

# **Polisi & Peraturan**

Teknologi Maklumat & Telekomunikasi (ICT)

# Polisi & Peraturan

Teknologi Maklumat & Telekomunikasi (ICT)

---

## Isi Kandungan

---

### A. Polisi Teknologi Maklumat Dan Komunikasi (ICT)

1. PENGENALAN	2
2. TUJUAN	2
3. SASARAN	2
4. KAEDAH PENGGUNAAN ICT	2
5. PELAKSANAAN	2
6. TEMPAT PENGGUNAAN PERKHIDMATAN ICT	2
7. HAK MILIK	2
8. HAK MILIK PERIBADI	3
9. PENGGUNAAN <i>INCIDENTAL</i>	3
10. TINDAKAN TATATERTIB	3

### B. Peraturan Penggunaan Internet

1. PENGENALAN	5
2. TUJUAN PERATURAN	5
3. SKOP PERATURAN	5
4. PERNYATAAN PERATURAN	5
5. PERNYATAAN PANDUAN	6

### C. Peraturan Penggunaan E-mel

1. PENGENALAN	8
2. TUJUAN PERATURAN	8
3. SKOP PERATURAN	8
4. PERNYATAAN PERATURAN	8
5. PANDUAN PENGGUNAAN E-MEL	9
6. MENYEDIA DAN MENYUNTING MEL	9
7. MENGHANTAR E-MEL	9
8. MENJADI AHLI DALAM AKAUN E-MEL KUMPULAN	10

### D. Peraturan Pengisian Kandungan dan Penerbitan dalam Laman Web

1. PENGENALAN	12
2. TUJUAN PERATURAN	12
3. SKOP PERATURAN	12
4. PERNYATAAN PERATURAN	12
4.1 PENGISIAN KANDUNGAN LAMAN WEB UTM	12
4.2 REKABENTUK LAMAN WEB	13
4.3 VERSI BAHASA	13

4.4	KEMUDAHAN INTERAKSI / PAUTAN DAN CARIAN	13
4.5	SPESIFIKASI LAMAN WEB	13
4.6	NAMA-NAMA DOMAIN DAN <i>UNIFORM RESOURCE LOCATOR</i> (URL)	14
4.7	PENGIKLANAN	14
4.8	KEBOLEHCAPAIAN WEB	15
5.	PERNYATAAN PANDUAN	15
5.1	ISI KANDUNGAN LAMAN WEB	15
5.2	REKA BENTUK LAMAN WEB	16
5.3	KEMUDAHAN INTERAKSI/ PAUTAN DAN CARIAN	16
5.4	SPESIFIKASI LAMAN WEB	16
5.5	ENJIN PENCARIAN OPTIMA - SEO	16
5.6	<i>BROWSERS</i>	18

### **E. Peraturan Pengagihan Komputer Kepada Staf**

1.	PENGENALAN	20
2.	TUJUAN PERATURAN	20
3.	SKOP PERATURAN	20
4.	PERATURAN PENGAGIHAN KOMPUTER KEPADA STAF	20
5.	PENGAGIHAN SEMULA KOMPUTER KEPADA STAF	21

### **F. Peraturan Penggunaan Makmal Komputer**

1.	PENGENALAN	23
2.	TUJUAN PERATURAN	23
3.	SKOP PERATURAN	23
4.	PERATURAN WAKTU PENGGUNAAN MAKMAL KOMPUTER	23
5.	PENEMPAHAN PENGGUNAAN MAKMAL KOMPUTER	23
6.	PERATURAN SEBELUM MEMASUKI MAKMAL KOMPUTER	23
7.	PERATURAN KETIKABERADA DI DALAM MAKMAL KOMPUTER	23
8.	TATACARA BERPAKAIAN	24
9.	KEBERSIHAN DAN KECERIAAN MAKMAL KOMPUTER	24
10.	PEMATUHAN PANDUAN KETIKA KECEMASAN	24
11.	PANDUAN WAKTU PENGGUNAAN MAKMAL KOMPUTER	24
12.	PENEMPAHAN PENGGUNAAN MAKMAL KOMPUTER	24
13.	PENGGUNAAN MAKMAL KOMPUTER	24
14.	KEBERSIHAN DAN KECERIAAN MAKMAL KOMPUTER	24

### **G. Peraturan Peminjaman Peralatan ICT**

1.	PENGENALAN	26
2.	TUJUAN PERATURAN	26
3.	SKOP PERATURAN	26
4.	PERNYATAAN PERATURAN	26
5.	PERNYATAAN PANDUAN	27

# Isi Kandungan

---

## H. Peraturan Pelupusan Peralatan ICT

1. PENGENALAN	29
2. TUJUAN PERATURAN	29
3. SKOP PERATURAN	29
4. PERATURAN PELUPUSAN PERALATAN ICT	29
5. PERNYATAAN PANDUAN	29

## I. Peraturan Keselamatan ICT

1. PENGENALAN	31
2. TUJUAN PERATURAN	31
3. SKOP PERATURAN	31
4. PERATURAN KESELAMATAN KAWALAN CAPAIAN FIZIKAL	31
5. PERATURAN KESELAMATAN KAWALAN CAPAIAN LOGIKAL	31
6. PERATURAN KESELAMATAN IDENTIFIKASI PENGGUNA	31
7. JEJAK AUDIT	32
8. MAKLUMAT SANDAR	32
9. PENYENGGARAAN	33
10. KESELAMATAN SISTEM APLIKASI	33
11. PERISIAN APLIKASI	33
12. PANGKALAN DATA	33
13. PENGUJIAN APLIKASI	33
14. PERISIAN BERKOD HASAD DAN CACAT	33
14. PERISIAN BERKOD HASAD DAN CACAT	34
15. PERUBAHAN VERSI	34
16. PENYIMPANAN KOD SUMBER	34
17. PERISIAN TIDAK BERLESEN	34
18. KAWALAN KOD HASAD(MALICIOUS CODE)	34
19. KESELAMATAN PENGGUNAAN E-MEL	34
20. KESELAMATAN PERALATAN RANGKAIAN	34
21. KESELAMATAN FIZIKAL	35
22. KESELAMATAN CAPAIAN FIZIKAL	35
23. KESELAMATAN CAPAIAN PERALATAN RANGKAIAN	35
24. KESELAMATAN CAPAIAN LOGIKAL	35
25. PENGGUNAAN PERALATAN TANPA KEBENARAN	35
26. KONFIGURASI PERALATAN	35
27. PENYELENGGARAAN PERALATAN	35
28. KEBOLEHCAPAIAN PENGGUNA MELAKUKAN PENGINTIPAN DATA RANGKAIAN UNIVERSITI	36
29. PROTOKOL RANGKAIAN YANG TIDAK DIGALAKKAN	36
30. FIREWALL	36

## Istilah

---

### BAHASA INGGERIS

Accessibility

Attachment

Back up Data

Defective

Disclaimer

Group e-mail

Internet Protocol

Junk or spam e-mail

Malicious

Malicious Code

Penggunaan *Incidental*

Privacy

Social network

Uniform Resource Locator (URL )

User Accessibility

Worm

### BAHASA MALAYSIA

Kebolehcapaian

Kepilan

Data Sandar

Cacat

Penafian

Akaun e-mel Kumpulan

IP

E-mail remeh

Perisian Berkod hasad

Kawalan Kod Hasad

Penggunaan sumber-sumber  
Universiti bagi selain tujuan rasmi

Hak Milik Peribadi

Rangkaian sosial

Pengenalan capaian

Kebolehcapaian Pengguna

Cecacing

## Takrifan

---

### **Akaun e-mel individu**

Akaun e-mel perseorangan yang menggunakan domain utm.my (contoh: aziz@utm.my).

### **Akaun e-mel kumpulan**

Akaun e-mel domain utm.my yang merujuk kepada sekelompok akaun khusus (contoh: rmc.rnd.net@groups.utm.my).

### **Akaun e-mel pentadbiran**

Akaun e-mel domain utm.my yang diberi kepada penjawat jawatan tertentu seperti dekan dan timbalan pendaftar (contoh: dekanfsksm@utm.my).

### **Aplikasi**

Aturcara atau program yang dibangunkan untuk melaksanakan tugas tertentu oleh komputer seperti Sistem Maklumat Kewangan dan Sistem Maklumat Akademik.

### **Bandwidth**

Keupayaan untuk pemindahan data pada satu sistem komunikasi elektronik

### **Cecacing**

Program yang berupaya membiakkan dirinya sendiri dalam sesebuah sistem komputer dan berupaya mengakibatkan kesesakan trafik internet dan pertambahan beban pengoperasian.

### **Chat Room**

Ruang sembang secara siber.

### **Cracked games**

Perisian komersial yang telah dicetak rompak dan diedarkan tanpa kebenaran pemilik sebenar.

### **Data Sandar**

Sandaran merujuk kepada salinan-salinan data yang dibuat supaya salinan-salinan tambahan ini boleh diguna untuk pemulihan apabila masalah berlaku terhadap data asal.

### **Domain**

Nama yang didaftarkan untuk kegunaan sistem rangkaian komputer.

### **E-mel bom**

Penghantaran mel secara bertalu-talu yang menyebabkan kotak masuk penerima atau pelayan mel menjadi penuh sehingga tidak boleh berfungsi dengan baik.

### **E-mel remeh**

E-mel serupa yang dihantar oleh sumber yang tidak dikenali mahupun diundang dan selalunya mempunyai unsur pengiklanan.

### **Gator**

Syarikat yang kini dikenali sebagai Claria Corporation yang menyediakan aplikasi yang menyediakan pengiklanan internet mengikut tabiat pengguna.

### **Hotbar & Searchbar**

Program yang menempatkan dirinya di bahagian atas tettingkap pelayan Internet Explorer. Program ini memantau maklumat mengenai laman web yang pernah dikunjungi oleh pengguna dan menyimpan sejarah data yang pernah dicari menggunakan enjin carian.

### **Insiden**

Satu kejadian atau keadaan lazim yang menyebabkan gangguan kepada perkhidmatan ICT.

### **IP**

Internet Protokol (IP) adalah satu protokol, yang digunakan untuk perhubungan data merentasi rangkaian internet menggunakan Set Keluarga Protokol Internet. Nombor IP pula adalah nombor unik yang ditetapkan bagi peranti perhubungan. Contoh nombor IP ialah 10.50.83.112.

### **Jejak Audit**

Satu jejak audit adalah satu urutan kronologi rekod-rekod audit. Setiap satu mengandungi bukti secara langsung dan berkaitan dengan hasil dari pelaksanaan satu proses perniagaan atau fungsi sistem.

### **Kebolehcapaian internet**

Merujuk kepada kualiti pencapaian terhadap sesuatu perkhidmatan sama ada tidak boleh dicapai langsung, lembab atau laju.

### **Kebolehsediaan**

Ukuran sesuatu alat atau sistem untuk beroperasi mengikut spesifikasi fungsi yang ditetapkan.

### **Kemudahan ICT**

Termasuk, tetapi tidak terhad kepada komputer peribadi, terminal, sistem komputer, alat-alat pingiran 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 universiti.

## **Kepilang**

Sebarang fail elektronik yang dikepilkan bersama-sama e-mel.

## **Kod hasad**

Program seperti virus, cecacing dan Trojan Horse yang menjalankan proses-proses tidak sah terhadap komputer atau rangkaian

## **Komunikasi**

Aktiviti penyampaian data dan maklumat di antara individu atau kumpulan melalui media elektronik.

## **Laman utama**

Merujuk kepada muka hadapan setiap laman web universiti.

