POLISI
TEKNOLOGI MAKLUMAT & KOMUNIKASI

TATI UNIVERSITY COLLEGE

VERSI 2.0 (SEPTEMBER 2016)

DISEDIAKAN

OLEH

PUSAT PERKHIDMATAN TEKNOLOGI MAKLUMAT, TATIUC

KANDUNGAN

BAB 1 POLISI UMUM TEKNOLOGI MAKLUMAT & KOMUNIKASI (ICT) 4
1.1 Tujuan 4
1.2 Objektif 4
1.3 Skop 4
1.4 Definisi 4
1.5 Am 6
1.6 Pelanggaran 7
1.7 Teknologi Maklumat Peringkat Kebangsaan 7
BAB 2 POLISI PENGURUSAN ICT 9
2.1 Tujuan 9
2.2 Skop 9
2.3 Pengurusan Organisasi 9
2.4 Pembangunan ICT 9
BAB 3 POLISI PERISIAN, APLIKASI DAN PERKAKASAN ICT 11
3.1 Tujuan 11
3.2 Skop 11
3.3 Polisi Perisian dan Aplikasi 11
3.4 Polisi Perkakasan 12
BAB 4 POLISI RANGKAIAN ICT 16
4.1 Tujuan 16
4.2 Skop 16
4.3 Pelayan Komputer 16
4.4 Rangkaian Kampus 17
4.5 Penggunaan Emel 18
4.6 Penamatan Akaun Emel 20
4.7 Laman Web 20
4.8 Capaian Internet / Intranet 21
BAB 5 POLISI PENGGUNAAN MAKMAL KOMPUTER 23
5.1 Tujuan 23
5.2 Skop 23
5.3 Penggunaan Makmal 23
5.4 Pelanggaran Peraturan 24
BAB 6 POLISI AKAUNTABILITI DAN KERAHSIAAN MAKLUMAT 26

6.1 Tujuan 26
6.2 Skop 26
6.3 Capaian Maklumat Sulit 26
6.4 Pemantauan Data dalam Rangkaian 27
6.5. Pengurusan Maklumat Sulit / Peribadi 27
BAB 7 POLISI KESELAMATAN ICT 29
7.1 Tujuan 29
7.2 Skop 29
7.3 Keselamatan Sistem Komputer Pelayan dan Sistem Aplikasi 29
7.4 Keselamatan Penggunaan Emel 30
7.5 Keselamatan Peralatan Rangkaian 30
7.6 Kebolehcapaian Pengguna (User Accessibility) 32
7.7 Sambungan Dengan Lain-Lain Rangkaian 32
BAB 8 PEMATUHAN KEPADA UNDANG-UNDANG 34
8.1 Pemakaian Peruntukan 34
8.2 Pematuhan Kepada Undang - Undang 34

BAB 1 POLISI UMUM TEKNOLOGI MAKLUMAT & KOMUNIKASI (ICT)

1.1 Tujuan

Menerangkan secara umum polisi penggunaan sumber-sumber ICT di Kolej Universiti TATI (TATIUC) dan diterima pakai sebagai Polisi Umum. Mana-mana polisi terperinci untuk setiap sumber yang disenaraikan adalah mengatasi Polisi Umum ini.

1.2 Objektif

Penggunaan ICT oleh warga TATIUC merupakan suatu instrumen asas yang penting dalam mencapai visi dan misi TATIUC. Ini bertujuan memastikan:

a. Warga TATIUC dimaklumkan mengenai kewujudan dan peranan Pusat Perkhidmatan Teknologi Maklumat (PPTM) dalam pelaksanaan & penguatkuasaan Polisi ICT TATIUC.

b. Kemudahan ICT digunakan secara bijaksana mengikut polisi yang ditetapkan.

c. Tanggungjawab pengguna dimaklumkan.

d. Kerosakan, kemusnahan dan penyalahgunaan ICT dapat diminimumkan.

1.3 Skop

a. Sumber

Sumber yang tersenarai di dalam dokumen, juga sumber yang tidak tersenarai tetapi dianggap sebagai sumber ICT oleh Jawatankuasa Teknologi Maklumat adalah juga tertakluk kepada polisi ini.

b. Pengguna

Semua pengguna adalah tertakluk kepada polisi ini. Pengguna yang melanggar polisi ini adalah dianggap melakukan kesalahan dan boleh dikenakan tindakan yang bersesuaian dengan kesalahan yang dilakukan.

1.4 Definisi

Definisi berikut digunakan dalam Penyataan Polisi yang berkaitan dengan penggunaan kemudahan ICT di TATIUC :

Perkataan	**Definisi**
Aplikasi “Helpdesk”	Aplikasi untuk menghantar sebarang aduan kerosakan & permohonan perkhidmatan kepada PPTM secara atas talian.

Aktiviti / Kegiatan Sulit / Rahsia Pengguna	Arahan yang dilaksanakan (run) atau "keystrokes" yang ditaip semasa pengguna berinteraksi dengan sumber ICT yang disediakan oleh TATIUC
Akaun pengguna	Ruang storan yang telah diperuntukkan kepada setiap pengguna yang sah dalam sesuatu sistem atau sumber ICT. Setiap pengguna dikenalpasti melalui penggunaan identiti pengguna
Aplikasi	Aturcara atau program yang dibangunkan untuk melaksanakan tugas tertentu oleh komputer seperti Sistem Maklumat Kewangan, Sistem Maklumat Kakitangan, Sistem Maklumat Pelajar dan sebagainya
CIO	Ketua Pusat Perkhidmatan Teknologi Maklumat yang bertanggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT di TATIUC
FTP	File Transfer Protocol
ICT	Information and Communication Technology atau Teknologi Maklumat dan Komunikasi
ICTSO	Pegawai Keselamatan ICT yang bertanggungjawab ke atas keselamatan ICT di TATIUC
IP	Internet Protocol
Kakitangan	Seseorang yang dilantik oleh TATIUC untuk sesuatu jawatan sama ada secara tetap, sementara atau kontrak dan masih berkhidmat
Kemudahan ICT	Termasuk, tetapi tidak terhad kepada sistem komputer peribadi, terminal, sistem komputer, alat-alat pinggiran komputer, peralatan komunikasi, rangkaian komunikasi, perisian komputer, dokumentasi bantuan, pembekalan, peralatan storan, kemudahan sokongan dan sumber tenaga. Kemudahan terhad kepada kemudahan yang dibeli, disewa, dipajak, dimiliki atau dipinjamkan kepada TATIUC. Ia termasuk semua kemudahan yang disediakan oleh TATIUC secara terpusat dan yang disediakan melalui Jabatan
Pelayan Komputer	Komputer yang mempunyai keupayaan tinggi yang memberi perkhidmatan berpusat
Maklumat Peribadi	Data atau maklumat tentang seseorang individu, termasuk nama, tarikh lahir dan sebagainya. yang mana data ini boleh digunakan untuk mengenali seseorang individu contohnya nombor kad pengenalan, nombor kakitangan dan sebagainya
Maklumat Rahsia / Sulit	Segala bentuk data sama ada teks, grafik, audio, animasi dalam pelbagai format sama ada yang boleh dicerna seperti teks ataupun dalam format binari yang terdapat dalam akaun pengguna. Maklumat ini juga boleh dicapai semasa dalam medium penghantaran (transmisi) seperti data e-mel dalam talian atau dalam simpanan fail sementara
MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, Jabatan Perdana Menteri
Perkakasan Pintar (Smart Device)	Perkakasan eletronik yang disambungkan kepada alatan atau rangkaian melalui protokol tanpa wayar yang berbeza seperti Bluetooth, NFC, Wi-fi, 3G dan sebagainya yang boleh beroperasi secara interaktif
Pengguna	Seseorang atau kumpulan orang yang dibenarkan menggunakan kemudahan ICT TATIUC

