, softwares, applications, documentations related to information and communication technology which are under the responsibility of the University;

"Data and Information" means facts or collection of facts whether in the form of paper or electronic which contained information which are stored or used by the University including all documentation, operational standard, records of the University, records of customers, staff or students;

"Students" means student of the University in accordance with the interpretation of Universities and University Colleges Act 1971;

"Staff" means employees of the University in accordance with the interpretation of the Constitution of the University.

Part B - Information and Communication Technology Policy

Requirement to Formulate Policy

3. The Board of Director of the University shall formulate a University policy on information and communication technology in Universiti Putra Malaysia including security and management of information and communication technologi and for other matters incidental hereto.

Policy Implementation and Amendment

4.(1) Policy on information and communication technology of the University formulated by the Board of Director shall be implemented by the University and shall be supervised by cost centre charged with the responsibilty of the University information technology affairs.

(2) Policy on information and communication technology of the University may be amended and made anew from time to time by the Board of Director of the University.

Part C - Establishment of Committees

Establishment of the University Committee on Information and Communication Technology

5.(1) The University Committee on Information and Communication Technology shall consists of:−

(a) Deputy Vice Chancellor charged with the responsibilty of information and communication technology as determined by the Vice Chancellor, who shall be the Chairman;

(b) Head of the cost centre charged with the responsibility of the information and communication technology affairs of the University, who shall be the Secretary;

(c) Registrar or his representative;

(d) Bursar or his representative;

(e) Chief Librarian or his representative;

(f) Dean of Faculty of Computer Science and Information Technology;

(g) Dean of Faculty of Engineering or his representative who has the expertise on information and communication technology;

(h) Head for the office charged with the responsibilty of the website of the University;

(i) Any other staff or students of the University appointed by the Vice Chancellor.

(2) Deputy Head of the cost centre charged with the responsibility of information and communication technology affairs shall be ex-officio member of the Committee but shall not have the rights to vote.

(3) Committee of the Information and Communication Technology shall have the following powers:−

(a) to recommend University Policy on Information and Communication Technology to the University Management Committee and Board of Director;

(b) make guidelines, work instructions or procedures for specific application on information and communication technology within University in accordance with the requirements of the University Policy on Information and Communication Technology and these Rules;

(c) to monitor the compliance of University Policy on Information and Communication Technology and these Rules by staff and students of the University; and

(d) evaluate the latest and suitable information and communication technology for the University and make recommendation in accordance with the proper needs for its usage to the University Management Committee;

Establishment of the Committee on Security of Information and Communication Technology

6.(1) Committee on Security of Information and Communication Technology shall consists of:−

(a) Head of the cost centre charged with the responsibility of the security affairs on information and communication technology, who shall be the Chairman;

(b) Deputy Head for the office charged with the responsibility of information and communication technology affairs;

(c) Head for the cost centre charged with the responsibility of University security;

(d) Head for the cost centre charged with the responsibility of University development and asset management;

(e) Head for the cost centre charged with the responsibility of University safety and occupational health;

(f) Head of Unit charged with the responsibility of security of University information and communication technology who shall be the Secretary;

(g) Any other staff of the University appointed by the Chairman.

(2) Heads of Unit of the cost centre charged with the responsibility of information and communication technology affairs shall be ex-officio member of the Committee but shall not have the right to vote.

(3) Committee on Security of Information and Communication Technology shall have the following powers:−

(a) make guidelines, work instructions or procedures for security on information and communication technology within University in accordance with the requirements of the University Policy on Information and Communication Technology and these Rules;

(b) enforcing the University guidelines, work instructions or procedures for security on information and communication technology;

(c) to receive reports on information and communication technology security including on any incidents of information and communication technology

within the University, and to take appropriate and expedient action pertaining to the reports;

(d) make any recommendation to the University Management Committee to prevent of security incidents of information and communication technology from occurring;

(e) evaluate the suitable information and communication technology and recommend solutions towards the need of information and communication technology; and

(f) establishing information and communication technology security incident handler team and determining the terms of reference for the information and communication technology security incident handler team.