## **Laman web**

Satu lokasi di World Wide Web. Setiap laman web memiliki laman utama, iaitu dokumen pertama yang dipaparkan kepada pengguna apabila berkunjung ke sesebuah laman web.

## **Laman web universiti**

Meliputi laman web universiti, fakulti, pusat, jabatan, unit, persatuan, (kecuali laman web Individu) yang diletakkan di bawah nama domain .utm.my dan mana-mana domain yang diiktiraf oleh jawatankuasa yang dilantik oleh universiti.

## **List**

Direktori pengguna internet yang disimpan bagi tujuan komunikasi dalam internet.

## **Makmal komputer**

Adalah fasiliti yang disediakan oleh universiti bagi menyokong aktiviti pentadbiran, pendidikan, pembangunan dan penyelidikan(R & D) / dan perkhidmatan. Penggunaan makmal komputer merangkumi aktiviti yang dilakukan di dalam makmal ataupun secara atas talian terus ke makmal.

## **Malware & Malicious Codes**

Singkatan kepada malicious software, iaitu perisian atau keratan kod yang direka khusus untuk mengganggu operasi sesebuah sistem komputer. Contoh malware ialah Trojan Horse, spyware, adware dan cecacing.

## **Metadata**

Maklumat berkaitan muka laman web yang terkandung di dalam permulaan aturcara laman web.

## **Moderator**

Salah seorang ahli dalam akaun e-mel kumpulan yang dipertanggungjawabkan untuk mengurus akaun tersebut.

## **Pelajar**

Seseorang yang mendaftar sesuatu program akademik (sama ada penuh atau separuh masa atau siswazah) di universiti dan statusnya masih aktif.

## **Peminjaman Peralatan ICT**

Proses memberi atau membekalkan peralatan ICT di dalam tempoh yang ditetapkan melalui proses permohonan yang sah.

## **Penafian UTM**

Pernyataan yang menafi tanggungjawab dan menolak tuntutan oleh individu atau organisasi luar kepada UTM terhadap sesuatu perkara seperti yang mungkin terjadi ekoran daripada penggunaan e-mel UTM.

## **Pengguna**

Seseorang atau kumpulan orang yang dibenarkan menggunakan kemudahan ICT universiti.

## **Penggunaan Incidental**

"Penggunaan Incidental" adalah penggunaan sumber-sumber universiti bagi selain tujuan rasmi itu berbanding dengan "Penggunaan Rasmi" di mana penggunaan adalah secara langsung bagi menjalankan misi universiti

## **Pentadbir e-mel UTM**

Seseorang staf CICT atau yang dilantik oleh fakulti, unit yang ditugaskan untuk mengurus tadbir sistem.

## **Pentadbir Laman Web Universiti**

Merujuk kepada pegawai yang dilantik secara rasmi oleh Universiti atau fakulti, bahagian untuk menguruskan laman web.

## **Peralatan rangkaian**

Peralatan dan komponen yang digunakan dalam sistem rangkaian seperti swis, hub dan router dan sebagainya

## **Perisian**

Atur cara atau program komputer yang digunakan untuk melaksanakan tugas tertentu seperti perisian automasi pejabat dan grafik.

## **Perkakasan**

Peralatan dan komponen ICT seperti komputer dan pencetak.

# Polisi & Peraturan

Teknologi Maklumat & Telekomunikasi (ICT)

---

## Rangkaian sosial

Satu jaringan antara sekelompok manusia yang berinteraksi secara langsung atau tidak langsung. Jaringan ini berlaku melalui sistem seperti friendster dan seumpamanya.

## Sebaran

Kaedah yang membolehkan data digital, maklumat atau informasi dikongsi dan diakses oleh pengguna lain menggunakan media elektronik.

## Tandatangan

Kemudahan fitur tandatangan yang terdapat pada perkhidmatan e-mel yang membenarkan pengguna e-mel menulis nama dan alamatnya pada setiap e-mel yang dihantar.

## Spyware dan Adware

Perisian yang mengumpulkan maklumat pengguna melalui sambungan internet tanpa pengetahuan pengguna bagi tujuan pengiklanan menggunakan mesej pop.

## Staf

Seseorang yang dilantik oleh universiti untuk sesuatu jawatan sama ada secara tetap, sambilan, sementara atau kontrak dan masih berkhidmat dengan universiti.

## Storan

Penyimpanan data atau maklumat dalam apa apa jenis fail (teks, suara, foto, perisian ) bagi tujuan pemuliharaan digital dan perkongsian

## Super user

Super user atau pengguna super (juga disebut pengguna akar - root user) adalah seseorang pengguna yang mempunyai akses terhadap akaun sistem dan dengan akaun ini pengguna tersebut dapat melakukan sebarang perubahan pentadbiran pada sistem tanpa sekatan di samping boleh mengubah konfigurasi sistem.

## Thumb drive

Sejenis storan luaran yang memiliki saiz fizikal cakera keras dan disambungkan ke komputer melalui sambungan USB.

## Transaksi komersial

Satu transaksi kewangan melibatkan satu perubahan dalam status kewangan bagi dua atau lebih individu atau perniagaan.

## Trojan

Malware yang merupakan program yang kelihatan seperti tidak merbahaya tetapi berupaya diam dan tanpa disedari mendatangkan kemudahan kepada komputer secara senyap.

## URL

Universal Resource Locator - merupakan pengenalan atau penanda untuk capaian sesuatu lokasi laman web.

## Virus

Program atau kod yang dimasukkan ke dalam sesebuah komputer tanpa pengetahuan pemilik komputer dan melaksanakan operasi komputer tanpa kebenaran.

## Waktu beban puncak

Waktu dan tempoh capaian ke internet yang tinggi dan boleh menjejaskan penggunaan ICT untuk tujuan pengurusan dan pentadbiran universiti. Waktu beban puncak di universiti ditetapkan antara 8:00 pagi hingga 5.00 petang.





## **A. Polisi Teknologi Maklumat dan Komunikasi (ICT)**



## A. Polisi Teknologi Maklumat dan Komunikasi (ICT)

### 1. PENGENALAN

Perkhidmatan Teknologi Maklumat dan Komunikasi (ICT) di Universiti Teknologi Malaysia (UTM) bertujuan membantu universiti ke arah mencapai visi dan misi selaras dengan matlamat pembangunan dan kemajuan negara serta kelestarian sejagat. Dalam usaha mencapai hasrat tersebut, Pihak univesiti menyediakan perkhidmatan ICT kepada warga kampus bagi meningkatkan kualiti pengajaran, pembelajaran, aktiviti penyelidikan dan perundingan serta tadbir urus universiti.

Polisi ICT dilaksanakan kepada seluruh masyarakat UTM supaya mereka dapat menggunakan ICT dengan lebih teratur dan mengikut peraturan.

Lapan peraturan dalam polisi ICT yang telah di persetujui adalah:

- 1.1. Peraturan Penggunaan internet
- 1.2. Peraturan Penggunaan Emel
- 1.3. Peraturan Pengisian Kandungan dan Penerbitan Dalam Laman Web
- 1.4. Peraturan Pengagihan Komputer Kepada Staf
- 1.5. Peraturan Penggunaan Makmal Komputer
- 1.6. Peraturan Peminjaman Peralatan ICT
- 1.7. Peraturan Pelupusan Peralatan ICT
- 1.8. Peraturan Keselamatan ICT

### 2. TUJUAN

Tujuan polisi ICT adalah untuk menggaris dan menetapkan peraturan penggunaan ICT di universiti. Polisi ini juga bertujuan untuk melindungi pihak universiti dari menghadapi sebarang implikasi perundangan serta mendidik warga kampus agar mereka mempunyai kesedaran sosial dan tanggungjawab intelektual ke atas penggunaan ICT. Selain itu, polisi ini juga bertujuan memastikan kebolehsediaan, integriti dan kerahsiaan perkhidmatan ICT di UTM tercapai.

### 3. SASARAN

Perkhidmatan ICT UTM adalah diberikan kepada semua warga kampus yang layak dan berdaftar. Perkhidmatan ini juga boleh diberikan kepada tetamu universiti yang dibenarkan.

### 4. KAEDAH PENGGUNAAN ICT

Warga kampus boleh menggunakan perkhidmatan ICT menerusi pelbagai bentuk capaian yang ditetapkan oleh pihak universiti.

### 5. PELAKSANAAN

Polisi penggunaan internet dan e-mel yang telah dibangunkan pada 2008 telah di tambahbaik dan dibawa untuk kelulusan bagi pelaksanaan pada Jun 2009.

### 6. TEMPAT PENGGUNAAN PERKHIDMATAN ICT

Warga kampus boleh menggunakan kemudahan perkhidmatan ICT yang terdapat di fakulti, pejabat pentadbiran, kolej kediaman serta lokasi-lokasi lain yang ditetapkan oleh pihak universiti.

### 7. HAK MILIK

Segala fail elektronik yang dihasilkan, dicetak, dihantar dan diterima atau disimpan pada komputer yang dimiliki, disewa atau ditadbir urus dibawah pengurusan dan pengawalan pihak UTM adalah menjadi hak milik UTM. Hak milik yang di tuntutan oleh UTM tidak termasuk hak milik harta intelek kepunyaan pemilik.

## **8. HAK MILIK PERIBADI**

Penggunaan dan proses sistem sumber ICT yang digunakan oleh individu termasuk e-mel, blog, fail elektronik dan lain-lain jaringan elektronik sosial yang dicipta seperti *myspace*, *facebook*, *youtube* dan seumpamanya yang dimuat turun, disimpan, diterima dalam sistem komputernya bukanlah merupakan hak milik individu. Segala maklumat yang telah dihasilkan boleh dicapai sekiranya perlu untuk tujuan pengurusan dan penyelenggaraan sistem maklumat, penyelesaian masalah teknikal, kawalan keselamatan sistem, kajian semula pentadbiran serta keakuran arahan mahkamah, sistem auditan dalaman atau mana-mana sistem audit dan lain-lain polisi berkaitan.

## **9. PENGGUNAAN INCIDENTAL**

Penggunaan capaian internet secara peribadi yang dicapai dari dalam atau luar universiti adalah dihadkan kepada pengguna yang berdaftar sahaja. Penggunaan ini tidak termasuk kepada ahli keluarga dan pihak-pihak lain yang berkaitan.

- 9.1. Penggunaan *incidental* tidak boleh menyebabkan peningkatan kos tambahan kepada universiti
- 9.2. Penggunaan *incidental* tidak boleh mengganggu prestasi tugas dan prestasi pengguna.
- 9.3. Memastikan tidak ada fail atau dokumen yang dihantar atau diterima boleh menyebabkan bebanan perundangan atau mencemarkan imej dan nama baik Universiti.
- 9.4. Storan fail atau dokumen elektronik yang disimpan dalam sistem ICT universiti mestilah dalam saiz yang seminima mungkin.
- 9.5. Segala fail dan dokumen termasuk fail dan dokumen rasmi peribadi pengguna adalah kepunyaan UTM dan boleh dicapai berdasarkan kepada kehendak dan peraturan universiti.