Pelajar	Seseorang yang mendaftar sesuatu program akademik (sama ada penuh atau separuh masa atau siswazah) di TATIUC dan statusnya masih aktif.
Pentadbir Sistem	Kakitangan yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan pelayan dan data yang disimpan
Pentadbir Rangkaian	Kakitangan yang bertanggungjawab mengurus, mengawal, memantau dan menyelenggara operasi dan keselamatan rangkaian kampus
Penasihat Sistem	Individu yang dilantik sebagai penasihat sistem aplikasi dan/atau teknologi ICT di TATIUC
Pentadbir Emel	Kakitangan yang diberikan tanggungjawab memantau dan menyelenggara sistem e-mel TATIUC
Perkakasan	Peralatan dan komponen ICT seperti komputer, notebook, pencetak, pengimbas dan sebagainya
Peralatan Rangkaian	Peralatan dan komponen yang digunakan dalam sistem rangkaian seperti switch, hub, router dan sebagainya
Jabatan	Semua fakulti, jabatan, pusat, seksyen dan unit di TATIUC
Sistem Maklumat (SM)	Sistem yang mengandungi semua aplikasi berkaitan dengan fungsi utama TATIUC, termasuk e-Campus, e-Attendance dan sebagainya.
TCP	Transport Communication Protocol
Tugas Dalaman	Tugas-tugas yang menyokong fungsi-fungsi TATIUC dalam pengajaran, pembelajaran, penyelidikan, perundingan dan pentadbiran
Tugas Luar	Tugas-tugas selain dan tugas dalaman.
Pemilik Maklumat	Individu yang boleh dikenal pasti melalui maklumat peribadi yang ada
TATIUC	TATI Univerisity College.
“Bring Your Own Device” (BYOD)	Amalan membenarkan kakitangan menggunakan komputer, telefon pintar atau perkakasan lain untuk tujuan menjalankan tugas.
Ketua Jabatan	Seseorang pekerja yang dilantik bagi mengetuai sesuatu fakulti, jabatan, pusat, seksyen atau unit.

1.5 Am

a. TATIUC bertanggungjawab menyediakan kemudahan ICT untuk kegunaan kakitangan akademik, pentadbiran, sokongan dan pelajar bagi menyokong fungsinya.

b. Semua kemudahan dan perkhidmatan ICT yang disediakan oleh TATIUC adalah hak mutlak TATIUC. Pengguna berdaftar diberikan keistimewaan untuk menggunakan kemudahan tersebut berdasarkan keperluan tugas dan bukannya hak yang diberikan kepada pengguna. TATIUC berhak menarik balik kebenaran dan/atau kemudahan yang diberikan pada bila-bila masa tanpa notis.

c. Kemudahan ICT yang disediakan oleh TATIUC hanya boleh digunakan untuk tujuan yang berkaitan dengan fungsi TATIUC. Penggunaan selain daripada itu seperti untuk tujuan peribadi, komersil dan politik adalah tidak dibenarkan, kecuali dengan kebenaran Ketua Jabatan.

d. Pengguna yang menggunakan peralatan ICT peribadi yang dibenarkan di dalam kampus juga tertakluk kepada polisi ini. Sebarang penggunaan adalah tertakluk kepada undang-undang

dan polisi TATIUC dan negara. TATIUC tidak akan bertanggungjawab terhadap sebarang penyalahgunaan yang dilakukan oleh pengguna.

e. Setiap pengguna mesti mematuhi Polisi ICT yang ditetapkan selaras dengan hasrat TATIUC melahirkan pengguna yang beretika dan menghormati pengguna yang lain.

f. TATIUC bertanggungjawab memastikan pelaksanaan Polisi ICT dan syarat yang berkaitan dengan pengguna dan kod etika diamalkan selaras dengan kemudahan di bawah kawalannya.

g. Ketua Jabatan bertanggungjawab memastikan Polisi ICT diamalkan selaras dengan kemudahan di bawah kawalan dan pengurusannya.

h. Polisi ini adalah tertakluk kepada perubahan dan pindaan dari semasa ke semasa mengikut keperluan. TATIUC berhak meminda, membatal, menghad dan menambah mana-mana Polisi ICT mengikut kesesuaian dan keperluan semasa.

1.6 Pelanggaran

a. Sebarang pelanggaran polisi dan peraturan oleh pengguna akan dikenakan tindakan berdasarkan kepada jenis pelanggaran dan keadaan semasa pelanggaran.

b. Sebarang aduan tentang pelanggaran Polisi ICT hendaklah dibuat secara bertulis kepada Jawatankuasa Teknologi Maklumat. Jawatankuasa Teknologi Maklumat boleh melantik Jawatankuasa Penyiasat untuk meneliti laporan dan menentukan sama ada siasatan terperinci perlu dilakukan.

c. Tindakan atau penalti yang boleh dikenakan oleh Jawatankuasa Teknologi Maklumat adalah penggantungan penggunaan kemudahan ICT. Tindakan atau penalti lain boleh diambil oleh Jawatankuasa Tatatertib Kakitangan bagi kakitangan atau Pengurus (Hal Ehwal Pelajar dan Alumni) bagi pelajar berdasarkan prosedur yang ditetapkan.

1.7 Teknologi Maklumat Peringkat Kebangsaan

Polisi ini tidak terhad kepada kandungan dokumen ini, malah ia turut mencakupi serta menerima pakai polisi / garis panduan ICT peringkat kebangsaan yang dikuatkuasakan seperti berikut :

a. Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan berdasarkan Surat Pekeliling Am Bil. 4 tahun 2004 yang dikeluarkan oleh MAMPU.

b. Polisi Keselamatan ICT Kerajaan berdasarkan Pekeliling Am Bil. 3 Tahun 2000 yang dikeluarkan oleh MAMPU.

c. Garis Panduan Malaysian Civil Service Link (MCSL) dan Laman Web Kerajaan berdasarkan Pekeliling Am BiL.1 tahun 2000 yang dikeluarkan oleh MAMPU.

d. Garis Panduan Pelaksanaan Perkongsian Pintar Antara Agensi-agensi Kerajaan Dalam Bidang Teknologi Maklumat berdasarkan Pekeliling Am Bil. 6 tahun 1999 yang dikeluarkan oleh MAMPU.

e. Penubuhan Jawatankuasa IT dan Internet Kerajaan (JITIK) berdasarkan Pekeliling Am Bil. 2 Tahun 1999 yang dikeluarkan oleh MAMPU.

f. Mekanisme Pelaporan Insiden Keselamatan ICT (ICT) melalui Pekeliling Am BiL.1 Tahun 2001 yang dikeluarkan oleh MAMPU.

g. Undang-undang Siber (Cyber Law) yang diperkenalkan oleh kerajaan dibawah program MSC Bill of Guarantees yang terdiri daripada akta berikut:

   i. Tandatangan Digital 1997

   ii. Hakcipta (amendment) 1997

   iii. Jenayah Komputer 1997

   iv. Komunikasi dan Multimedia 1998

   v. Suruhanjaya Komunikasi dan Multimedia Malaysia 1998

BAB 2 POLISI PENGURUSAN ICT

2.1 Tujuan

Menerangkan secara umum aspek pengurusan organisasi dan pembangunan Teknologi Maklumat TATIUC.

2.2 Skop

Skop polisi meliputi aspek :

a. Pengurusan organisasi ICT yang mempunyai kuasa dan kepakaran untuk merancang, melaksana dan mengurus keperluan ICT di TATIUC menerusi strategi yang ditetapkan.

b. Pembangunan ICT bagi merancang, mengurus, melaksana dan menyelenggara keperluan ICT di TATIUC menerusi strategi yang ditetapkan.

2.3 Pengurusan Organisasi

a. Penubuhan Pusat Perkhidmatan Teknologi maklumat (PPTM)

   i. Pusat Perkhidmatan Teknologi Maklumat diketuai oleh seorang ketua pusat yang bertanggungjawab dalam merancang, melaksana, mengurus, memantau dan menyelenggara projek ICT di TATIUC.

   ii. Pusat hendaklah mempunyai kakitangan teknikal yang mempunyai kepakaran ICT dan kakitangan pentadbiran / sokongan secukupnya.

   iii. Ketua pusat dilantik menganggotai Senat.

   iv. Pusat Perkhidmatan Teknologi Maklumat menubuhkan Jawatankuasa Teknikal ICT (dipengerusikan oleh ketua pusat atau wakil).