Secretariat

7. The Centre charged with the responsibility of the information and communication technology affairs of the University shall be the Secretariat for the Committee of the Information and Communication Technology and Committee on Security of Information and Communication Technology.

Part D - Management of Information and Communication Technology Assets

Identification of Management of Information and Communication Technology Assets

8.(1) Head of a cost centre in the University shall identify and record all information and communication technology assets existing in his cost centre in the manner prescribed by the Committee of the Information and Communication Technology and Committee on Security of Information and Communication Technology.

(2) If there is any additional or disposal of the assets of information and communication technology at the cost centre, the Head of that cost centre shall update the additional or disposal information.

Security Control of Assets and Vicinity

9. Head of a cost centre in the University shall protect assets of information and communication technology, and the vicinity of that assets, from trespass, threat, damage and unauthorised access, and shall:−

(a) identify assets of information and communication technology which are available at his cost centre and ensure the security of that assets by establishing control of the accessibility of that assets; and

(b) identify the physical security vicinity of the information and communication technology and employ security parameter including setting up barriers such as walls, closed circuit camera, security fence, security guards, security door, biometric access control, smart card and authorised access only to secure the vicinity which contain information and information processing facilities.

Maintenance of Information and Communication Technology Assets

10. Head of a cost centre in the University shall ensure:-

(a) maintenance for an information and communication technology assets is made from time to time according to:

(i) specification set by the manufacturer of that information and communication technology assets; or

(ii) guidelines, work instructions or procedures as determined by the University Committee of the Information and Communication Technology and Committee on Security of Information and Communication Technology.

(b) information and communication technology assets are maintained by qualified staff or third party and granted access to the assets by Head of the cost centre;

(c) periodic maintenance for information and communication technology assets is implemented according to schedule which is prescribed from time to time; and

(d) maintenance made on the information and communication technology assets are perform within the knowledge of the information and communication technology officer charged with the responsibility of information and communication technology in the cost centre.

Computer Network Infrastructure

11.(1) University shall develop computer network infrastructure for the use of the University main campus and University branch campus.

(2) Head of a cost centre in the University shall identify and record computer network infrastructure existing in his cost centre in the manner prescribed by the Committee of the Information and Communication Technology and Committee on Security of Information and Communication Technology.

(3) Head of a cost centre in the University shall take security measures to prevent trespass or damage to computer network infrastructure as recommenden or directed by the Head charged with the responsibility for the University information and

communication technology affairs or by the Committee on Security of Information and Communication Technology.

(4) If there is any additional or disposal of the computer network infrastructure, the Head of that cost centre shall update the additional or disposal information.

(5) The Head charged with the responsibility for the University information and communication technology affairs shall install anti-threat and anti-trespass system on the computer network infrastructure to prevent trespassing activities to the University computer network system and internet access.

Part E - Software Management

Copyright Protection and Licensing

12.(1) Staff or students shall only use softwares or applications which are legally licensed from the owner of that softwares or applications.

(2) Any staff or students which use softwares or applications of electronic media or otherwise which are copyrighted without valid licence shall be responsible personally against any liability or damages claimed by the owner of the softwares or applications and shall at all times indemnify the University from any loss suffered by the University pursuant to the claim by the copyright owner of the softwares or applications or elctronic media or otherwise, to the University.

Protection from Malicious Softwares

13.(1) Staff at a cost centre shall refrain himself from downloading or uploading or installing any malicious softwares, or as advised by the Head of the cost centre charged with the responsibility of the information and communication technology affairs for University or by the information and communication technology officer charged with the

responsibility of information and communication technology at the cost centre as malicious, into the information and communication technology hardwares.

(2) Students at a cost centre shall refrain himself from downloading or uploading or installing any malicious softwares, or as advised by the Head of the cost centre charged with the responsibility of the information and communication technology affairs for University or by the information and communication technology officer charged with the responsibility of information and communication technology at the cost centre as malicious, into the information and communication technology hardwares.

(3) Any staff or students who breach this provision commits an act of discplinary offence and shall be liable to discplinary action according to the discplinary procedures relating to the staff or students.