## **10. TINDAKAN TATATERTIB**

Perlanggaran polisi ini boleh mengakibatkan tindakan disiplin diambil terhadap pelajar dan staf. Mereka boleh dihalang daripada mendapat kemudahan ICT yang disediakan. Pelajar yang melanggar polisi ini boleh dikenakan tindakan tatatertib di bawah Kaedah-kaedah Universiti Teknologi Malaysia (Tatatertib Pelajar-pelajar, 1999). Staf tetap universiti boleh dikenakan tindakan termasuk tindakan tatatertib di bawah Akta Badan-badan Berkanun (Tatatertib dan Surcaj) 2000 (Akta 605) atau mana-mana akta yang berkaitan ;

- 9.1. Perlembagaan Universiti Teknologi Malaysia - S6(1)®
- 9.2. Akta Rahsia Rasmi 1972 – S8
- 9.3. Akta Akta Komunikasi dan Multimedia 1998
- 9.4. Akta Jenayah Komputer 1997
- 9.5. Pengubahsuaian Tanpa Kuasa – S5
- 9.6. Komunikasi Salah – S6
- 9.7. Perubahatan dan Percubaan – S7
- 9.8. Akta Teleperubatan
- 9.9. Akta Tandatangan Digital 1997

Staf Kontrak, Sementara dan Sambilan pula boleh dikenakan tindakan yang sewajarnya termasuklah diberhentikan kerja.

A decorative graphic on the left side of the slide, featuring a globe at the bottom left, several interlocking gears of different sizes and colors (blue, red, white) in the upper left, and a control panel with various buttons and screens in the lower left. The background of the graphic is a light blue gradient.

## **B. Peraturan Penggunaan Internet**



## B. Peraturan Penggunaan Internet

### 1. PENGENALAN

Internet merupakan rangkaian komuniti global yang membenarkan sesiapa sahaja untuk berkongsi maklumat dan berinteraksi antara satu sama lain. Perkhidmatan internet yang disediakan di universiti digunakan oleh para staf dan pelajar dalam aktiviti harian dan ia merupakan salah satu platform untuk berkomunikasi dengan pihak luar. Komunikasi secara elektronik dilihat sebagai salah satu saluran penting dalam membantu mewujudkan perkongsian maklumat. Dengan adanya peraturan penggunaan internet ini, risiko gangguan operasi internet di universiti dapat dikurangkan.

Peraturan ini mengguna pakai **Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 2003; Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan**, sebagai sumber asas dan disesuaikan untuk penggunaan di universiti.

### 2. TUJUAN PERATURAN

Tujuan peraturan ini diadakan untuk:

- 2.1. Menyokong dan menjayakan visi dan misi universiti.
- 2.2. Menerang tatacara penggunaan internet yang disediakan oleh universiti.
- 2.3. Meningkatkan tahap keselamatan dokumen rasmi dalam persekitaran internet.
- 2.4. Memastikan penggunaan internet yang teratur dan terkawal oleh warga universiti.
- 2.5. Mengurangkan risiko gangguan operasi internet.

### 3. SKOP PERATURAN

Peraturan ini merangkumi penggunaan perkhidmatan internet yang disediakan oleh pihak universiti.

### 4. PERNYATAAN PERATURAN

- 4.1. Penggunaan internet adalah untuk tujuan menyokong misi asas universiti dalam pengajaran, pembelajaran, penyelidikan dan perundingan.
- 4.2. Penggunaan internet bagi tujuan yang disebut di atas mestilah menghormati hak cipta, harta intelek dan hak persendirian pengguna lain.
- 4.3. Penggunaan internet oleh warga universiti adalah satu keistimewaan dan bukan satu hak mutlak.
- 4.4. Penggunaan internet untuk akademik dan pentadbiran diberi keutamaan pada waktu beban puncak berbanding penggunaannya di kolej kediaman pelajar.
- 4.5. Pengguna internet bertanggungjawab memastikan integriti dan keselamatan ke atas pengenalan diri (ID) dan kata laluan semasa mengakses rangkaian dan sistem-sistem di universiti.
- 4.6. Penggunaan internet oleh warga universiti hendaklah tidak mengganggu kebolehcapaian dan keboleharapan prasarana ICT. Aktiviti memuat naik/turun data bersaiz besar yang memonopoli *bandwidth* dalam bentuk P2P dan seumpamanya dianggap mengganggu kebolehcapaian dan keboleharapan prasarana ICT.
- 4.7. Pihak universiti berhak memastikan penggunaan sebarang aplikasi atas talian yang memerlukan sumber yang tinggi seperti aplikasi *video streaming* tidak mengganggu kebolehcapaian dan keboleharapan prasarana ICT universiti.
- 4.8. Pengguna adalah bertanggungjawab ke atas maklumat yang disebar dengan memastikan kesahihan maklumat tersebut serta mendapatkan pengesahan atau keizinan dari pada pemiliknya.
- 4.9. Pengguna bertanggungjawab memastikan peranti yang mencapai internet adalah bebas dari kod hasad seperti *spyware*, *adware* dan *virus*.
- 4.10. Penggunaan internet bagi sebarang transaksi komersial adalah tidak dibenarkan. Sekiranya pengguna didapati melakukan transaksi tersebut untuk kepentingan peribadi maka pihak universiti boleh mengambil tindakan yang sewajarnya dan tidak akan bertanggungjawab sekiranya berlaku kerugian, kehilangan dan kerosakan di pihak pengguna.

- 4.11. Pengguna yang mencapai sesuatu perkhidmatan yang memerlukan pembayaran dalam bentuk urusniaga elektronik dan menggunakan kad kredit, *Paypal* (dan seumpamanya) atau perbankan atas talian adalah bertanggungjawab ke atas setiap transaksi yang dilakukan.
- 4.12. Setiap pengguna hendaklah memaklumkan kepada Pusat Teknologi Maklumat dan Komunikasi (CICT) sekiranya mengetahui atau mengesyaki berlakunya insiden yang boleh menggugat keselamatan komunikasi universiti.
- 4.13. Penyebaran dan memuat turun bahan-bahan pornografi, berunsur lucah, fitnah, ugutan dan bebaur politik adalah dilarang sama sekali.
- 4.14. Pihak universiti berhak menarik balik keistimewaan kemudahan internet apabila berlaku pelanggaran peraturan dan polisi yang ditetapkan.
- 4.15. Pihak universiti berhak merujuk kepada pihak berkuasa berkaitan untuk mendapatkan nasihat berkaitan tindakan yang wajar bagi memastikan pelanggaran peraturan dan polisi tidak berulang.

## 5. PERNYATAAN PANDUAN

- 5.1. Aktiviti pengajaran dan pembelajaran adalah merujuk kepada Polisi Pengajaran dan Pembelajaran Universiti 2007.
- 5.2. Aktiviti penyelidikan adalah merujuk kepada Polisi Penyelidikan Universiti 2008.
- 5.3. Aktiviti perundingan adalah merujuk kepada Polisi Perundingan Universiti 2008.
- 5.4. Pengguna harus menggunakan kemudahan kata laluan untuk *screen saver* atau log keluar apabila hendak meninggalkan komputer.
- 5.5. *Chatting, forum, Instant Messenger* dan teknologi berkaitan penggunaan internet untuk komunikasi adalah terhad kepada tujuan pengajaran, pembelajaran, penyelidikan, pengurusan dan pentadbiran.
- 5.6. Bagi memastikan kebolehsediaan *bandwidth* kepada setiap warga universiti, pihak universiti berhak menetapkan nilai maksima muat turun dan muat naik yang bersesuaian dari masa ke semasa.
- 5.7. Penyimpanan data dalam storan yang disediakan oleh universiti adalah terhad kepada tujuan pengajaran, pembelajaran, penyelidikan, penerbitan, penulisan, perundingan dan aktiviti sokongan yang berkaitan.
- 5.8. Penyebaran dan penyimpanan, muat turun, muat naik bahan-bahan pornografi, berunsur lucah, fitnah, ugutan, perniagaan dan bebaur politik adalah dilarang sama sekali.
- 5.9. Hak cipta dan harta intelek adalah merujuk kepada Polisi IP Universiti 1999.
- 5.10. Aktiviti penggodaman, pengimbasan, penyelusuran sistem, *phishing* dan *decrypt* data secara tidak sah di dalam dan di luar Universiti adalah melanggar privasi dan dilarang sama sekali.
- 5.11. Pengguna yang dipertanggungjawab untuk memuat naik dan menyebarkan maklumat perlu terlebih dahulu mendapatkan pengesahan kesahihan dan kekinian maklumat serta mendapatkan keizinan untuk penyebaran.
- 5.12. Pengguna adalah dimestikan mematuhi Peraturan Keselamatan ICT Universiti semasa dalam menetap dan menguruskan ID dan kata laluan pengguna.
- 5.13. Pengguna bertanggungjawab memasang sistem pengoperasian dan aplikasi yang tulen dan sentiasa dikemaskini pada peranti yang digunakan. Pihak universiti tidak akan bertanggungjawab sekiranya berlaku sebarang implikasi perundangan sekiranya pengguna memasang sistem pengoperasian dan aplikasi cetak rompak.
- 5.14. Pengguna bertanggungjawab memasang perisian nyah-kod hasad seperti antivirus, *anti-spam, anti-spyware* dan *anti-adsware* serta sentiasa mengemaskini perisian tersebut.
- 5.15. Pengguna bertanggungjawab membuat imbasan ke atas peranti dengan perisian nyah-kod hasad sekurang-kurangnya sekali dalam masa sehari.
- 5.16. Pengguna dinasihatkan untuk memastikan peranti diletakkan di tempat yang mempunyai kawalan fizikal yang selamat daripada penceroboh atau sebarang bentuk capaian tidak sah.
- 5.17. Pengguna tidak dibenarkan untuk memasang sebarang perisian berunsur perjudian, permainan, *hotbar, searchbar, gator* atau melayari laman-laman web yang terlarang seperti *cracked games*, permainan atas talian dan lain-lain di komputer hak milik universiti.
- 5.18. Sebarang iklan komersil yang ditawarkan oleh pengguna menerusi enjin carian seperti *Google Adsense* adalah tidak dibenarkan sama sekali.



## **C. Peraturan Penggunaan E-mel**



## C. Peraturan Penggunaan E-mel

### 1. PENGENALAN

E-mel adalah salah satu perkhidmatan yang disediakan dalam internet dan sering digunakan pada masa kini. Aplikasi e-mel digunakan secara meluas dan ia membenarkan komunikasi pelbagai hala dengan cara yang pantas. Aplikasi e-mel lebih sesuai untuk penulisan yang ringkas. Setiap staf dan pelajar universiti diberikan alamat e-mel universiti masing-masing dan mereka perlu menggunakan kemudahan ini secara aktif.

Peraturan ini menggunakan pakai **Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 2003; Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan** sebagai sumber asas dan disesuaikan untuk penggunaan di universiti.

### 2. TUJUAN PERATURAN

Tujuan peraturan ini diadakan untuk:

- 2.1. Menerangkan peraturan dan etika penggunaan e-mel di universiti.
- 2.2. Menggariskan cara penggunaan e-mel yang berhemah dan selamat agar kemudahan yang disediakan dapat dimanfaatkan dengan sepenuhnya oleh semua staf dan pelajar.
- 2.3. Mengurangkan risiko gangguan operasi internet dan e-mel.