2.4 Pembangunan ICT

a. Perancangan ICT

   i. Perancangan hendaklah memenuhi fungsi dan keperluan TATIUC dalam pengajaran, pembelajaran, penyelidikan, perundingan, pentadbiran dan pengurusan.

   ii. Perancangan hendaklah selaras dengan agenda ICT Negara dan mematuhi Polisi, Peraturan dan Garis Panduan yang ditentukan oleh Kerajaan Malaysia.

b. Perolehan ICT

   i. Semua perolehan hendaklah mematuhi Prosedur Perolehan serta Kewangan TATIUC dan Kerajaan kecuali bagi kes tertentu dengan mendapat perakuan / kelulusan Bendahari.

ii. Perolehan hendaklah memenuhi teknologi terkini dengan mendapat perakuan spesifikasi oleh Jawatankuasa Teknikal PPTM.

iii. Semua perisian aplikasi dan perisian sistem hendaklah mempunyai lesen yang sah.

iv. Semua pembangunan atau perolehan sistem aplikasi yang ada hubungkait dengan pangkalan data Sistem Pengurusan Maklumat hendaklah dibuat melalui Jawatankuasa Teknikal ICT bagi menjamin keseragaman, keserasian dan keselamatan sistem.

c. Pemasangan dan Penyelenggaraan

i. Pemasangan perkakasan dan/atau perisian dilakukan di bawah penyeliaan PPTM.

ii. Ketua PPTM hendaklah memastikan peralatan ICT diselenggara sewajarnya.

d. Naik taraf atau Pelupusan

i. Semua naik taraf perkakasan dan perisian hendaklah mendapat kelulusan Jawatankuasa Teknikal ICT.

ii. Perkakasan yang tidak berkeupayaan dan/atau tidak sesuai untuk dinaiktaraf atau diperbaiki boleh dicadang untuk pelupusan mengikut Prosedur Pelupusan TATIUC.

e. Pembangunan Sumber Manusia

i. Merancang keperluan sumber manusia yang secukupnya bagi menyokong perkhidmatan ICT di TATIUC.

ii. Merancang dan melaksana pelan pembangunan sumber manusia bagi meningkatkan pengetahuan dan kemahiran teknikal.

iii. Merancang dan melaksana pelan pembangunan sumber manusia bagi meningkatkan pengetahuan dan kemahiran asas ICT serta penggunaan aplikasi ICT untuk pengguna.

BAB 3 POLISI PERISIAN, APLIKASI DAN PERKAKASAN ICT

3.1 Tujuan

Menentukan tanggungjawab pengguna dan pihak TATIUC mengenai perkara yang berhubung dengan perisian, aplikasi dan perkakasan ICT TATIUC.

3.2 Skop

Skop polisi melibatkan semua perisian, sistem aplikasi dan perkakasan ICT TATIUC yang dimiliki, diguna, dibangun, diperoleh atau berada dalam simpanan pengguna tidak kira di mana ianya berada.

3.3 Polisi Perisian dan Aplikasi

a. Hak milik

i. Semua perisian dan aplikasi yang diperolehi untuk atau bagi pihak TATIUC atau semua perisian yang dibangunkan oleh staf atau pelajar TATIUC untuk tujuan pengajaran, pembelajaran, penyelidikan atau pentadbiran adalah menjadi hak milik TATIUC.

ii. Bagi perisian dan aplikasi yang dibangunkan, maklumat tentang semua pengarang / pencipta mestilah dikekalkan.

iii. Semua perisian dan aplikasi hak milik TATIUC tidak boleh dijual, disewa, dilesenkan semula, dipinjam, disalin semula, disebar atau diberi kepada sesiapa atau entiti tanpa kebenaran pengurusan TATIUC.

b. Perolehan

i. Semua perolehan perisian dan aplikasi hendaklah mengikut Prosedur Perolehan TATIUC.

ii. Penggunaan adalah tertakluk kepada terma dan syarat penggunaan yang ditetapkan oleh pihak TATIUC, pembekal atau pembangun perisian.

iii. TATIUC tidak akan bertanggungjawab terhadap sebarang perolehan dan penggunaan perisian tanpa lesen yang dilakukan oleh pengguna.

iv. TATIUC bertanggungjawab melaksanakan peningkatan dan naik taraf perisian dan aplikasi bagi memastikan versi yang sesuai digunapakai.

v. TATIUC bertanggungjawab menyediakan perkhidmatan penyelenggaraan bagi aplikasi yang memerlukan kepakaran khusus mengikut tempoh yang sesuai.

vi. TATIUC menggalakkan penggunaan dan pembangunan aplikasi sistem perisian sumber terbuka (open source).

c. Tanggungjawab Pengguna

i. Pengguna secara peribadi bertanggungjawab untuk membaca, memahami dan mematuhi peraturan dan pelesenan bagi setiap perisian yang digunakan.

ii. Pengguna tidak dibenarkan memuat turun, membuat pemasangan dan menggunakan perisian yang boleh mendatangkan kemudaratan dan kerosakan kepada komputer dan rangkaian kampus seperti perisian P2P (peer to peer), perisian Proxy dan seumpamanya.

iii. Semua pengguna tidak dibenarkan menyebar sebarang perisian berlesen secara tidak sah.

iv. TATIUC tidak akan bertanggungjawab ke atas sebarang kesalahan yang dilakukan oleh pengguna.

v. Sebarang bentuk permainan komputer tidak dibenarkan kecuali untuk tujuan akademik dan penyelidikan setelah mendapat kelulusan daripada Ketua Jabatan.

3.4 Polisi Perkakasan

a. Hak milik

i. Semua perkakasan yang diperolehi, dicipta atau dipasang menggunakan peruntukan TATIUC oleh kakitangan atau pelajar adalah menjadi hak milik TATIUC.

ii. Bagi perkakasan yang dicipta, maklumat tentang semua pencipta mestilah dikekalkan.

iii. Perkakasan tersebut tidak dibenarkan dijual, disewa, dilesenkan semula, dipaten, dipinjam atau diberi kepada sesiapa atau entiti tanpa kebenaran pengurusan TATIUC.

b. Perolehan Perkakasan

i. Semua perolehan perkakasan hendakah mengikut Prosedur Perolehan TATIUC.

ii. Spesifikasi perkakasan hendaklah diperakukan oleh Jawatankuasa Teknikal ICT bagi memastikan piawaian, keseragaman dari segi teknologi dan keperluan semasa.

iii. Setiap perolehan perkakasan hendaklah mendapat kelulusan spesifikasi daripada Ketua PPTM.

c. Pengagihan Perkakasan

i. Semua pengagihan perkakasan hendaklah mengikut prosedur TATIUC.

ii. Kakitangan Akademik sepenuh masa layak mendapat satu (1) unit komputer dan pencetak setiap seorang. Kemudahan perkakasan dari sumber lain tertakluk kepada kelulusan Ketua Jabatan.

iii. Kakitangan Pengurusan dan Profesional sepenuh masa layak mendapat satu (1) unit komputer dan pencetak untuk setiap seorang. Kemudahan perkakasan dari sumber lain tertakluk kepada kelulusan Ketua Jabatan.

iv. Kakitangan Lantikan Khas (Prof. Emeritus / Prof. Adjung / Prof. Pelawat / Sarjana Tamu - disediakan kemudahan komputer di dalam bilik guna sama di jabatan yang berkenaan.

v. Pensyarah Kontrak layak dibekalkan komputer (setara) sedia ada dalam simpanan.

vi. Kakitangan kategori lain layak diberi komputer berdasarkan keperluan kerja yang ditentukan oleh Ketua Jabatan.

vii. Setiap pengguna hanya layak mendapat peruntukan satu (1) unit komputer dan satu (1) pencetak dalam satu-satu masa.

viii. Kakitangan yang tamat perkhidmatan termasuk tetapi tidak terhad kepada bersara atau meletak jawatan dan bercuti sabatikal luar negara perlu memaklum dan memulangkan perkakasan di bawah tanggungjawabnya kepada PPTM selewat-lewatnya satu (1) minggu sebelum tarikh berkenaan.

d. Gantian Komputer

Komputer yang telah berusia lima (5) tahun akan diganti tertakluk kepada adanya peruntukan dan komputer asal dikembalikan ke PPTM.