Part F - Management of Data and Information

Responsibility to Manage and Control Data and Information

14.(1) Staff and students who have been granted access and authorised to use the University information and communication technology assets shall be responsible to protect the data and information therein and ensure the data and information which was stored in the information and communication technology asset storage, may be utilised again.

(2) Any staff or students who breach this provision commits an act of discplinary offence and shall be liable to discplinary action according to the discplinary procedures relating to the staff or students.

Maintenance of Data and Information

15. Head of a cost centre in the Universiy shall ensure−

(a) data and information, which are stored in the storage using the University information and communication technology assets, are maintained from time to time according to specification prescribed by guidelines, work instructions, procedures determined by the Committee of the Information and Communication Technology and Committee on Security of Information and Communication Technology;

(b) periodic maintenance for data and information is implemented according to schedule which is prescribed from time to time;

(c) maintenance of data and information shall be made by qualified staff or third party granted access to the data and information by the Head of the cost centre;

(d) maintenance of data and information is made within the knowledge of the information and communication technology officer charged with the responsibility of information and communication technology in the cost centre.

Sharing of data and information

16. Data and information in the University computer network, or in any digital storage media owned by the University, may be shared among staff, among students, among staff and students or with other third party subject to Security Instruction and any other confidential information provision in force from time to time in the University, and further subject to−

(a) need to know principle which is the sharing is restricted to staff, students or certain third parties whose functions or roles require them to obtain the data and information and rights to access the data or information is granted at the minimum level which is access only to read or sight;

(b) a staff, student or third party who has been granted access to the data or information shall be responsible in respect of confidentiality of the data and information including not disclosing the data and information to unauthorised parties;

(c) the staff, students or third parties agree to execute any confidentiality instrument provided by the University before the data and information is shared.

Making Public Statement Using Social Media

17.(1) Staff or students are prohibited from making public statement using social media which may be detrimental, embarrassing or disreputing good name and reputation of the University or other staff or students.

(2) Any staff or students who breach this provision commits an act of discplinary offence and shall be liable to discplinary action according to the discplinary procedures relating to the staff or students.

Electronic Mail

18.(1) University shall provide electronic mail facilities for its staff and students.

(2) Staff and students having the University electronic mail facilities shall comply with any guidelines, work instructions or procedures for the usage of the University electronic mail as determined by the Committee of the Information and Communication Technology or Head charged with the responsibility of the information and communication technology affairs .

(3) Staff and students having the University electronic mail facilities shall utilise the electronic mail facilities responsibly and shall be liable personally against any liability or damages caused by wrong usage of the University electronic mail and shall at all times

indemnify University from any loss suffered by the University pursuant to the wrong usage of the electronic mail.

(4) any staff or students not complying with the guidelines, work instructions, or procedures for the usage of the University electonic mail determined by the University Committee of Information and Communication Technology or Head charged with the responsibility of the information and communication technology affairs commit an act of discplinary offence and shall be liable to discplinary action according to the discplinary procedures relating to the staff or students.

Online Transaction

19.(1) The Head charged with the responsibility of the information and communication technology affairs shall ensure the security of the overall University computer network so that online transactions involving the University are abled to be carried out safely.

(2) The Head of the cost centre charged with the responsibility of handling any online transactions involving the University shall comply with any guidelines, work instructions or procedures for the usage of University online transaction determined by University Committee of Information and Communication Technology and Committee on Security of Information and Communication Technology or Head charged with the responsibility of the information and communication technology affairs.

(3) The Head of the cost centre charged with the responsibility of handling any online transactions involving the University shall ensure that all online transactions involving the University are abled to be carried out safely and all data and information procured from staff, students or public are protected in accordance with any legal provisions relating to protection or confidentiality of the data and information.

(4) The Head of the cost centre charged with the responsibility of handling any online transactions involving the University shall ensure online data and information procured by the University is updated from time to time.

Part G - Security Control of Information and Communication Technology

Security of Information and Communication Technology System

20.(1) Head of the cost centre charged with the responsibility of the University on information and communication technology affairs shall ensure the overall security of the University information and communication technology system encompasing equipments, hardwares, data, storage media, computer networking equipments, computer network access, softwares and applications, database and documentations, and physical vicinity of information and communication technology assets.