### 3. SKOP PERATURAN

Peraturan ini adalah untuk semua staf, pelajar dan mereka yang dibenarkan menggunakan kemudahan e-mel universiti (contoh, Siswa Mail, Webmail UTM, e-mel fakulti). Peraturan ini meliputi tiga jenis akaun iaitu:

- 3.1. Akaun e-mel individu
- 3.2. Akaun e-mail pentadbiran
- 3.3. Akaun e-mel kumpulan

### 4. PERNYATAAN PERATURAN

- 4.1. Semua akaun e-mel universiti adalah hak universiti.
- 4.2. Kerja-kerja rasmi yang boleh dilakukan melalui internet hendaklah menggunakan perkhidmatan e-mel universiti dan ia mestilah selaras dengan peraturan-peraturan urusan rasmi Kerajaan yang sedia ada.
- 4.3. Pengguna adalah dilarang menyalahguna kemudahan e-mel untuk tujuan menghasut, memfitnah, menghantar berita palsu, menyebarkan semula hak cipta terpelihara atau aktiviti-aktiviti lain yang ditegah oleh undang-undang siber.
- 4.4. E-mel urusan rasmi yang bersifat Terhad, Sulit, Rahsia atau Rahsia Besar mesti diberi perlindungan untuk kepentingan keselamatan.
- 4.5. Penggunaan bahasa kurang sopan dan terlampau dalam penulisan e-mel rasmi universiti adalah dilarang sama sekali.
- 4.6. Pengguna akaun e-mel universiti adalah bertanggungjawab ke atas akaun mereka yang merangkumi kandungan, penyelenggaraan kotak e-mel dan keselamatan e-mel.
- 4.7. Setiap e-mel yang dihantar mestilah mempunyai disclaimer universiti dan tandatangan rasmi penghantar e-mel tersebut di akhir e-mel.
- 4.8. Pengguna dilarang membenarkan pihak ketiga untuk menjawab e-mel kepada penghantar asal bagi pihaknya.
- 4.9. Kemudahan akaun e-mel universiti boleh ditarik balik pada bila-bila masa jika penggunaannya melanggar Peraturan Penggunaan E-mel universiti.
- 4.10. Penubuhan sesuatu akaun e-mel kumpulan perlulah dilakukan secara rasmi di peringkat universiti dan ditadbir oleh seorang moderator.



## **5. PANDUAN PENGGUNAAN E-MEL**

- 5.1. Penggunaan e-mel universiti untuk tujuan-tujuan berikut adalah dilarang:
  - 5.1.1 Kegiatan yang menyalahi undang-undang negara.
  - 5.1.2 Urusan-urusan yang tidak selaras dengan dasar dan peraturan kerajaan.
  - 5.1.3 Tujuan komersial yang tidak berkaitan dengan universiti.
  - 5.1.4 Kegiatan perniagaan peribadi.
- 5.2. Pengguna hendaklah memastikan e-mel tidak mengandungi maklumat rahsia yang boleh disalahguna dan menjejaskan imej individu, organisasi atau negara.
- 5.3. Pengguna digalakkan menggunakan kemudahan protokol seperti https untuk penghantaran e-mel yang lebih terjamin dan selamat.
- 5.4. Pengguna dinasihatkan untuk mengelak daripada menulis perkara sulit atau peribadi dalam e-mel. Jika terdapat keperluan untuk menghantar e-mel berbentuk sulit, pengguna hendaklah mengambil langkah-langkah keselamatan seperti menggunakan kemudahan encryption e-mel.
- 5.5. Pengguna mesti merahsiakan kata laluan dari pengetahuan orang lain.
- 5.6. Pengguna hendaklah sentiasa berwaspada ketika membuka akaun e-mel universiti apabila menggunakan komputer di tempat umum dengan memastikan bahawa nama pengenalan dan kata laluan tidak disimpan oleh aplikasi pelayan internet di komputer tersebut. Pastikan pengguna telah log keluar setelah menggunakannya.
- 5.7. Pengguna hendaklah menghubungi pentadbir e-mel universiti dengan segera jika mengesan atau mengesyaki akaun atau alamat e-mel universiti telah disalahgunakan oleh orang lain atau berlakunya kes penyamaran alamat e-mel universiti.
- 5.8. Pengguna hendaklah bertanggungjawab untuk memaklumkan kepada Pentadbir e-mel universiti sekiranya berada di luar pejabat dalam tempoh waktu yang panjang, bercuti atau bertukar tempat kerja bagi memudahkan penyelenggaraan dilakukan.
- 5.9. Pengguna harus mengehadkan jumlah e-mel yang disimpan dalam kotak mel supaya sesuai dengan kemampuan saiz kuota yang diberikan oleh Pentadbir e-mel universiti. Hapuskan e-mel yang tidak perlukan.
- 5.10. Pengguna bertanggungjawab mengadakan salinan atau penduaan pada media storan kedua elektronik seperti disket dan sebagainya bagi tujuan keselamatan.
- 5.11. Pengguna boleh mendapatkan disclaimer universiti daripada pentadbir e-mel universiti.

## **6. MENYEDIA DAN MENYUNTING MEL**

- 6.1. Pengguna digalakkan menulis dalam satu e-mel yang menyentuh tentang satu perkara sahaja.
- 6.2. Pengguna hendaklah memastikan tajuk dan kandungan e-mel menyentuh perkara yang sama. E-mel yang bertajuk memudahkan penerima menentukan keutamaan ke atas setiap e-mel yang masuk ke dalam kotak mel.
- 6.3. Pengguna disarankan menulis e-mel mengikut kebiasaan format menulis sebarang dokumen. Kandungan e-mel yang ditaip dalam huruf besar sepenuhnya akan dianggap sebagai mesej berbentuk amaran.
- 6.4. Pengguna digalakkan menggunakan fail kepilan semasa menyedia e-mel sekiranya maklumat yang ingin disertakan telah tersedia ada seperti melampirkan fail minit mesyuarat dalam fail format Microsoft Word.
- 6.5. Pengguna hendaklah memastikan fail yang dikepilkan bebas daripada virus.
- 6.6. Pengguna perlulah memastikan saiz fail kepilan tidak melebihi had yang diperuntukkan. Jika saiz fail kepilan terlampau besar, pecahkan fail tersebut kepada fail-fail yang bersaiz lebih kecil dan buatlah penghantaran secara berasingan atau gunakan perisian pemampatan.

## **7. MENGHANTAR E-MEL**

- 7.1. Pengguna hendaklah sentiasa berwaspada sebelum menghantar e-mel kerana e-mel yang telah dihantar sukar untuk ditarik balik.
- 7.2. Pastikan kandungan e-mel lengkap dan mencapai maksud yang dikehendaki.
- 7.3. Pastikan alamat e-mel yang hendak dihantar adalah betul. Satu alamat e-mel mungkin mewakili satu individu atau mewakili sekumpulan individu.

4. Pengguna disarankan menjawab e-mel selewat-lewatnya 4 hari dari tarikh e-mel berkenaan diterima.
5. Pengguna diingatkan tidak melibatkan diri dalam aktiviti penghantaran e-mel remeh atau e-mel bom.
6. Pengguna dinasihatkan menggunakan kemudahan yang disediakan dengan bijak:
  - 6.1.1 Salinan kepada cc - Apabila e-mel tersebut perlu dimaklumkan kepada penerima lain.
  - 6.1.2 Salinan terselindung bcc - Apabila e-mel yang dihantar disalinkan kepada pihak ketiga, tanpa diketahui oleh penerima-penerima lain. Namun pengguna dinasihatkan untuk mengelakkan penggunaan kemudahan ini atas dasar ketelusan.
  - 6.1.3 reply - Apabila menjawab e-mel kepada penghantar sahaja.
  - 6.1.4 reply all - Apabila menjawab e-mel kepada penghantar dan individu lain yang terdapat dalam ruangan salinan.
  - 6.1.5 forward - Apabila ingin memanjangkan e-mel yang diterima kepada individu lain tanpa menyunting kandungan asal e-mel.

## 8. MENJADIAHLI DALAM AKAUN E-MEL KUMPULAN

- 8.1. Pengguna boleh menyertai mana-mana akaun e-mel kumpulan yang terdapat di universiti sekiranya bersesuaian dengan tugas profesional mereka. Contoh: rangkaian akademik bagi tujuan perbincangan profesional.
- 8.2. Pengguna diingatkan untuk berhati-hati apabila mendaftar dalam sesuatu akaun e-mel kumpulan kerana ia mungkin menyebabkan kotak e-mel penuh jika tidak diurus dengan baik. Hubungi moderator akaun e-mel berkenaan jika anda ingin mengeluarkan alamat e-mel anda dari senarai mel tersebut.
- 8.3. Pengguna dinasihatkan apabila menjadi ahli dalam sesuatu akaun e-mel kumpulan, pastikan anda menjadi pemerhati untuk beberapa hari pertama. Lihat dan perhati perkara-perkara yang dibincangkan. Sekiranya berpuas hati dan berupaya menyumbang kepada sesi perbincangan, maka bolehlah pengguna mengambil bahagian dalam perbincangan tersebut.
- 8.4. Pengguna disarankan apabila seseorang menawarkan sesuatu perkhidmatan atau memohon nasihat, jawablah dengan tertib dan jujur. E-mel komen peribadi hendaklah dihantar kepada penerimanya sahaja dan tidak harus dihantar atau disalin kepada senarai mel atau kumpulan perbincangan.
- 8.5. Pengguna diingat bahawa tidak semua ahli dalam kumpulan perbincangan mempunyai kepakaran, pendekatan dan pendapat yang sama. Oleh yang demikian, gunakan sumber rujukan untuk menerangkan sesuatu yang pada anggapan anda sukar difahami atau diterima oleh ahli lain.
- 8.6. Pengguna dinasihatkan untuk membuat pertanyaan atau komen yang berkaitan dengan kumpulan itu sahaja. Jika ada ahli yang menimbulkan masalah seperti menghantar maklumat yang tidak wajar, jawab dengan tertib dan elakkan daripada bertelagah.



## **D. Peraturan Pengisian Kandungan dan Penerbitan dalam Laman Web**



## D. Peraturan Pengisian Kandungan dan Penerbitan dalam Laman Web

### 1. PENGENALAN

Kandungan laman web universiti adalah penting bagi tujuan menyampai dan menyebarkan maklumat-maklumat, aktiviti-aktiviti terkini, pemasaran serta penjenamaan khususnya kepada seluruh warga universiti dan amnya kepada pengguna lain. Susun atur kandungan laman web yang betul dan mengikut panduan membolehkan maklumat disampaikan dengan berkesan dan bermanfaat. Pengisian dan penyenggaraan kandungan dalam laman web universiti adalah di bawah tanggungjawab pentadbir-pentadbir laman web universiti yang dilantik.

Peraturan ini mengguna pakai **Pekeliling Am Bilangan 1 Tahun 2006, Pengurusan Laman Web/Portal Sektor Awam** sebagai sumber asas dan disesuaikan untuk penggunaan di universiti.

### 2. TUJUAN PERATURAN

Tujuan peraturan ini adalah untuk:

- 2.1. Memberi panduan kepada pentadbir-pentadbir laman web universiti iaitu laman webuniversiti/ fakulti/ pusat/ jabatan/ unit/ persatuan atau sesiapa yang berkenaan dalam pengisian kandungan bagi laman web yang di bawah hakmilik Universiti Teknologi Malaysia (UTM).
- 2.2. Memastikan semua maklumat dan bahan yang diletak di laman web universiti adalah diselaras, terkawal, selamat dan menepati ciri-ciri yang dikehendaki oleh pihak pengurusan universiti.
- 2.3. Menjadi rujukan pembangunan dan penyenggaraan laman web universiti.

### 3. SKOP PERATURAN

Peraturan ini adalah diguna pakai untuk merangkumi perkara-perkara berikut:

- 3.1. Semua maklumat dan bahan yang akan atau telah dimuat dalam laman web universiti.
- 3.2. Semua laman web yang mengguna domain **utm.my** serta berada di bawah seliaan universiti seperti laman web fakulti/ pusat/ jabatan/ unit yang dikendalikan oleh pentadbir-pentadbir laman web universiti yang dilantik.
- 3.3. Pentadbir-pentadbir laman web universiti atau sesiapa yang bertanggungjawab dalam menguruskan dan memuatkan sebarang kandungan laman web yang menjadi hak milik universiti.
- 3.4. UTM berhak untuk tidak memaparkan laman-laman web yang tidak memenuhi peraturan dan spesifikasi yang telah ditetapkan.