e. Pemilikan Komputer

Kakitangan yang akan bersara dan ingin memiliki komputer yang diterima semasa dalam perkhidmatan perlu membuat permohonan bertulis kepada Pengurus Jabatan Kewangan TATIUC.

f. Peminjaman Perkakasan

i. Semua peminjaman perkakasan hendaklah mengikut Prosedur Pinjaman di TATIUC.

ii. Setiap Jabatan yang menyediakan kemudahan pinjaman perkakasan perlu merekod maklumat peminjaman pemulangan.

iii. Peminjam bertanggungjawab sepenuhnya terhadap keselamatan peralatan yang dipinjam.

iv. Peminjam perlu melapor secara bertulis dengan segera sekiranya berlaku kerosakan atau kehilangan perkakasan yang dipinjam kepada Ketua Jabatan berkenaan.

v. Peminjam perlu memulangkan perkakasan yang dipinjam dalam keadaan baik, berfungsi dan dalam set lengkap pada tarikh dan masa pemulangan yang ditetapkan.

vi. Peminjam perlu mengganti atau membayar kos perkakasan sekiranya berlaku kerosakan ke atas perkakasan yang dipinjam.

vii. Tempoh pinjaman adalah tertakluk kepada kelulusan Ketua Jabatan berkenaan.

viii. Peminjam dari kalangan pelajar hendaklah melalui pensyarah atau pegawai di jabatan berkenaan. Pensyarah atau pegawai di Jabatan berkenaan bertanggungjawab ke atas perkakasan tersebut.

g. Baik Pulih dan Penyelenggaraan Perkakasan ICT

i. Semua baik pulih dan penyelenggaraan perkakasan hendaklah mengikut prosedur ditetapkan.

ii. Bagi kerosakan perkakasan yang dibekalkan oleh PPTM, jabatan dikehendaki mengisi aplikasi “Helpdesk”.

iii. Bagi kerosakan perkakasan yang dibeli menggunakan peruntukan jabatan , jabatan diminta membuat aduan kepada PPTM untuk tujuan pemeriksaan dan pengesahan kerosakan (tidak termasuk peralatan komputer di makmal). Sekiranya masih dalam tempoh jaminan, jabatan dikehendaki menghubungi pembekal untuk pembaikan.

iv. PPTM bertanggungjawab menyediakan perkhidmatan penyelenggaraan bagi perkakasan yang memerlukan kepakaran khusus mengikut tempoh yang sesuai.

h. Pelupusan Perkakasan

i. Semua perkakasan yang didapati tidak sesuai dinaiktaraf atau diselenggara hendaklah dicadang dilupus mengikut Prosedur Pelupusan TATIUC.

ii. Bagi perkakasan yang dibekalkan oleh PPTM, PPTM akan membuat cadangan pelupusan kepada Jawatankuasa Pelupusan TATIUC.

iii. Bagi perkakasan yang dibeli menggunakan peruntukan jabatan, jabatan diminta membuat permohonan pelupusan kepada Jawatankuasa Pelupusan TATIUC.

iv. Mana-mana perkakasan yang dilupuskan akan diganti baru tertakluk kepada adanya peruntukan.

i. Tanggungjawab Pengguna

i. Pengguna tidak berhak mengganggu dengan apa cara sekalipun perkakasan yang bukan berada di bawah kawalannya. Ini termasuk mengguna atau mengambil tanpa kebenaran, menceroboh dan mencuri perkakasan atau komponennya.

ii. Penggunaan secara perkongsian (sharing) adalah menjadi tanggungjawab bersama pengguna terbabit dan perlu mempunyai syarat dan peraturan yang dipersetujui oleh pengguna.

iii. Pengguna hendaklah melaporkan secara atas talian dengan segera kepada PPTM sekiranya perkakasan tersebut rosak atau tidak berfungsi melalui aplikasi "Helpdesk".

iv. Pengguna hendaklah melaporkan secara bertulis dengan segera kepada Ketua PPTM sekiranya perkakasan yang dibekalkan oleh Pusat PPTM tersebut hilang/dicuri.

BAB 4 POLISI RANGKAIAN ICT

4.1 Tujuan

Menentukan penyediaan, penggunaan dan pengoperasian pelayan komputer, perkhidmatan rangkaian kampus, dan penyambungan infrastruktur rangkaian Internet/Intranet.

4.2 Skop

Skop adalah :

a. Merangkumi semua sistem pelayan (perkakasan dan perisian) yang dibangun atau disediakan untuk pengguna yang dibenarkan. Ini termasuk pelayan aplikasi, pelayan operasi rangkaian dan pelayan kegunaan setempat. (domain, fail server).

b. Merangkumi semua sumber rangkaian, termasuk tetapi tidak terhad kepada peralatan rangkaian seperti “switches” dan “routers”, perisian aplikasi rangkaian seperti “e-mail”, “web browser” dan “ftp”, konsep konfigurasi rangkaian seperti penggunaan alamat IP dan teknologi dan protokol rangkaian yang diguna seperti teknologi Gigabit dan protokol TCP / IP.

c. Merangkumi penggunaan kemudahan emel TATIUC dan bukan TATIUC.

d. Merangkumi pembangunan laman web di TATIUC, sama ada dibangunkan secara berpusat oleh Jawatankuasa Laman Web TATIUC menggunakan laman web utama atau secara berasingan oleh jabatan.

e. Merangkumi penggunaan Internet / Intranet termasuk tetapi tidak terhad kepada capaian sistem aplikasi / portal TATIUC, laman web, pemindahan data atau maklumat dan perbincangan melalui “list group” atau “chat room”.

4.3 Pelayan Komputer

a. Hak milik

Semua pelayan komputer yang diperolehi untuk atau bagi pihak TATIUC adalah menjadi hak milik TATIUC.

b. Perolehan

Semua perolehan hendaklah mengikut Prosedur Perolehan TATIUC.

i. Spesifikasi pelayan komputer hendaklah diperakukan oleh Jawatankuasa Teknikal ICT bagi memastikan piawaian dan keseragaman dari segi teknologi dan keperluan semasa.

ii. Setiap perolehan pelayan komputer perlu dimaklumkan kepada PPTM untuk pengesahan spesifikasi dan rekod aset.

c. Konfigurasi dan Operasi

i. Semua pelayan komputer untuk kegunaan dalaman akan diberi alamat IP dalaman statik. Alamat IP global boleh dipertimbangkan oleh PPTM (sebagai pentadbir alamat IP TATIUC) bagi keperluan capaian fail daripada luar / Local Area Network (LAN).

ii. Semua pelayan komputer perlu didaftarkan dengan PPTM, berada di dalam "domain" TATIUC dan perlu menyatakan dengan jelas fungsi pelayan tersebut.

iii. Pentadbir Sistem perlu memastikan keselamatan pelayan daripada pencerobohan. Ini termasuk tetapi tidak terhad kepada membuat pemeriksaan ke atas proses tersembunyi (hidden processes), daemons, mengemaskini perisian seperti emel dan laman web dan mengenalpasti tahap capaian pengguna dan penggunaan pelayan komputer.

iv. Pelayan Komputer yang digunakan untuk tujuan penyelidikan yang menggunakan rangkaian secara intensif (high bandwidth usage) perlu ditempatkan dalam rangkaian persendirian yang dipisahkan daripada rangkaian utama Kampus melalui penggunaan switch / router untuk mengelak gangguan kepada rangkaian utama. Sebarang ujian yang memerlukan penggunaan rangkaian utama secara terus perlu mendapat kelulusan daripada Ketua PPTM.

v. Pelayan komputer yang digunakan untuk projek pelajar perlu mendapat kelulusan daripada penyelia projek / Dekan. Alamat IP dalaman statik digunakan untuk server ini. Alamat IP global boleh diberi kepada projek yang memerlukan capaian Internet.

vi. Komputer server untuk kegunaan lain (contoh kafe siber) tidak dibenarkan menggunakan rangkaian Kampus.Net / College.Net untuk mengelak gangguan rangkaian.

vii. Alamat IP tidak dibenarkan diubah sama sekali kecuali setelah mendapat kelulusan Ketua PPTM.

viii. Login dan kata laluan untuk id root dan super-user adalah di bawah kawalan dan tanggungjawab Pentadbir Sistem sepenuhnya.