(2) Head of the cost centre charged with the responsibility of the University information and communication technology affairs may from time to time issue any direction relating to security for information and communication technology system.

(3) Head of the cost centre charged with the responsibility of the University on information and communication technology affairs, on the consideration to safeguard the security of the University information and communication technology system, may monitor, filter, prevent, or discontinue any activities within the University computer network.

Cryptography Control

21. Head of the cost centre charged with the responsibility of the University on information and communication technology affairs shall set up control on the University information and communication technology system by way of establishing one or more of the following cryptographic control:−

(a) using encryption method for classified and sensitive data and information which pass through the University computer network such as data and information in the financial system or students or staff database;

(b) verifying electronic transaction transmission between staff or students with the University or between the University with third party or any other electronic communication by the University with any parties through digital signature according to Digital Signature Act 1997 (Act 562); or

(c) using public key infrastructure management method for identifying identity of digital certificate which binds individuals as assigned by Registration Authorities which cannot be altered, destroyed or disclosed throughout the period of its validity.

Control of File System

22.(1) Head of a cost centre shall establish and administer a system to control file and electronic data storage which can be accessed online through the University computer network subject to cryptography control in Rule 21, of these Rules.

(2) Maintenance for the system to control file and electronic data storage shall be made from time to time by complying Rule 15 and 16 of these Rules.

Softwares or Applications Development Processes

23.(1) Head of the cost centre charged with the responsibility of the University on information and communication technology affairs shall ensure the overall security of the University information and communication technology system while developing any softwares or applications which will be used by the University and may make decision whether to develop the softwares or applications in house or to develop the softwares and applications by using other third parties services.

(2) If the softwares or applications are developed in house, the following items shall be given consideration by Head of the cost centre charged with the responsibility of the University on information and communication technology affairs:−

(a) skills and expertise of information and communication technology staff in developing a software or application;

(b) the software and application customised in accordance to and fulfill specific requirements of the University and cost centre;

(c) the software and application is easily adaptable if there is requirement for frequent changes;

(d) period of development of the software and application; and

(e) development cost for a software or application.

(3) If the softwares or applications are developed using third parties services, the following items shall be given consideration by Head of the cost centre charged with the responsibility of the University on information and communication technology affairs:−

(a) lack of skills and expertise of information and communication technology staff in developing a software or application;

(b) cost and human resource for the development of a software or application is lower than being developed in house;

(c) the software and application can be customised in accordance with, and fulfill specific requirements of the University and cost centre;

(d) the software and application is easily adaptable if there is requirement for frequent changes without regular coordination from other third parties;

(e) source code and copyright for any software and application developed specifically for the University shall belong to the University; and

(f) development processes of software and application shall be supervised and monitored continuously by the cost centre charged with the responsibility of the University on information and communication technology affairs.

Part H - Management of Security Incidents of Information and Communication Technology

Reporting Security Incidents of Information and Communication Technology

24. All staff and students shall be responsible to make report on security incident to Committee on Security of Information and Communication Technology when the staff or students discover the occurance of security incidents of information and communication technology.

Explanation

Security incidents of information and communication technology includes trespass, threat, crippling the system and unauthorised access to the University information and communication technology services.

Illustrations

(a) A, a University staff used information and communication technology to leak information about decision of the personnel appointment before the decision is announced by the Registrar. A breaches the Information and Communication Technology Policy.

(b) A, a University student accessed the scoring module of students information system without authorisation of the University and make data changes. The act of A amounts to an act of trespassing against University information and communication technology services.

(c) A, a University staff used denial of service software to the human resource system rendering the system inaccessible by all staff. The act of A amounts to an act of denial of service to the University staff and a threat.

(d) A, a University staff having granted authorisation to use information and communication technology asset has modified features of the equipments, softwares or any components of a system without knowledge, direction or consent of the University. The act of A amounts to an act of sabotage to the University information and communication technology service.