### 4. PERNYATAAN PERATURAN

#### 4.1 PENGISIAN KANDUNGAN LAMAN WEB UTM

- 4.1.1. Isi kandungan laman web universiti adalah ditentukan oleh unit masing-masing, tetapi tertakluk kepada panduan atau arahan yang dikeluarkan oleh Universiti dari masa ke semasa.
- 4.1.2. Segala kandungan yang dimuatkan dalam laman web universiti perlu mendapat kebenaran dan kelulusan dari pihak yang bertanggungjawab.
- 4.1.3. Isi kandungan yang diletakkan dalam Laman Web Unversiti adalah tertakluk kepada peraturan dan akta berkaitan dengan hakcipta, harta intelek dan cap dagangan.
- 4.1.4. Isi kandungan laman web universiti tidak boleh mengandungi sebarang unsur-unsur yang menyalahi undang-undang universiti, negeri dan negara.
- 4.1.5. Pihak pentadbir laman web universiti dibenar untuk menukar/ mengubahsuai/ membuang kandungan laman web yang tidak sesuai bagi tujuan keberkesanan penggunaan dan keselamatan.
- 4.1.6. Pihak pentadbir laman web universiti bertanggungjawab memastikan setiap isi kandungan laman web dikemaskini mengikut keperluan semasa.
- 4.1.7. Pihak pentadbir laman web universiti yang dilantik adalah bertanggungjawab terhadap semua kandungan dan aspek keselamatan laman web.
- 4.1.8. Laman web individu yang mengunaksn domain **utm.my** bertanggungjawab ke atas laman web tersebut dan adalah tertakluk kepada peraturan ini.

- 4.1.9. Bahasa pengantar yang digunakan di muka utama laman web adalah mengikut peraturan semasa yang ditetapkan pihak universiti. Walau bagaimanapun, kemudahan untuk memilih ke bahasa-bahasa lain hendaklah disediakan di muka utama.

## **4.2 REKABENTUK LAMAN WEB**

- 4.2.1. Reka bentuk muka utama laman web setiap fakulti/ pusat/ jabatan/ unit/ persatuan hendaklah selari dengan tema dan konsep yang ditetapkan oleh Universiti.
- 4.2.2. Reka bentuk yang diguna seharusnya bercirikan mesra pengguna, menarik dan mudah dicapai.
- 4.2.3. Struktur isi kandungan setiap muka utama laman web hendaklah mengikut format yang ditetapkan oleh universiti. Walau bagaimanapun, pengembangan struktur adalah dibenarkan mengikut fungsi dan keperluan unit berkenaan.
- 4.2.4. Susun atur kandungan atau elemen dalam laman web hendaklah seragam dan konsisten untuk setiap halaman dalam laman web yang sama.

## **4.3 VERSIBAHASA**

- 4.3.1. Setiap laman web mesti mempunyai sekurang-kurangnya dua versi pilihan bahasa iaitu Bahasa Melayu dan Bahasa Inggeris.
- 4.3.2. Selain Bahasa Melayu, jika ada percanggahan terjemahan, maka versi Bahasa Inggeris adalah dirujuk.

## **4.4 KEMUDAHAN INTERAKSI/ PAUTAN DAN CARIAN**

- 4.4.1. Setiap laman web unit hendaklah menyediakan pautan ke laman web utama universiti.
- 4.4.2. Setiap pautan keluar dari laman web universiti adalah tertakluk kepada peraturan universiti dan akta-akta berkaitan.
- 4.4.3. Setiap unit hendaklah menyediakan kemudahan enjin atau sistem carian maklumat yang berkesan bagi kemudahan pengguna.

## **4.5 SPESIFIKASI LAMAN WEB**

### **4.5.1. Penetapan Identifikasi Laman Web**

- 4.5.1.1. Setiap laman web perlu mempunyai ciri identifikasi yang melambangkan unit atau isi kandungan laman web tersebut.

### **4.5.2. Penggunaan Logo**

- 4.5.2.1. Setiap muka utama laman web universiti hendaklah memaparkan logo rasmi universiti.
- 4.5.2.2. Kedudukan logo hendaklah diletakkan di kedudukan yang sama dan konsisten di antara satu halaman dengan halaman yang lain.

### **4.5.3. Aspek Tipografi**

- 4.5.3.1. Pemilihan aspek tipografi hendaklah mengambil kira kejelasan paparan dan keselesaan membaca.
- 4.5.3.2. Aspek tipografi yang digunakan juga perlu mengambilkira keperluan bagi tujuan percetakan.

### **4.5.4. Penggunaan Elemen Multimedia (Grafik, Animasi, Audio dan Video)**

- 4.5.4.1. Penggunaan sebarang sumber visual seperti gambar foto, grafik, animasi, klip video dan sebagainya hendaklah bersesuaian dari segi saiz, kebolehcapaian dan mesra pengguna.
- 4.5.4.2. Pemuatan sebarang gambar foto hendaklah dibuat dengan kebenaran individu ataupun kebenaran secara lisan atas sebab kepentingan rekod atau melibatkan aktiviti rasmi universiti.
- 4.5.4.3. Sebarang elemen audio visual yang digunakan dalam laman web universiti adalah tertakluk kepada akta hakcipta, harta intelek dan cap dagangan dan perlu mendapat kebenaran daripada pemilik asal secara sah sebelum boleh digunakan.

4.5.4.4 Sebarang pemuatan elemen multimedia ke laman web universiti tidak boleh mengandungi sebarang unsur-unsur yang menyalahi undang-undang universiti, negeri dan negara.

4.5.4.5. Sebarang pemuatan elemen multimedia ke laman web universiti tidak boleh memaparkan sebarang unsur-unsur yang menyinggung sensitiviti mana-mana individu, masyarakat, agama dan bangsa tertentu.

## 4.6 NAMA-NAMA DOMAIN DAN *UNIFORM RESOURCE LOCATOR* (URL)

4.6.1. Dasar ini menjelaskan rangka kerja bagi seni bina dan infrastruktur maklumat UTM yang berasaskan web agar dapat dipastikan pencapaian maklumat berkesan kepada pengguna yang disasar. Semua entiti universiti dikehendaki menerbitkan kandungan web mereka dengan penamaan *utm.my*. Penamaan ini dapat menyumbang penarafan web universiti.

Entiti	Penamaan URL
Fakulti, SPS, CTL, RMC, BIP, PSZ, SPACE, Pusat Kecemerlangan dan <i>Research Alliances</i>	<i>www.entity.utm.my</i> <b>Contoh</b> : <i>www.fka..utm.my</i> <i>www.pusat-kecemerlangan.utm.my</i> <i>www.cepp.utm.my</i>
Jabatan di bawah fakulti	<i>www.faculty.utm.my/jabatan</i> <b>Contoh</b> : <i>www.fsksm.utm.my/kejurteraaan-perisian</i>
Pejabat / Unit Strategik di UTM	<i>www.utm.my/pejabat</i> <b>Contoh</b> : <i>www.utm.my/ehwal-koporat</i>
Persatuan Rasmi Staf / Kelab	<i>www.utm.my/namakelab</i> <b>Contoh</b> : <i>www.utm.my/wangi</i>
Persatuan Rasmi Pelajar Kediaman Kolej / Kelab	<i>www.utm.my/namakelab</i> <b>Contoh</b> : <i>www.utm.my/utm-netball-club</i> <i>www.utm.my/Kolej-Rahman-Putra</i>
Peristiwa	<i>www.utm.my/peristiwa</i> <b>Contoh</b> : <i>www.utm.my/citra-karisma</i>

4.6.2. Gunakan huruf kecil untuk semua perkataan URL.

4.6.3. Tidak gunakan underscore pada URL tetapi gunakan tanda sengkang

**Contoh** : *www.utm.my/staff-info* tetapi bukan *www.utm.my/staff\_info*

4.6.4. Tidak menggabungkan dua perkataan menjadi satu untuk menamakan URL.

**Contoh** : *www.utm.my/corporate-affairs* tetapi bukan *www.utm.my/corporateaffairs*

4.6.5. Kolej, jabatan dan unit-unit lain di universiti hendaklah menamakan domain dengan nama yang dapat melambangkan atau yang berpadanan dengan universiti atau perkhidmatan kepada universiti.

## 4.7 PENGIKLANAN

4.7.1. Pengiklanan pihak ketiga atau promosi komersial daripada kumpulan bukan UTM/ organisasi/ individu adalah tidak dibenarkan pada mana-mana rangkaian universiti atau pada mana-mana laman web universiti.

- 4.7.2. Semua laman-laman web pengiklanan yang rasmi mesti berpandukan kepada polisi bahan-bahan hak cipta.
- 4.7.3. Sebarang jualan bahan-bahan lucah tidak dibenarkan pada mana-mana iklan di laman web universiti.

#### **4.8 KEBOLEHCAPAIAN WEB**

- 4.8.1. Perlu dipastikan laman-laman web universiti boleh dicapai dan dibaca oleh pelbagai pengguna termasuk orang kurang upaya. Kebolehcapaian laman web ini adalah penting agar semua maklumat berkenaan pengajaran dan pembelajaran dapat dicapai oleh semua. berkenaan pengajaran dan pembelajaran dapat dicapai oleh semua.

### **5. PERNYATAAN PANDUAN**

Panduan ini bertujuan untuk membantu pereka bentuk, pembangun dan pengarang kandungan dari semua tahap kemahiran mewujudkan, mengekal dan menguruskan laman-laman web yang berkualiti tinggi.

#### **5.1 ISI KANDUNGAN LAMAN WEB**

- 5.1.1. Isi kandungan yang diletak di dalam laman web universiti haruslah mengambil kira aspek-aspek utama tujuan pembangunan laman web khususnya bagi tujuan penyaluran maklumat yang diperlukan oleh pengguna sasaran.
- 5.1.2. Isi kandungan yang melibatkan hakcipta, harta intelek dan cap dagangan perlulah mendapat kebenaran dari pemiliknya terlebih dahulu sekiranya ingin dimasukkan ke dalam laman web universiti.
- 5.1.3. Setiap unit hendaklah menyediakan struktur dan prosedur kebenaran/ kelulusan berkaitan dengan pengisian dan pengubahsuaian isi kandungan dalam laman web unit masing-masing.
- 5.1.4. Isi kandungan laman web yang bersifat semasa hendaklah dikemaskini mengikut tempoh masa yang munasabah atau yang ditetapkan. Tarikh akhir laman web dikemaskini perlu dipaparkan di bahagian bawah kiri pada laman web utama tersebut.
- 5.1.5. Setiap unit hendaklah menyediakan satu mekanisme yang sesuai dan efektif untuk menjamin keselamatan kandungan laman web daripada diceroboh/ dipinda oleh pihak yang tidak bertanggungjawab.
- 5.1.6. Setiap unit hendaklah memastikan kandungan muka utama laman web mempunyai perkara-perkara berikut:
  - 5.1.6.1. Teks atau grafik yang mengandungi nama penuh unit berkenaan.
  - 5.1.6.2. Staf – Direktori staf.
  - 5.1.6.3. Maklumat perhubungan – alamat/ nombor telefon/ faks/e-mel.
  - 5.1.6.4. Maklumat untuk dan maklumat berkaitan (Information For and Information About)

Walau bagaimanapun setiap unit boleh menambah maklumat yang berkaitan dengan fungsi dan keperluan unit masing-masing seperti berikut :

- 5.1.6.1 Pengenalan/ Ucapan aluan.
- 5.1.6.2 Berita atau peristiwa.
- 5.1.6.3 Berita utama atau berita semasa.
- 5.1.6.4 Peristiwa yang akan datang.
- 5.1.6.5 Organisasi – Mengandungi carta organisasi.
- 5.1.6.6 Akademik – Maklumat mengenai akademik.
- 5.1.6.7 Penyelidikan – Maklumat mengenai bidang penyelidikan, geran penyelidikan, kepakaran penyelidikan, penerbitan dan pencapaian.
- 5.1.6.8 Kemudahan – Penyelidikan, perpustakaan dan lain-lain.
- 5.1.6.9 Pautan – Menyatakan pautan ke laman web universiti dan pautan-pautan lain yang berkaitan sahaja.
- 5.1.6.10 Maklum balas/ Feedback – Maklum balas daripada pelawat-pelawat web.
- 5.1.6.11 Sebarang penambahan menu adalah digalakkan.