4.4 Rangkaian Kampus

a. Hak milik

Semua sumber rangkaian yang diperolehi untuk atau bagi pihak TATIUC adalah menjadi hak milik TATIUC.

b. Perolehan

i. Semua perolehan sumber rangkaian hendaklah mengikut Prosedur Perolehan TATIUC.

ii. Perolehan peralatan rangkaian seperti “router” dan titik akses tanpa wayar (wireless access point) oleh jabatan adalah tidak dibenarkan kecuali dengan kelulusan Jawatankuasa Teknikal ICT.

c. Kemudahan Rangkaian Kampus

i. Pengguna tidak dibenarkan dalam apa bentuk sekali pun mengganggu lain-lain pengguna Internet dan sebarang rangkaian yang lain termasuk tetapi tidak terhad kepada menghantar maklumat rambang (spam) secara emel atau mesej atas talian (online).

ii. Pengguna tidak boleh memberi sumber rangkaian di bawah jagaannya termasuk tetapi tidak terhad kepada nod rangkaian dan kad tanpa wayar untuk diguna oleh orang lain walaupun kepada pelajar atau kakitangan TATIUC tanpa mendapat kelulusan Ketua PPTM.

iii. Pengguna bertanggungjawab sepenuhnya terhadap semua aktiviti yang dilakukannya termasuk tetapi tidak terhad kepada stesen kerja, komputer peribadi atau gajet yang melibatkan atau melalui rangkaian kampus termasuk akses ke Internet dan rangkaian yang lain.

iv. Mana-mana komputer yang menjadi sumber ancaman atau penyebaran virus akan disekat capaiannya ke rangkaian kampus dan akan ditutup sehingga komputer tersebut disahkan bebas dari ancaman virus.

d. Penyambungan Rangkaian

i. Perolehan peralatan rangkaian dan penyambungan ke rangkaian kampus perlu mendapat kelulusan Ketua PPTM. Konfigurasi penyambungan hendaklah dibuat oleh pembekal di bawah pengawasan dan kawalan kakitangan PPTM.

ii. Sebarang penyambungan rangkaian kampus yang tidak mendapat kebenaran PPTM adalah menyalahi peraturan dan PPTM berhak memutuskan penyambungan tersebut. Tindakan susulan boleh diambil ke atas pengguna atas nasihat pengurusan TATIUC.

iii. Penyambungan Rangkaian Antara Kampus dan Rangkaian Luas (WAN) tidak boleh dilakukan oleh pengguna tanpa kelulusan.

iv. Setiap bangunan baru yang akan dibina perlu memasukkan keperluan infrastruktur rangkaian yang ditentukan bersama oleh pengguna, PPTM dan Jabatan Pembangunan dan Pengurusan Harta (JPPH). Kos pemasangan infrastruktur rangkaian perlu dimasukkan dalam kos peruntukan pembinaan bangunan.

4.5 Penggunaan Emel

a. Pengguna hendaklah mendaftar dan menggunakan perisian emel rasmi TATIUC untuk tujuan komunikasi rasmi melalui emel.

b. Aktiviti “spamming” atau “mail-bombing” dan penyebaran emel dengan kandungan tidak beretika (seperti lucah, ugutan, politik, perkauman dan gangguan) kepada individu, “mailing list” atau “discussion group” sama ada di dalam rangkaian Internet / Intranet adalah tidak dibenarkan.

c. PPTM berhak memasang sebarang jenis perisian atau perkakasan penapisan emel dan virus (email filter and anti virus) yang difikirkan sesuai dan boleh menggunakannya untuk mencegah, menapis menyekat atau menghapuskan mana-mana emel yang disyaki mengandungi “virus” atau berunsur “spamming” daripada memasuki pelayan, stesen kerja atau rangkaian kampus dan keluar daripada pelayan, stesen kerja dan rangkaian kampus.

d. PPTM tidak bertanggungjawab terhadap pengguna yang menjadi penghantar (sender) atau penerima (receiver) kepada sebarang emel yang berunsur “spamming” atau penyebaran emel dengan kandungan tidak beretika.

e. PPTM tidak bertanggungjawab terhadap sebarang kerosakan, kehilangan atau sebarang kesan lain kepada maklumat, aplikasi, data, kotak emel atau fail yang disimpan oleh pengguna di dalam stesen kerja atau pelayan akibat daripada penggunaan perkhidmatan emel.

f. Pengguna digalakkan menukar kata laluan secara berkala (dicadangkan dibuat setiap 3 bulan oleh pengguna).

g. Kemudahan emel juga boleh disediakan kepada organisasi atau persatuan rasmi TATIUC melalui permohonan rasmi kepada PPTM.

h. Pengguna individu tidak dibenarkan memohon dan / atau memiliki Iebih daripada satu akaun atau alamat emel TATIUC pada satu-satu masa.

i. Setiap alamat emel yang disediakan adalah untuk kegunaan individu atau organisasi / persatuan berkenaan sahaja dan tidak boleh digunakan oleh pihak lain sama ada dengan kebenaran atau tanpa kebenaran.

j. Pengguna dilarang menggunakan kemudahan emel untuk sebarang aktiviti yang tidak dibenarkan oleh peraturan TATIUC dan undang-undang negara.

k. Semua pengguna yang diberi kemudahan emel TATIUC tidak dibenarkan mengguna emel luar (seperti hotmail, gmail, yahoo dan lain-lain) untuk tujuan rasmi. Pentadbir emel berhak menghalang penggunaan emel tersebut jika didapati memudarat dan membebankan rangkaian kampus.

l. Di dalam kes sistem tergendala (rosak), pihak pentadbir sistem hanya bertanggungjawab untuk memulihkan kembali (restore) maklumat akaun pengguna dan bukannya kandungan / kotak emel (mailbox) pengguna.

m. Pentadbir Emel dengan kelulusan TATIUC berhak memeriksa dan melihat isi kandungan emel dan ruang storan pengguna dari semasa ke semasa atas keperluan audit dan keselamatan.

4.6 Penamatan Akaun Emel

TATIUC boleh menamatkan kemudahan akaun emel yang telah diberikan kepada kakitangan dan pelajar atas sebab berikut:

a. kakitangan telah tamat perkhidmatan.

b. pelajar telah tamat pengajian (akaun emelnya dipindah secara automatik ke alamat emel alumni) atau ditamatkan pengajian.

c. persatuan yang telah dibubarkan secara rasmi.

d. permintaan daripada kakitangan atau pelajar sendiri.

e. kakitangan atau pelajar tidak bersetuju atau melanggar polisi yang ditetapkan.

4.7 Laman Web

a. TATIUC menyediakan tapak untuk laman web rasmi jabatan/persatuan atau aktiviti rasmi sahaja.

b. Ketua jabatan/persatuan/organisasi adalah bertanggungjawab sepenuhnya terhadap semua kandungan dan keselamatan laman web masing- masing. TATIUC tidak akan bertanggungjawab terhadap kandungan dan sebarang penyalahgunaan hak cipta yang dilakukan dan TATIUC juga boleh menghadkan atau memansuhkan akses kepada tapak laman web tersebut.

c. Semua laman web jabatan mesti mempunyai pautan dengan laman utama TATIUC. TATIUC berhak menukar atau mengubahsuai kandungan laman web atas kepentingan TATIUC.

d. TATIUC berhak menentukan perisian pembangunan laman web bagi tujuan pengoptimuman penggunaan dan keselamatan.

e. Laman web peribadi yang berbentuk ilmiah adalah dibenarkan dengan kelulusan terlebih dahulu. TATIUC tidak akan bertanggungjawab terhadap kandungan dan sebarang penyalahgunaan hakcipta yang dilakukan oleh jabatan atau individu.

f. Kandungan laman web hendaklah dipersembahkan dalam Bahasa Melayu dan/atau Bahasa Inggeris. Penggunaan bahasa lain perlu mendapat kelulusan terlebih dahulu.

g. Kandungan laman web hendaklah tidak mengandungi maklumat atau terdedah kepada kemasukan maklumat yang menyalahi peraturan TATIUC dan undang-undang negara termasuk tetapi tidak terhad kepada maklumat yang berbentuk keganasan, lucah, politik, hasutan dan yang boleh menimbulkan atau membawa kepada keganasan, keruntuhan akhlak dan kebencian.

h. Semua laman web jabatan / peribadi / persatuan yang dibangunkan sendiri perlu dimaklumkan kepada PPTM dan mematuhi garis panduan yang ditetapkan.