(e) A, a University staff falsified his salary information obtained from the Bursar payroll system for applying personal loan from financial institutions. The act of A amounts to falsification of University information.

(f) A, a University staff sent electronic mail using University information and communication technology asset about direct selling operated by him to a number of other individual electronic mails at a time and repeatedly doing so, and may cause network congestion and slow down the response. The act of A amounts to an act of spamming to the University electronic mail facilities.

(g) A, a University staff downloaded virus software in the University information and communication technology system and causing virus attack on the system. The act of A amounts to an act of putting malicious code to the University information and communication technology system.

(h) A, a University staff sent electronic mail which contained elements of harrassment or personal threat towards B. The act of A amounts to harrassment or threat towards B.

(i) *A, a University staff stole computer network switch which connects cost centre X to cost centre Y. The act of A amounts to an act of crippling the system of the University computer network.*

Action Against Report

25.(1) The Committee on Security of Information and Communication Technology of the University shall take necessary action against report submitted by any person on security incidents of information and communication technology of the University and if necessary, to make any recommendatation to the University Management Committee to avoid the occurance of similar incidents.

(2) Committee on Security of Information and Communication Technology of the University shall prepare and maintain a register on security incidents of information and communication technology reported to it and shall from time to time report to the University Management Committee about the register.

Part I - General

Exception

26. Vice Chancellor may grant exception to any staff or students from complying with any provision of these Rules or guidelines, work instructions or procedures determined by the Committee of the Information and Communication Technology and Committee on Security of Information and Communication Technology on reasons of the interest of national security.

Provided that such exemption shall not affect any other laws in force from time to time or any obligations and terms contained in the contract between the University and other third parties.

Indemnifying the University

27. Any staff or students who fail to comply with the provisions of these Rules and cause losses to the University, shall indemnify, refund and release the University from any claims, actions, losses, expenses, legal cost, damages and liabilities which is taken or claimed against or incurred by the University related or caused by negligence, omission, neglects or actions of staff or students who fail to comply with these Rules.

General Advise and Assistance

28. The cost centre charged with the responsibility of the University information and communication technology affairs may be contacted for advise and assistance on questions arising pursuant or related to these Rules.

General Interpretation

29. These Rules shall be read and interpreted together with other Rules of the University which is in force from time to time.

Made 2013
[BOD Minutes of Meeting]
[UPM/PPUU/100/1/1/3/ICT;UPM/IDEC]

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

Chairperson, Board of Directors

Universiti Putra Malaysia

Nota Penjelasan kepada Draf Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2013

Kaedah 1
Kaedah ini bertujuan untuk menamakan Kaedah-Kaedah ini sebagai Kaedah-Kaedah Universiti Putra Malaysia (Teknologi Maklumat dan Komunikasi) 2013.

Kaedah 2
Kaedah ini bertujuan untuk mengadakan peruntukan mengenai tafsiran kepada beberapa perkataan khusus yang digunakan dalam Kaedah-Kaedah ini.

Kaedah 3
Kaedah ini bertujuan untuk mengadakan peruntukan bagi Universiti membuat dasar berkaitan teknologi maklumat dan komunikasi.

Kaedah 4
Kaedah ini bertujuan untuk mengadakan peruntukan bagi pelaksanaan dan pindaan dasar berkaitan teknologi maklumat dan komunikasi.

Kaedah 5
Kaedah ini bertujuan untuk mengadakan peruntukan bagi menubuhkan Jawatankuasa Teknologi Maklumat dan Komunikasi Universiti dan menyenaraikan bidangkuasa Jawatankuasa itu.

Kaedah 6
Kaedah ini bertujuan untuk mengadakan peruntukan bagi menubuhkan Jawatankuasa Keselamatan Teknologi Maklumat dan Komunikasi Universiti dan menyenaraikan bidangkuasa Jawatankuasa itu.

Kaedah 7
Kaedah ini bertujuan untuk mengadakan peruntukan bagi mewujudkan urus setia kepada kedua-dua Jawatankuasa yang ditubuhkan dalam Kaedah 5 dan Kaedah 6.