- 5.1.7. Setiap laman web utama mesti mengandungi counter untuk mengira hits laman berkenaan.

## 5.2 REKABENTUK LAMAN WEB

- 5.2.1. Setiap unit haruslah merujuk kepada unit yang dilantik oleh universiti untuk menyelaras tema dan konsep reka bentuk laman web.
- 5.2.2. Reka bentuk yang diguna seharusnya bercirikan mesra pengguna, menarik dan mudah dicapai.
- 5.2.3. Untuk memastikan reka bentuk bercirikan mesra pengguna, menarik dan mudah dicapai, setiap unit mestilah memberi perhatian kepada perkara-perkara berikut:
- 5.2.3.1. Masa muat turun yang pantas dan munasabah.
  - 5.2.3.2. Penggunaan teknologi yang sesuai dan boleh dicapai oleh majoriti pengguna.
  - 5.2.3.3. Mengadakan capaian alternatif dengan menyediakan maklumat dalam mod text only.
  - 5.2.3.4. Reka letak sistem navigasi yang konsisten dan mudah digunakan bagi semua halaman.

## 5.3 KEMUDAHAN INTERAKSI/ PAUTAN DAN CARIAN

- 5.3.1. Setiap laman web unit hendaklah menyediakan logo atau teks “Universiti Teknologi Malaysia” yang dipautkan ke laman web utama universiti.
- 5.3.2. Setiap laman web unit hendaklah memaparkan notis hakcipta terpelihara (Contoh: Hakcipta Terpelihara Universiti Teknologi Malaysia) sekurang-kurangnya di laman utama setiap unit.
- 5.3.3. Setiap laman web unit hendaklah memaparkan notis penolakan tuntutan (disclaimer) bagi setiap pautan luar yang dinyatakan di dalam laman web universiti.
- 5.3.4. Setiap unit hendaklah memastikan pautan keluar dari laman web UTM adalah bersesuaian dengan kepentingan universiti. Pautan yang membawa kesan negatif kepada universiti hendaklah dielakkan seperti:
- 5.3.4.1. Laman web berunsur politik.
  - 5.3.4.2. Laman web berunsur pengiklanan/ perniagaan (kecuali yang diluluskan oleh pihak universiti).
  - 5.3.4.3. Laman web yang tidak bermoral dan melanggar etika.
  - 5.3.4.4. Laman web yang menyentuh sensitiviti individu, mana-mana agama dan kaum.
  - 5.3.4.5. Setiap laman web universiti hendaklah menyediakan mekanisme carian maklumat bagi kemudahan pengguna.

## 5.4 SPESIFIKASI LAMAN WEB

- 5.4.1. Penetapan ciri identifikasi yang melambangkan unit dan/ atau isi kandungan laman hendaklah diletakkan di bahagian tajuk halaman (Page Title).
- 5.4.2. Logo universiti yang diletakkan pada muka utama Laman Web setiap unit hendaklah ditetapkan lokasinya di bahagian yang mudah dilihat khususnya di bahagian atas kiri atau kanan skrin.
- 5.4.3. Bagi meningkatkan kebolegunaan dan keselesaan pengguna, teks yang digunakan haruslah:
- 5.4.3.1. Menggunakan warna yang kontra dengan warna latar belakang laman web.
  - 5.4.3.2. Dipecahkan kepada perenggan-perenggan yang lebih kecil sekiranya teks adalah panjang.
- 5.4.4. Pemilihan rupa taip dan fon yang digunakan haruslah mengambil kira faktor-faktor berikut:
- 5.4.4.1. Diambil dari koleksi umum.
  - 5.4.4.2. Menggunakan rupa taip dari kategori Sans Serif (seperti Arial, Tahoma dan Verdana misalnya) bagi memudahkan dibaca secara atas talian.
  - 5.4.4.3. Tidak menggunakan terlalu banyak jenis rupa taip dalam satu laman web yang sama.

**Kesemua elemen yang dinyatakan dibawah perlu ada pada laman web yang dibangunkan**

## 5.5 ENJIN PENCARIAN OPTIMA - SEO

### 5.5.1. Frasa dan kunci

- 5.5.1.1. Tumpuan pada keperluan pengguna yang disasarkan. Penekanan pada perkataan dan frasa yang akan digunakan oleh pengguna dalam mencari maklumat laman web yang dikehendaki.



5.5.1.2. Terdapat beberapa enjin carian yang memberi tumpuan yang lebih kepada perkataan dan frasa yang berdekatan dengan bahagian atas muka paparan. Oleh itu, masukkan kunci kata dan frasa terutama pada kedudukan antara tajuk dengan beberapa perenggan pertama.

## 5.5.2. Tag Tajuk :<Tajuk><Tajuk>

- 5.5.2.1. Perkataan dalam tag tajuk adalah amat penting terutama sekali oleh enjin carian dalam menentukan penarafan laman web.
- 5.5.2.2. Memastikan kunci kata yang paling penting digunakan dalam tag tajuk untuk setiap muka paparan. Lebih dekat kedudukan kunci kata ini dengan tag tajuk adalah lebih baik.
- 5.5.2.3. Gunakan tajuk yang singkat tetapi bermakna.
- 5.5.2.4. Tag tajuk perlu munasabah, kerana kebanyakan enjin carian menggunakan teks yang berada antara tag tajuk sebagai teks pautan. Ia juga digunakan sebagai tajuk oleh pelayar web dan sebagai tanda buku sesuatu muka paparan.

## 5.5.3. Pautan kepada laman-laman web yang berkaitan

- 5.5.3.1. Lebih banyak pautan laman-laman web lain kepada muka paparan adalah lebih baik untuk penarafan enjin carian.
- 5.5.3.2. Penggunaan kunci kata membolehkan kawalan dibuat ke muka paparan dan rujukan kepada pautan laman-laman web lain.

contoh : 'Lihat kekosongan jawatan' bukan 'Untuk kekosongan jawatan "klik di sini"'.  
</p></div><div data-bbox="171 524 645 541" data-label="Section-Header><h2>5.5.4. Pautan teks (<a href>linkto</a>) and tag imej alt="linkto"</div><div data-bbox="225 549 544 565" data-label="List-Group><ul style="list-style-type: none;"><li>5.5.4.1. Deskriptif terhadap pautan teks label.</li></ul></div><div data-bbox="282 573 895 602" data-label="Text"><p>Contoh : Gunakan Melihat Prospektus Pelajar, bukan 'Untuk melihat Prospektus Pelajar klik di sini.'</p></div><div data-bbox="225 610 895 652" data-label="List-Group"><ul style="list-style-type: none;"><li>5.5.4.2. Perkara ini serupa juga dengan tag alt imej. Masukkan teks yang berkaitan dengan imej, atau jika ianya adalah pautan, tunjukkan kedudukannya seperti: alt='Melihat Prospektus Pelajar'.</li></ul></div><div data-bbox="171 660 657 677" data-label="Section-Header"><h2>5.5.5. Tag deskripsi meta <meta name="deskripsi" content=" "></div><div data-bbox="225 686 895 776" data-label="List-Group"><ul style="list-style-type: none;"><li>5.5.5.1. Tag ini membolehkan penulisan deskripsi unik untuk hasil carian. Ia akan muncul di bawah pautan teks pada senarai hasil carian dan merupakan cara terbaik bagi memaklumkan seseorang yang telah membuat carian berkenaan apa yang mereka akan perolehi kelak.</li><li>5.5.5.2. Perlu pastikan deskripsi pendek dan menepati maksud.</li><li>5.5.5.3. Tidak semua enjin carian akan menggunakan deskripsi. Google, contohnya akan bina deskripsi sendiri pada kandungan paparan.</li></ul></div><div data-bbox="171 785 300 800" data-label="Section-Header"><h2>5.5.6. Metadata</h2></div><div data-bbox="225 810 895 851" data-label="List-Group"><ul style="list-style-type: none;"><li>5.5.6.1. Attention' perlu ada pada metadata untuk tujuan carian (informasi berkenaan laman web perlu dimasukkan antara head tags). Pastikan tajuk tag berada pada kedudukan yang betul dan mempunyai deskripsi yang sebaik mungkin.</li></ul></div><div data-bbox="282 859 613 875" data-label="Text"><p>Contoh : Jabatan Bahasa UTM: Berkaitan Kami</p></div><div data-bbox="225 884 895 913" data-label="List-Group"><ul style="list-style-type: none;"><li>5.5.6.2. Perkataan 'UTM' mesti dimasukkan dalam setiap penamaan laman web jabatan/ unit/ fakulti/ pejabat.</li></ul></div><div data-bbox="282 921 895 950" data-label="Text"><p>Contoh : UTM Pejabat Hal Ehwal Pelajar, UTM Jabatan Kejuruteraan Bioproses, UTM Unit Web, dll)</p></div><div data-bbox="865 942 895 959" data-label="Page-Footer"><p>17</p></div>

## 5.5.7. Kandungan

- 5.5.7.1. Kemaskini dan tambahan kandungan baru hendaklah kerap dilakukan pada laman web.
- 5.5.7.2. Letakkan kandungan yang dapat menarik minat pengguna ke laman web.
- 5.5.7.3. Adalah sangat digalakkan untuk setiap laman web terdapat peta laman.

## 5.5.8. Paparan

- 5.5.8.1. Penggunaan rangka (frames) tidak dibenarkan untuk laman web rasmi
- 5.5.8.2. Penggunaan jaringan (nested) tidak dibenarkan untuk laman web rasmi

## 5.5.9. Kandungan dinamik

- 5.5.9.1. Bahan-bahan bukan teks tidak dapat dibaca oleh pembaca skrin dan pelayar-pelayar teks sahaja. Alternatif teks perlu dibekalkan untuk sebarang kandungan yang dinamik. Bekalkan teks yang setara untuk item-item bukan teks yang lain.
- 5.5.9.2. Bekalkan alternatif yang setara untuk sebarang persembahan multimedia dan selaraskan alternatif-alternatif ini dengan persembahan tersebut.

## 5.6 BROWSERS

Semua laman web yang dibangunkan mesti menyokong paparan sekurang-kurangnya Mozilla Firefox dan Internet Explorer.



## **E. Peraturan Pengagihan Komputer Kepada Staf**



## E. Peraturan Pengagihan Komputer Kepada Staf

### 1. PENGENALAN

Penggunaan komputer yang meluas di Universiti Teknologi Malaysia (UTM) telah banyak membantu meningkatkan produktiviti staf di dalam menjalankan tugas harian UTM turut mengagihkan komputer kepada pengguna yang layak menerimanya. Ini selaras dengan aspirasi UTM untuk menjadi sebuah universiti bertaraf dunia

### 2. TUJUAN PERATURAN

Peraturan ini menerangkan kepada semua staf di universiti tentang pengurusan pengagihan komputer. Perolehan komputer dan aksesori secara berpusat adalah di bawah tanggungjawab Pusat ICT. Selain itu, peraturan ini juga bertujuan untuk menyelaraskan dan menyeragamkan pengagihan komputer di universiti.