4.8 Capaian Internet / Intranet

a. Laman Yang boleh Dilayari

i. TATIUC berhak menyediakan dan memasang perisian penapisan isi kandungan Internet / Intranet.

ii. Laman yang boleh dilayari, dilanggan dan diguna adalah berbentuk akademik dan pengetahuan. Laman yang berbentuk keganasan, lucah, politik, hasutan dan yang boleh menimbul atau membawa kepada keganasan, keruntuhan akhlak dan kebencian adalah tidak dibenarkan sama sekali, kecuali mendapat keizinan daripada Ketua PPTM melalui sokongan ketua jabatan bagi tujuan akademik, penyelidikan atau pentadbiran.

iii. Capaian laman yang berbentuk hiburan, hobi atau santai tidak dibenarkan di waktu pejabat, termasuk tetapi tidak terhad kepada laman game online, radio online dan video streaming yang membebankan rangkaian kampus kecuali yang telah disediakan oleh PPTM dengan kelulusan TATIUC.

iv. Melayari internet tanpa tujuan atau meninggalkan capaian “Internet unattended” adalah amat tidak beretika dan tidak digalakkan kerana ianya boleh menyebabkan kesesakan.

v. TATIUC berhak menapis, menghalang dan menegah penggunaan mana-mana laman web yang dianggap tidak sesuai.

b. Penyalahgunaan Laman Web

i. Pengguna dilarang mengganggu atau menceroboh laman web mana-mana jabatan, organisasi atau negara.

ii. Pengguna dilarang memasuki, menyalin, menciplak, mencetak dan menyebarkan maklumat daripada internet yang menyalahi undang-undang negara.

iii. Penggunaan “Internet chatting” tidak dibenarkan kecuali untuk tujuan rasmi.

iv. Pengguna tidak dibenarkan menggunakan sumber ICT TATIUC untuk mendapatkan atau cuba menggodam mana-mana sistem komputer sama ada di dalam atau luar TATIUC. Ini termasuk membantu, mendorong, menyembunyikan percubaan untuk mencapai sistem komputer tersebut atau mencapai sumber ICT TATIUC dengan menggunakan identiti pengguna lain.

v. Pengguna tidak dibenar mencapai atau cuba mencapai sumber elektronik (data, paparan, keystrokes, fail atau media storan) dalam sebarang bentuk yang dimiliki oleh pengguna lain tanpa mendapat kebenaran/kelulusan pengguna terbabit terlebih dahulu. Ini termasuk membaca, menyalin, menukar, merosak atau

memadam data, program dan perisian. Penggunaan penganalisis rangkaian (network analyzer) atau pengintip (sniffer) adalah dilarang kecuali untuk tujuan pembelajaran dan telah mendapat kelulusan daripada jabatan.

vi. Pengguna yang mencapai sesuatu perkhidmatan yang perlu dibayar (contohnya pangkalan data online komersial), hendaklah bertanggungjawab ke atas segala bayaran yang dikenakan.

BAB 5 POLISI PENGGUNAAN MAKMAL KOMPUTER

5.1 Tujuan

Menerangkan penguatkuasaan penggunaan makmal komputer di TATIUC dan sebagai garis panduan umum untuk penyelia makmal komputer di jabatan selain daripada peraturan khusus yang disediakan oleh jabatan.

5.2 Skop

Setiap pengguna mesti mematuhi syarat dan peraturan penggunaan makmal yang ditetapkan oleh penyelia makmal masing-masing. Sebarang pelanggaran peraturan atau penyalahgunaan adalah tertakluk kepada Polisi ICT.

5.3 Penggunaan Makmal

a. Penggunaan makmal komputer adalah tertakluk kepada aktiviti TATIUC sahaja.

b. Setiap jabatan hendaklah menyedia, memaklum dan menguatkuasakan peraturan penggunaan makmal komputer masing-masing kepada pengguna.

c. Peraturan makmal yang digubal hendaklah melarang pengguna melakukan perkara berikut :

   i. Sembang siber (chatting).

   ii. Melayari laman web pornografi dan yang diharamkan oleh undang-undang dan TATIUC.

   iii. Makan dan minum.

   iv. Menghisap rokok.

   v. Membuat bising termasuk tetapi tidak terhad kepada berbual, berbincang, memasang dan mendengar muzik.

   vi. Mengganggu pengguna lain dengan apa cara sekalipun, termasuk menimbulkan rasa aib, marah dan tidak selesa.

   vii. Berkelakuan tidak senonoh atau mengaibkan.

   viii. Menukar kedudukan komputer dan peranti.

   ix. Menukar konfigurasi komputer.

   x. Menambah atau membuang sebarang perisian.

   xi. Menyimpan atau memuat turun maklumat atau data ke dalam cakera keras komputer.

xii. Membawa keluar sebarang peralatan dan makmal.

xiii. Bermain sebarang bentuk permainan komputer.

xiv. Mencuri peranti dan perkakasan komputer.

xv. Sebarang perlakuan yang menyalahi peraturan yang telah ditetapkan oleh PPTM atau jabatan berkaitan dari semasa ke semasa.

d. Pengguna hendaklah mendapat kebenaran penyelia makmal untuk memasang perisian ke dalam komputer.

e. Pengguna hendaklah mematuhi sebarang arahan tambahan dari penyelia makmal yang bertugas.

f. Pengguna hendaklah berpakaian mengikut Etika Pakaian TATIUC yang dikuatkuasakan termasuk memaparkan/memakai tanda nama kad pelajar setiap masa.

g. Semua penggunaan komputer di dalam makmal (sama ada yang disambung ke sistem rangkaian kampus atau tidak) mesti direkodkan ke dalam Buku Log atau sistem secara online yang dikuatkuasakan. Rekod tersebut hendaklah mempunyai sekurang-kurangnya maklumat berikut:

i. Tarikh

ii. Nama Pengguna

iii. No. Matrik / No. Pekerja / No. Kad Pengenalan

iv. No. Komputer / Alatan

v. Masa mula penggunaan

vi. Masa tamat penggunaan

vii. Tandatangan pengguna (jika manual)

Buku Log ini (sama ada berbentuk digital atau manual) perlu disimpan dengan baik sekurang-kurangnya untuk tempoh lima (5) tahun bagi tujuan rujukan jika diperlukan.

h. Sebarang tempahan makmal perlu mengikut prosedur yang telah ditetapkan oleh jabatan berkaitan.

5.4 Pelanggaran Peraturan

Pengguna yang melanggar mana-mana peraturan di atas boleh diambil tindakan tegas, termasuk tetapi tidak terhad kepada:

a. Dilarang masuk menggunakan peralatan di dalam makmal.

b. Ditarik balik kemudahan menggunakan alatan / akaun pengguna (jika ada).

c. Bertanggungjawab mengganti atau membayar kos peralatan yang dicuri, hilang atau rosak atas kecuaian semasa penggunaan.

d. Dihadapkan ke Jawatankuasa Tatatertib Kakitangan bagi kakitangan dan Pengurus (Hal Ehwal Pelajar dan Alumni) bagi pelajar.

BAB 6 POLISI AKAUNTABILITI DAN KERAHSIAAN MAKLUMAT

6.1 Tujuan

Menyatakan tanggungjawab pihak yang terlibat dengan penggunaan kemudahan ICT di TATIUC seperti berikut:

a. melindungi kepentingan pengguna utama ICT apabila berlaku kejadian pelanggaran atau pencabulan Polisi Keselamatan ICT (Bab 7).

b. memelihara dan melindungi maklumat peribadi yang dimiliki TATIUC.

c. menyokong usaha TATIUC untuk menjaga kepentingan "stakeholder".

d. menerangkan aktiviti yang dilakukan oleh pentadbir operasi yang melibatkan capaian data, maklumat, atau kegiatan pengguna yang diklasifikasikan sebagai rahsia atau sulit.

6.2 Skop

Meliputi tanggungjawab pengguna dan TATIUC berkaitan capaian maklumat sulit.