Kaedah 8
Kaedah ini bertujuan untuk mengadakan peruntukan bagi pengenalpastian dan perekodan aset teknologi maklumat dan komunikasi Universiti.

Kaedah 9
Kaedah ini bertujuan untuk mengadakan peruntukan bagi mengawal dan melindungi keselamatan aset teknologi maklumat dan komunikasi dan kawasan persekitaran aset itu.

Kaedah 10
Kaedah ini bertujuan untuk mengadakan peruntukan bagi penyelenggaraan aset teknologi maklumat dan komunikasi.

Kaedah 11
Kaedah ini bertujuan untuk mengadakan peruntukan bagi pembangunan infrastruktur rangkaian komputer Universiti.

Kaedah 12
Kaedah ini bertujuan untuk mengadakan peruntukan bagi perlindungan hak cipta dan keperluan mendapatkan lesen bagi menggunakan perisian dan aplikasi pihak ketiga.

Kaedah 13
Kaedah ini bertujuan untuk mengadakan peruntukan bagi perlindungan daripada perisian berbahaya.

Kaedah 14
Kaedah ini bertujuan untuk mengadakan peruntukan bagi tanggungjawab mengurus dan mengawal data dan maklumat Universiti ke atas pelajar dan staf.

Kaedah 15
Kaedah ini bertujuan untuk mengadakan peruntukan bagi penyelenggaran data dan maklumat di Universiti.

Kaedah 16
Kaedah ini bertujuan untuk mengadakan peruntukan bagi perkongsian data dan maklumat di Universiti adalah tertakluk kepada Arahan Keselamatan dan peruntukan kerahsiaan.

Kaedah 17
Kaedah ini bertujuan untuk mengadakan peruntukan bagi melarang pelajar atau staf membuat pernyataan awam menggunakan media sosial.

Kaedah 18
Kaedah ini bertujuan untuk mengadakan peruntukan bagi penyediaan kemudahan mel elektronik dan kebertanggungjawaban penggunaannya.

Kaedah 19
Kaedah ini bertujuan untuk mengadakan peruntukan bagi transaksi dalam talian yang dilakukan dalam Universiti dapat dijalankan dengan selamat.

Kaedah 20
Kaedah ini bertujuan untuk mengadakan peruntukan bagi keselamatan sistem teknologi maklumat dan komunikasi.

Kaedah 21
Kaedah ini bertujuan untuk mengadakan peruntukan bagi penggunaan kawalan kriptografi.

Kaedah 22
Kaedah ini bertujuan untuk mengadakan peruntukan bagi kawalan sistem fail.

Kaedah 23
Kaedah ini bertujuan untuk mengadakan peruntukan bagi proses pembangunan perisian atau aplikasi dan membolehkan Universiti memutuskan pembangunan itu dibuat secara dalaman atau oleh pihak ketiga.

Kaedah 24
Kaedah ini bertujuan untuk mengadakan peruntukan bagi melaporkan insiden keselamatan teknologi maklumat dan komunikasi dan memberi contoh insiden keselamatan.

Kaedah 25
Kaedah ini bertujuan untuk mengadakan peruntukan bagi membolehkan tindakan diambil terhadap laporan insiden keselamatan teknologi maklumat dan komunikasi yang dilaporkan.

Kaedah 26
Kaedah ini bertujuan untuk mengadakan peruntukan bagi Naib Canselor memberikan pengecualian pematuhan kepada Kaedah-Kaedah ini atas alasan kepentingan keselamatan negara.

Kaedah 27
Kaedah ini bertujuan untuk mengadakan peruntukan bagi staf atau pelajar Universiti yang tidak mematuhi Kaedah-Kaedah ini menanggung rugi Universiti dan melepaskan Universiti daripada tuntutan dan liabiliti.

Kaedah 28
Kaedah ini bertujuan untuk mengadakan peruntukan bagi penasihatan umum dan bantuan penggunaan Kaedah-Kaedah ini.

Kaedah 29
Kaedah ini bertujuan untuk mengadakan peruntukan bagi penafsiran dan bacaan Kaedah-Kaedah ini bersama Kaedah-Kaedah lain.