### 3. SKOP PERATURAN

Skop peraturan merangkumi ;

- 3.1. Semua perkakasan dan perisian milik rasmi universiti yang digunakan atau berada dalam simpanan pengguna tanpa mengira situasi penggunaannya.
- 3.2. Semua aplikasi yang dibangunkan dan dimiliki oleh Universiti tanpa mengira situasi penggunaan aplikasi tersebut.
- 3.3. Staf universiti yang layak adalah seperti berikut :
  - 3.3.1 Mengikut jawatan khas iaitu Naib Canselor / Timbalan Naib Canselor/Pendaftar/ Bendahari / Ketua Pustakawan /Penasihat Undang-Undang / Pengarah Kerja / Dekan / Timbalan Dekan / Pengarah / Ketua Jabatan / Pengurus Teknologi Maklumat / Pengetua.
  - 3.3.2 Mengikut jawatan akademik iaitu pensyarah (tetap / kontrak / lantikan bahagian).
  - 3.3.3 Mengikut jawatan bukan akademik iaitu Pegawai Kumpulan Pengurusan & Profesional (Tetap/ Kontrak/ lantikan bahagian) dan staf sokongan pejabat (Tetap/ Kontrak/ lantikan bahagian) yang terlibat dengan kerja-kerja khusus yang memerlukan penggunaan komputer meja atau *notebook* dengan kebenaran Ketua Jabatan.
- 3.4. Pinjaman komputer peribadi atau komputer riba boleh dipertimbangkan kepada staf universiti seperti berikut:
  - 3.4.1 Profesor adjung
  - 3.4.2 Pensyarah pelawat
  - 3.4.3 Pengajar/ Calon SLAB UTM
  - 3.4.4 Staf sokongan lain
- 3.5. Pusat Tanggung Jawab (PTJ) bertanggungjawab untuk membuat perolehan komputer yang diguna di Makmal Pengajaran dan Penyelidikan serta memaklumkan kepada Pusat ICT maklumat perolehan tersebut untuk rekod inventori universiti.

### 4. PERATURAN PENGAGIHAN KOMPUTER KEPADA STAF

Berikut merupakan peraturan pengagihan komputer kepada staf:

- 4.1. Semua pengagihan perkakasan hendaklah mengikut prosedur universiti.
- 4.2. Staf akademik serta Pengurusan dan Profesional layak mendapat satu (1) unit komputer peribadi atau satu (1) unit komputer riba setiap seorang. Kemudahan perkakasan daripada sumber-sumber lain tertakluk kepada kelulusan Ketua PTJ. Peruntukan adalah berasaskan kekananan jawatan, beban tugas dan kesediaan perkakasan.
- 4.3. Staf kategori lain layak diagihkan satu (1) unit komputer *peribadi atau komputer riba* berdasarkan keperluan kerja yang ditentukan oleh Ketua PTJ.
- 4.4. Staf yang tamat perkhidmatan atau staf yang dikehendaki memulangkan komputer peribadi atau komputer riba oleh universiti atas sebab cuti belajar di universiti selain daripada UTM mesti memulangkan perkakasan di bawah tanggungjawabnya kepada PTJ selewat-lewatnya satu (1) minggu sebelum tarikh berkaitan.

Perkakasan yang hendak dipulangkan hendaklah berada dalam keadaan baik. Adalah menjadi tanggungjawab ketua PTJ untuk memberitahu Pusat ICT tentang pemulangan komputer peribadi atau komputer riba tersebut.

- 4.5. Penggantian komputer peribadi atau komputer riba hanya boleh dipertimbangkan jika terdapat keperluan aplikasi khusus yang tidak disokong oleh komputer ,terdapat kegagalan fungsi atau penggunaannya telah melebihi 3 tahun digunakan dari tarikh pengagihan dan disokong oleh ketua PTJ. Namun begitu, tempoh masa boleh dipertimbangkan jika terdapat masalah teknikal yang tidak dapat dielakkan. Bagaimanapun keputusan muktamad tertakluk kepada pengesahan Pengarah CICT.

## **5. PENGAGIHAN SEMULA KOMPUTER KEPADA STAF**

Ketua PTJ atau mana-mana pegawai yang diberi kuasa berhak ;

- 5.1. Mengagihkan semula komputer yang telah diperuntukkan kepada mana-mana staf sama ada yang telah menamatkan perkhidmatan secara kontrak, bersara, kerja, cuti belajar selain daripada UTM, hilang keupayaan disebabkan oleh masalah kesihatan (diperaku oleh Lembaga Kesihatan) kepada mana-mana staf yang mengisi semula kekosongan jawatan tersebut atau bergantung kepada keperluan PTJ.



## **F. Peraturan Penggunaan Makmal Komputer**



## F. Peraturan Penggunaan Makmal Komputer

### 1 PENGENALAN

Makmal komputer disediakan oleh pihak universiti adalah untuk menyokong aktiviti pentadbiran, pendidikan, pembangunan dan penyelidikan, dan perkhidmatan di universiti.

### 2 TUJUAN PERATURAN

Peraturan penggunaan makmal komputer bertujuan :

- 2.1. Untuk memastikan tiada penyalahgunaan kemudahan makmal komputer termasuk peralatan dan perisian yang disediakan.
- 2.2. Menerangkan penguatkuasaan penggunaan makmal komputer.
- 2.3. Mewujudkan suasana yang sesuai untuk penggunaan makmal komputer.
- 2.4. Menanamkan sifat tanggungjawab di kalangan pengguna makmal komputer.

### 3 SKOP PERATURAN

Peraturan ini merangkumi semua staf, pelajar dan sesiapa yang terlibat dalam penggunaan makmal komputer. Peraturan penggunaan ini tidak merangkumi pengurusan makmal komputer sahaja.

### 4 PERATURAN WAKTU PENGGUNAAN MAKMAL KOMPUTER

Waktu penggunaan makmal perlu ditetapkan dan dimaklumkan kepada pengguna. Waktu ini adalah tertakluk kepada perubahan dan notis perubahan.

### 5 PENEMPAHAN PENGGUNAAN MAKMAL KOMPUTER

- 5.1. Semua penempahan penggunaan perlu direkodkan.
- 5.2. Penempahan makmal perlu melalui prosedur yang telah ditetapkan.

### 6. PERATURAN SEBELUM MEMASUKI MAKMAL KOMPUTER

- 6.1. Pengguna perlu mendaftar kepada pihak yang bertanggungjawab
- 6.2. Pengguna perlu membawa bersama kad matrik atau kad pengenalan diri semasa memasuki makmal (kecuali jika mendapat kebenaran dari petugas makmal yang bertugas).

### 7. PERATURAN KETIKABERADA DI DALAM MAKMAL KOMPUTER

- 7.1. Pengguna dikehendaki mematuhi peraturan keselamatan akaun.
- 7.2. Keselamatan data pengguna adalah di bawah tanggungjawab pengguna.
- 7.3. Pengguna dilarang mengubah, mengalih dan membawa keluar sebarang peralatan yang terdapat dalam makmal komputer.
- 7.4. Semua bentuk permainan komputer tidak dibenarkan.
- 7.5. Pengguna tidak dibenarkan mengubah, menambah atau memadam sebarang perisian dalam sistem komputer makmal yang disediakan.
- 7.6. Pengguna dilarang menyalin perisian berlesen daripada sistem komputer makmal yang disediakan.
- 7.7. Pengguna tidak dibenarkan untuk mengubah aturan atau konfigurasi komputer.
- 7.8. Penggunaan internet di dalam makmal tertakluk kepada peraturan penggunaan internet.
- 7.9. Tatacara perlakuan di dalam makmal komputer adalah tertakluk kepada peraturan universiti.
- 7.10. Keselamatan barang berharga pengguna adalah di bawah tanggungjawab pengguna.
- 7.11. Penggunaan komputer peribadi di dalam makmal tertakluk kepada peraturan penggunaan makmal komputer.
- 7.12. Penggunaan kemudahan makmal komputer secara atas talian tertakluk kepada peraturan penggunaan komputer.

## 8. TATACARA BERPAKAIAN

Tatacara berpakaian di makmal komputer adalah mengikut peraturan berpakaian Universiti.

## 9. KEBERSIHAN DAN KECERIAAN MAKMAL KOMPUTER

- 9.1. Dilarang membawa masuk makanan dan minuman ke dalam makmal (kecuali dengan izin).
- 9.2. Dilarang membuang sampah merata-rata di dalam makmal.

## 10. PEMATUHAN PANDUAN KETIKA KECEMASAN

Jika berlaku sebarang keadaan kecemasan (seperti kebakaran atau sebagainya) di dalam makmal, pengguna hendaklah mematuhi kehendak (atau panduan) keselamatan yang disediakan di makmal tersebut

## 11. PANDUAN WAKTU PENGGUNAAN MAKMAL KOMPUTER

Penempahan makmal sebaik-baiknya dilakukan atau disahkan oleh pegawai bertanggungjawab bagi mengelakkan timbulnya kekeliruan mengenai tarikh, masa dan tujuan tempahan.

## 12. PENEMPAHAN PENGGUNAAN MAKMAL KOMPUTER

Penempahan makmal sebaik-baiknya dilakukan atau disahkan oleh pegawai bertanggungjawab bagi mengelakkan timbulnya kekeliruan mengenai tarikh, masa dan tujuan tempahan.

## 13. PENGGUNAAN MAKMAL KOMPUTER

- 13.1. Penggunaan telefon di dalam makmal mestilah berhemah.
- 13.2. Sebarang masalah perlu merujuk kepada petugas.

## 14. KEBERSIHAN DAN KECERIAAN MAKMAL KOMPUTER

Kebersihan makmal adalah tanggungjawab bersama.





## **G. Peraturan Peminjaman Peralatan ICT**



## G. Peraturan Peminjaman Peralatan ICT

### 1. PENGENALAN

Peraturan peminjaman peralatan ICT merupakan panduan yang perlu diikuti dalam meminjam sebarang peralatan ICT yang dimiliki oleh pihak universiti.

### 2. TUJUAN PERATURAN

Tujuan peraturan ini adalah untuk memberi makluman kepada pengguna tentang tatacara dan tanggungjawab pengguna berhubung dengan peminjaman peralatan ICT UTM.

### 3. SKOP PERATURAN

Peraturan ini merangkumi semua peralatan ICT universiti yang dipinjamkan kepada pengguna tanpa mengira lokasi peralatan tersebut (merujuk peraturan membawa peralatan keluar kampus). Pengguna di dalam skop peminjaman ini adalah merujuk kepada staf dan pelajar yang meminjam peralatan ICT universiti.

### 4. PERNYATAAN PERATURAN

#### 4.1. PENGGUNAAN PERALATAN ICT YANG DIPINJAM

Berikut merupakan tatacara penggunaan peralatan ICT :

- 4.1.1 Pengguna tidak berhak mengganggu dengan apa cara sekalipun peralatan ICT yang bukan berada di bawah kawalannya. Ini termasuk mengguna atau mengambil tanpa kebenaran, menceroboh dan mencuri peralatan ICT atau komponen-komponennya.
- 4.1.2 Pengguna hendaklah melaporkan dengan segera kepada pihak yang bertanggungjawab sekiranya peralatan ICT tersebut rosak atau tidak berfungsi untuk tujuan pembaikan.
- 4.1.3 Pengguna hendaklah melaporkan dengan segera kepada pihak bertanggungjawab sekiranya perkakasan ICT di bawah kawalannya didapati hilang atau dicuri mengikut prosedur yang telah ditetapkan oleh pihak universiti.
- 4.1.4 Dilarang meninggalkan peralatan ICT dalam keadaan terpasang tanpa pengawasan.
- 4.1.5 Dilarang mengguna kabel sambungan elektrik yang rosak atau bermasalah.
- 4.1.6 Penggunaan kabel sambungan elektrik yang tidak disambung secara terus ke punca elektrik adalah dilarang sama sekali.