Nota :
Maklumat peribadi yang diambil untuk memudahkan seseorang individu berhubung, seperti alamat yang disediakan oleh seseorang individu adalah tidak termasuk dalam polisi ini.

6.3 Capaian Maklumat Sulit

a. Pengguna ditegah menyimpan data atau maklumat sensitif, rahsia atau sulit.

b. Pentadbir Sistem mempunyai kuasa untuk mencapai, merekod, atau memantau data, maklumat atau kegiatan pengguna dari semasa ke semasa sebagai rutin pemantauan keselamatan ICT. Maklumat yang direkodkan ini akan digunakan untuk tujuan penjagaan keselamatan ICT. Contohnya, arahan dalam sistem pelayan komputer UNIX seperti last, syslogd, acctcom, pacct yang berfungsi merekod aktiviti pengguna untuk tujuan pengauditan.

c. Pentadbir Sistem mempunyai kuasa tanpa perlu mendapat kebenaran terlebih dahulu daripada pihak TATIUC untuk memantau kegiatan dan aktiviti pengguna yang melanggar Polisi Keselamatan ICT (Bab 7). Segala maklumat yang direkodkan boleh digunakan sebagai bukti. Sekiranya pelanggaran Polisi Keselamatan ICT tersebut serius seperti menggunakan identiti pengguna lain untuk mencuri data atau merosakkan sumber ICT, maka bukti yang dikumpul akan dikemukakan kepada Jawatankuasa ICT TATIUC.

d. Pentadbir Sistem boleh membuat salinan sama ada dalam bentuk bercetak atau digital kesemua atau sebahagian kandungan akaun pengguna sebagai pemeliharaan bukti. Pentadbir sistem dengan kebenaran TATIUC boleh mencapai maklumat atau data sulit atau rahsia pengguna seperti emel atau fail yang tersimpan dalam akaunnya.

e. Pengguna diberi jaminan bahawa selain daripada perkara-perkara yang disebutkan di atas, data, maklumat rahsia atau sulit yang terdapat dalam akaun pengguna tidak akan dicapai oleh sesiapa pun. Sekiranya ada individu atau pengguna lain mencapai data atau maklumat pengguna lain tanpa kebenaran, maka individu tersebut (pengguna biasa atau pentadbir sistem) telah melanggar Polisi Capaian Maklumat Sulit (6.3).

6.4 Pemantauan Data dalam Rangkaian

a. Pentadbir Sistem mempunyai kuasa untuk memantau dan merekodkan data yang berada dalam rangkaian sebagai sebahagian daripada rutin penjagaan keselamatan sumber ICT. Peralatan rangkaian seperti "router" atau sistem pelayan komputer yang menggunakan perisian tertentu mampu merekodkan data dalam rangkaian. Jaminan diberikan bahawa data yang direkodkan tidak akan didedahkan melainkan jika berlaku kejadian pelanggaran Polisi Keselamatan ICT (Bab 7).

b. Sekiranya Pentadbir Sistem mengesyaki pengguna melanggar Polisi Keselamatan ICT (Bab 7), maka Pentadbir Sistem mempunyai mandat tanpa perlu mendapat kebenaran TATIUC untuk memantau dan merekodkan data dalam talian yang melibatkan aktiviti pengguna dengan lebih teliti. Data komunikasi daripada mesin/peralatan yang digunakan oleh pengguna yang disyaki akan direkodkan dan setiap "keystroke" juga akan direkodkan. Data ini akan digunakan sebagai bahan bukti untuk proses pengauditan yang akan dilakukan oleh Jawatankuasa Keselamatan ICT.

c. Jaminan adalah diberikan kepada pengguna bahawa selain daripada perkara yang dinyatakan di atas, adalah menjadi kesalahan jika pengguna (pentadbir sistem atau pengguna biasa) memantau atau merekodkan data yang berada dalam rangkaian.

6.5. Pengurusan Maklumat Sulit / Peribadi

Pengambilan dan Kaedah Maklumat Sulit / Peribadi

a. Pengambilan selain daripada pemberi maklumat (bukan pemilik maklumat), bagi kes di mana maklumat diambil daripada pihak ketiga, pemilik maklumat hendaklah dimaklumkan tentang maklumat yang diambil dan tujuan penggunaan maklumat tersebut. Apabila maklumat yang diberi oleh seseorang kepada seseorang yang lain dengan izin pemberi maklumat, perkara berikut hendaklah diikuti:

    i. Tujuan pengambilan maklumat.

    ii. Jenis maklumat yang diambil.

    iii. Tanggungjawab untuk memastikan maklumat dijaga atau disimpan dengan baik.

b. Had-Had Penggunaan

    Maklumat peribadi mestilah digunakan untuk tujuan yang telah dinyatakan ketika maklumat itu diperolehi daripada pemberi maklumat dalam skop yang dibenarkan oleh TATIUC.

    i. Had-had penggunaan untuk tujuan yang diperlukan penggunaan maklumat peribadi yang telah diambil mestilah mengikut syarat-syarat berikut:

(aa) Pemilik maklumat telah memberi kebenaran menggunakan maklumat tersebut.

(bb) Maklumat boleh digunakan oleh pemilik maklumat bagi pengesahan sesuatu kontrak.

(cc) Maklumat boleh digunakan untuk tujuan mahkamah atau perundangan.

(dd) Maklumat boleh digunakan untuk melindungi maklumat dalam semua perkara.

Nota:
Dalam menyediakan perlindungan yang efektif berkaitan maklumat peribadi seseorang, maklumat peribadi tidak boleh digunakan selain daripada syarat-syarat yang dijelaskan di atas.

ii. Penggunaan maklumat peribadi untuk tujuan selain daripada yang dinyatakan ketika maklumat itu diperolehi apabila maklumat peribadi digunakan selain daripada tujuan asal ketika maklumat itu diambil, kebenaran daripada pemilik maklumat mestilah diperolehi dengan kaedah yang dinyatakan dalam kaedah pengambilan data. Pemilik maklumat mempunyai hak untuk tidak memberi keizinan penggunaan maklumat tersebut.

c. Penyelenggaraan Maklumat Peribadi

i. Pengguna bertanggungjawab memastikan ketepatan maklumat peribadi dan sentiasa dikemaskinikan.

ii. Pejabat Pendaftar perlu mengemaskini maklumat peribadi jika pengguna telah tamat atau ditamatkan perkhidmatan atau pengajian.

iii. TATIUC bertanggungjawab menjamin keselamatan dan kerahsiaan maklumat yang disimpan.

iv. Data perlu disulitkan (encrypted) sekiranya disimpan dalam media elektronik untuk penghantaran secara rangkaian.

v. Permintaan untuk mencapai maklumat peribadi oleh individu untuk tujuan pengesahan (verification) mestilah diberi untuk satu tempoh yang berpatutan. Penerima maklumat hendaklah diberitahu sekiranya terdapat kesilapan maklumat ketika diperiksa oleh individu tersebut.

vi. Pihak TATIUC berhak menggunakan maklumat peribadi untuk tujuan pengesahan atau bagi memenuhi keperluan TATIUC, negeri atau negara.

BAB 7 POLISI KESELAMATAN ICT

7.1 Tujuan

a. Memastikan pengawalan dan pengurusan keselamatan ke atas perkakasan, perisian, aplikasi dan operasi komputer.

b. Menerangkan perlaksanaan keselamatan rangkaian kampus rupakan infrastruktur rangkaian setempat (LAN) untuk penyambungan bagi tujuan komunikasi dan perkongsian maklumat/sumber.

7.2 Skop

a. merangkumi aspek keselamatan perkakasan, perisian sistem, pangkalan data dan sistem aplikasi.

b. aspek reka bentuk keselamatan rangkaian.

7.3 Keselamatan Sistem Komputer Pelayan dan Sistem Aplikasi

PPTM perlu memastikan sistem komputer dan pelayan perlu mempunyai kawalan capaian logikal dan fizikal, sistem penyalinan maklumat (backup), penyelenggaraan berkala dan jejak audit.

a. Kawalan Capaian Fizikal

   i. Kawalan terhadap individu/staf yang memasuki Bilik Pusat Data dan kawalan akses kepada komputer pelayan serta sumber-sumber ICT lain.

   ii. Mewujudkan prosedur kawalan capaian fizikal terhadap komputer pelayan bagi staf/individu.

b. Kawalan Capaian Logikal

   Kawalan dibuat semasa proses pemasangan. Hanya mereka yang dibenarkan sahaja boleh mencapai sistem dan mekanisma kawalan capaian adalah berasaskan identifikasi pengguna iaitu pengguna sistem boleh terdiri daripada individu atau kumpulan pengguna yang berkongsi akaun kumpulan pengguna yang sama.

c. Jejak Audit

   PPTM bertanggungjawab menyedia dan menyimpan rekod jejak audit bagi mengenalpasti akauntabiliti pengguna dan keselamatan data. Jejak audit untuk sistem komputer dan manual operasi perlu diwujudkan bagi:

   i. Capaian kepada maklumat yang kritikal.

   ii. Capaian kepada perkhidmatan rangkaian.

iii. Kebenaran istimewa kepada pengguna biasa digunakan seperti arahan-arahan keselamatan dan fungsi-fungsi superuser.

d. Penyalinan Maklumat (Back-up)

i. PPTM bertanggungjawab memulihkan sistem sepenuhnya jika berlaku masalah atau kerosakan.

ii. Proses penyalinan hendaklah dibuat secara berjadual dan semasa membuat sebarang perubahan konfigurasi pada sistem. Salinan perlu disimpan dengan baik di tempat yang selamat.

e. Penyelenggaraan

PPTM perlu melaksanakan kawalan dan penyelenggaraan bagi memastikan integriti sistem pengoperasian tidak terdedah kepada sebarang pencerobohan keselamatan.

7.4 Keselamatan Penggunaan Emel

Rujuk Bab 4.5 Penggunaan Emel

7.5 Keselamatan Peralatan Rangkaian

a. Keselamatan Pemasangan

Setiap peralatan yang akan dipasang mestilah mematuhi Factory Acceptance Check (FAC) sebelum pemasangan dan konfigurasi dilakukan.

b. Keselamatan Fizikal

i. Peralatan rangkaian hendaklah ditempatkan di tempat yang bebas daripada risiko di luar jangkaan seperti banjir, kilat, gegaran, kekotoran dan sebagainya.

ii. Suhu hendaklah terkawal di dalam had suhu peralatan rangkaian berkenaan dengan memasang sistem penghawa dingin sepanjang masa.

iii. Memasang Uninterruptible Power Supply (UPS) dengan minimum 15 minit masa beroperasi jika terputus bekalan elektrik dan perlindungan daripada kilat dan menyokong penutupan (shut down) pelayan secara automatik.

c. Capaian Fizikal

i. Capaian Pengkabelan Rangkaian

Langkah yang perlu diambil untuk melindungi kabel rangkaian daripada dicapai oleh yang tidak berkenaan:

(aa) melindungi pengkabelan di dalam kawasan awam dengan cara memasang conduit atau lain-lain mekanisma perlindungan.

(bb) pusat pendawaian terletak di dalam ruang atau bilik yang berkunci dan hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja.

ii. Capaian Peralatan Rangkaian

(aa) Peralatan hendaklah ditempatkan di tempat yang selamat dan terkawal.

(bb) Peralatan rangkaian hanya boleh dicapai oleh kakitangan yang dibenarkan sahaja.

iii. Capaian Logikal

(aa) ID dan kata laluan diperlukan untuk mencapai perisian rangkaian. Capaian hanya boleh dibuat oleh kakitangan yang dibenarkan sahaja.

(bb) Komposisi kata laluan mestilah konsisten dengan garis panduan yang telah ditetapkan.

(cc) Maklumat capaian ke “router” hendaklah direkodkan - pegawai, tarikh, masa dan aktiviti. Maklumat mestilah disimpan sekurang- kurangnya selama 90 hari.

(dd) Rangkaian hanya menerima trafik daripada alamat IP dalaman yang berdaftar sahaja. Semua perubahan konfigurasi suis rangkaian hendaklah dilogkan termasuk pengguna yang membuat perubahan, pengesahan, tarikh dan masa.

(ee) Perubahan perisian konfigurasi mestilah direkodkan - pegawai yang membuat perubahan, pegawai yang membenarkan perubahan dibuat dan tarikh.

(ff) secara berpusat.

iv. Penggunaan Peralatan Tanpa Kebenaran

(aa) Mengadakan kawalan capaian logikal (rujuk perenggan 7.3b).

(bb) Menempatkan peralatan di tempat yang selamat dan terkawal.

(cc) Bilik pendawaian atau “wiring closet” hanya boleh dicapai oleh pegawai yang dibenarkan sahaja.

(dd) menyelenggara inventori peralatan dan membuat semakan secara berkala.

v. Konfigurasi Peralatan

(aa) Mengaktifkan (enable) perkhidmatan yang diperlukan sahaja.

(bb) Menghadkan capaian konfigurasi kepada nod atau alamat IP yang dibenarkan sahaja.

(cc) Mematikan (disable) penyiaran trafik (broadcast).

(dd) Menggunakan kata laluan yang selamat.

(ee) Dilaksanakan oleh kakitangan yang terlatih dan dibenarkan sahaja.

vi. Penyelenggaraan Peralatan

(aa) Peralatan hendaklah dipasang, dioperasi dan diselenggarakan mengikut spesifikasi pengilang.

(bb) Dibaiki dan diselenggara hanya oleh kakitangan yang terlatih dan dibenarkan sahaja.

(cc) Mengemaskini rekod penyelenggaraan.

7.6 Kebolehcapaian Pengguna (User Accessibility)

Rangkaian Setempat (Local Area Network)

a. Hanya kakitangan dan pelajar TATIUC dibenarkan membuat penyambungan ke rangkaian TATIUC rujuk Polisi Rangkaian ICT (Bab 4).

b. Pengguna luar perlu mendapatkan kebenaran Ketua PPTM sebelum membuat capaian ke rangkaian TATIUC.

c. pengguna yang disahkan sahaja dibenarkan membuat capaian kepada sistem pengkomputeran TATIUC.

d. Perisian pengintip (sniffer) atau penganalisis rangkaian (network analyzer) tidak dibenar digunakan pada sebarang komputer kecuali setelah mendapat kebenaran daripada Ketua PPTM. Status komputer hendaklah disemak setiap tahun.

7.7 Sambungan Dengan Lain-Lain Rangkaian

a. Firewall

i. Semua trafik rangkaian daripada dalam ke luar TATIUC dan sebaliknya mestilah melalui firewall dan hanya trafik yang disahkan sahaja dibenarkan untuk melepasinya. (rujuk Polisi Rangkaian ICT - Bab 4).

ii. Reka bentuk firewall hendaklah mengambil kira perkara berikut:

(aa) keperluan audit dan arkib.

(bb) kebolehsediaan.

(cc) kerahsiaan.

(dd) melindungi maklumat TATIUC.

iii. Jabatan yang mempunyai pelayan komputer sendiri boleh menyediakan firewall khusus untuk tujuan keselamatan.

b. Capaian Rangkaian Teragih (Distributed Network Access)

Kawalan capaian teragih hendaklah berasaskan kepada:

i. Identification dan authentication (contoh: password / smartcard).

ii. Capaian kawalan fizikal.

BAB 8 PEMATUHAN KEPADA UNDANG-UNDANG

8.1 Pemakaian Peruntukan

Jika terdapat apa-apa peruntukan di dalam Polisi ICT TATIUC ini yang diputuskan sebagai tidak sah atau salah di sisi undang-undang yang terpakai, peruntukan tersebut akan menjadi tidak terpakai sepenuhnya dan Polisi ICT TATIUC ini akan ditafsirkan seolah-olah peruntukan tersebut tidak menjadi sebahagian daripada Polisi ICT TATIUC ini dan peruntukan yang selebihnya di dalam Polisi ICT TATIUC ini adalah kekal berkesan dan berkuatkuasa sepenuhnya.

8.2 Pematuhan Kepada Undang - Undang

TATIUC dan setiap pengguna adalah dengan ini dikehendaki mematuhi segala undang-undang dan peraturan-peraturan mengenai penggunaan ICT yang sedang berkuatkuasa di Malaysia.