#### 4.2. PEMINJAMAN PERALATAN ICT

Berikut merupakan peraturan peminjaman peralatan ICT:

- 4.2.1. Semua peminjaman peralatan ICT hendaklah mengikut prosedur peminjaman peralatan yang telah ditetapkan oleh universiti.
- 4.2.2. Pihak yang memberi pinjam peralatan ICT ini perlu merekodkan sekurang-kurangnya maklumat yang berikut:
  - 4.2.2.1 Maklumat peminjam.
  - 4.2.2.2 Tempoh peminjaman.
  - 4.2.2.3 Tujuan peminjaman.
  - 4.2.2.4 Maklumat kelulusan.
- 4.2.3. Peminjam hendaklah melaporkan dengan segera sekiranya berlaku kerosakan atau kehilangan peralatan ICT yang dipinjam kepada universiti.
- 4.2.4. Semasa dalam tempoh peminjaman, pihak peminjam adalah bertanggungjawab ke atas aspek keselamatan peralatan ICT (virus, perisian sistem dan sebagainya).
- 4.2.5. Pelajar yang ingin membuat peminjaman perlu melalui pegawai universiti.
- 4.2.6. Sebarang kehilangan peralatan ICT yang dipinjamkan, akan melalui Jawatankuasa Pelarasan Kehilangan Harta Universiti dengan mengemukakan laporan Polis kepada Bahagian Keselamatan Universiti dan pengurusan Fakulti.

4.2.7. Universiti berhak untuk menarik balik pinjaman pada bila-bila masa sekiranya:

4.2.7.1 Berlaku pelanggaran peraturan universiti.

4.2.7.2 Ada keperluan universiti.

4.2.8. Peminjaman adalah berdasarkan ketersediaan peralatan yang hendak dipinjam.

#### **4.3. PEMULANGAN PERALATAN ICT**

4.3.1. Peminjam perlu memulangkan peralatan yang dipinjam pada tarikh yang telah dinyatakan. Sekiranya peminjam gagal memulangkan pada tarikh yang ditetapkan, tindakan boleh diambil oleh pihak pengurusan ICT.

4.3.2. Peralatan ICT yang dipulangkan mestilah berada dalam keadaan baik, berfungsi dan di dalam set yang lengkap.

#### **5. PERNYATAAN PANDUAN**

5.1. Pengguna dinasihatkan agar meletakkan kata nama dan laluan sekiranya komputer yang digunakan mengandungi maklumat sulit universiti yang tidak boleh didedahkan kepada orang lain.

5.2. Pastikan peralatan komputer dan kebersihannya dijaga secara berkala.

5.3. Peralatan komputer yang telah disediakan oleh pihak universiti hendaklah digunakan secara berhemah.



## H. Peraturan Pelupusan Peralatan ICT



## H. Peraturan Pelupusan Peralatan ICT

### 1. PENGENALAN

Pelupusan adalah adalah satu proses untuk mengeluarkan aset dari milikan, kawalan, simpanan dan rekod mengikut kaedah yang ditetapkan. Peralatan ICT adalah merangkumi semua perkakasan atau komponen fizikal, dan perisian dalam sesuatu sistem komputer.

### 2. TUJUAN PERATURAN

Tujuan garis panduan ini adalah untuk memberi panduan kepada semua Fakulti/ Pusat/ Jabatan/ Unit mengenai tatacara pelupusan sebarang peralatan ICT.

### 3. SKOP PERATURAN

Kriteria-kriteria dan justifikasi pelupusan adalah tertakluk kepada Pekeliling Perbendaharaan Bil 5/2007 dan Pekeliling Bendahari UTM Bil x/2008. Berikut adalah perkara yang perlu diambil kira untuk melupuskan peralatan ICT:

- 3.1. Keupayaan dan/ atau kecekapan peralatan adalah rendah atau semakin menjadi rendah berbanding dengan beban kerja (keusangan).
- 3.2. Tidak dapat memenuhi keperluan semasa disebabkan perubahan teknologi.
- 3.3. Kos penyelenggaraan dan/ atau kos pengoperasian komputer terlalu tinggi berbanding dengan prestasi peralatan.
- 3.4. Kekerapan berlaku ralat adalah tinggi.
- 3.5. Syarikat atau ejen pembekal tidak lagi memberi khidmat sokongan ke atas peralatan komputer berkenaan.
- 3.6. Alat ganti sukar atau tidak boleh diperoleh.

### 4. PERATURAN PELUPUSAN PERALATAN ICT

- 4.1. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan peralatan ICT UTM yang terkini.
- 4.2. Peralatan ICT yang hendak dilupuskan adalah termasuk perkakasan yang dibekalkan oleh Pusat ICT atau yang dibekalkan oleh pihak universiti.

### 5. PERNYATAAN PANDUAN

- 5.1. Prosedur pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan universiti.
- 5.2. Langkah berjaga-jaga hendaklah diambil sebelum pelupusan dilaksanakan. Ini termasuklah menghapuskan semua kandungan data dalam peralatan khususnya maklumat rahsia rasmi sebelum ia dilupuskan.
- 5.3. Panduan jangka hayat:

5.3.1	Komputer Peribadi	-	4 Tahun
5.3.2	Pencetak	-	4 Tahun
5.3.3	Komputer Riba	-	4 Tahun
5.3.4	Pengimbas	-	4 Tahun
5.3.5	Lcd Projector	-	4 Tahun
5.3.6	Monitor	-	4 Tahun
5.3.7	Server	-	4 Tahun

- 5.4. Panduan lupus/ baikpulih:

5.4.1 Alatan ICT yang belum mencapai jangka hayat boleh dilupus sekiranya kos baikpulih melebihi 50% daripada kos perolehan baru.



## **I. Peraturan Keselamatan ICT**



## I. Peraturan Keselamatan ICT

### 1. PENGENALAN

Antara cabaran utama di dalam menyediakan perkhidmatan ICT dengan kebolehsediaan yang tinggi dan berintegriti adalah menangani isu-isu berkaitan pencerobohan, pengodaman, perkhidmatan yang disanggah secara sengaja atau tidak dan pengintipan data. Universiti telah membelanjakan jumlah wang yang besar bagi meningkatkan tahap keselamatan sistem penyampaian perkhidmatan ICT. Namun begitu, faktor manusia dan proses merupakan faktor yang perlu diberi keutamaan pembaikan pada masakini.

### 2. TUJUAN PERATURAN

Peraturan keselamatan ICT bertujuan ;

- 2.1. Memastikan pengawalan dan pengurusan keselamatan ke atas perkakasan, perisian, aplikasi dan operasi komputer terjamin;
- 2.2. Menambah baik dan meningkatkan proses keselamatan sistem rangkaian komputer universiti.

### 3. SKOP PERATURAN

- 3.1. Merangkumi aspek keselamatan perkakasan, perisian sistem, pangkalan data dan sistem aplikasi.
- 3.2. Berkaitan aspek reka bentuk keselamatan sistem capaian internet.

### 4. PERATURAN KESELAMATAN KAWALAN CAPAIAN FIZIKAL

- 3.1. Melindungi kabel dalam kawasan awam dengan pemasangan konduit atau lain-lain mekanisma perlindungan.
- 3.2. Kawalan terhadap individu/ staf yang masuk ke Bilik Pelayan Komputer dan juga kawalan akses kepada semua pelayan serta sumber ICT lain.
- 3.3. Mewujudkan mekanisma kawalan capaian fizikal untuk staf /individu mencapai pelayan berkenaan.

### 5. PERATURAN KESELAMATAN KAWALAN CAPAIAN LOGIKAL

Kawalan dibuat semasa pemasangan agar hanya mereka yang dibenarkan sahaja boleh mencapai kawalan capaian.

### 6. PERATURAN KESELAMATAN IDENTIFIKASI PENGGUNA

Pengguna sistem boleh terdiri daripada individu atau kumpulan pengguna yang berkongsi akaun kumpulan pengguna yang sama. Dalam kedua-dua keadaan, pengguna perlu bertanggungjawab ke atas keselamatan sistem yang digunakan. Langkah yang diambil untuk mengenalpasti pengguna yang sah ialah :

- 6.1. Memberi satu identifikasi (ID) yang unik kepada setiap pengguna individu.
- 6.2. Menyimpan dan menyelenggara semua ID pengguna yang bertanggungjawab untuk setiap aktiviti.
- 6.3. Memastikan adanya kemudahan pengauditan untuk menyemak semua aktiviti pengguna.
- 6.4. Memastikan semua ID pengguna yang diwujudkan adalah berdasarkan permohonan dan tiada ID pengguna yang tidak diperlukan.
- 6.5. Perubahan ID pengguna untuk sistem aplikasi perlu mendapat kebenaran daripada pemilik sistem tersebut.
- 6.6. Bagi memastikan ID pengguna yang tidak aktif tidak disalahgunakan, langkah berikut mesti diambil ;
  - 6.6.1 Menggantug semua kemudahan ID pengguna yang tidak digunakan selama 30 hari secara berterusan dan menghapuskan ID berkenaan selepas dari tempoh 30 hari tersebut.
  - 6.6.2 Menghapuskan semua kemudahan untuk pengguna yang berpindah atau tamat perkhidmatan.
- 6.7. Jejak audit untuk setiap aktiviti pengguna hendaklah disimpan dan diarkib sekiranya keperluan storan adalah mencukupi terutamanya untuk pengguna yang boleh mencapai maklumat sulit agar dapat dikenal pasti sekiranya berlakunya pencerobohan maklumat.

## 6.8. Pengesahan pengguna

Proses pengesahan bertujuan mengenal pasti hanya pengguna yang sah sahaja dibenarkan menggunakan sistem melalui penggunaan kata laluan. Sistem mestilah boleh menyediakan kemudahan ;

6.8.1 Kata laluan yang boleh dimasukkan dalam bentuk yang tidak boleh dilihat.

6.8.2 Panjang kata laluan sekurang-kurangnya 8 aksara.

6.8.3 Merupakan kombinasi daripada aksara, angka dan simbol-simbol lain.

6.8.4 Kata laluan dienkrip semasa penghantaran.

6.8.5 Fail kata laluan disimpan berasingan daripada data sistem aplikasi utama.

6.8.6 Cubaan capaian dihadkan kepada tiga (3) kali sahaja. ID pengguna berkenaan perlu digantung selepas tiga (3) kali berturut-turut.

## 7. JEJAKAUDIT

7.1. Universiti bertanggungjawab menyediakan dan menyimpan rekod jejak audit bagi mengenalpasti akauntabiliti pengguna dan keselamatan.

7.2. Penggunaan jejak audit untuk sistem komputer dan manual operasi perlu diwujudkan untuk:

7.2.1. Capaian kepada maklumat yang kritikal.

7.2.2 Capaian kepada perkhidmatan rangkaian.

7.2.3 Keistimewaan atau kebenaran tertentu yang melebihi kebenaran sebagai pengguna biasa seperti arahan keselamatan dan fungsi *super-user*.

7.3 Maklumat jejak audit merangkumi

7.3.1 Identifikasi (ID) pengguna.

7.3.2 Fungsi, sumber dan maklumat yang digunakan atau dikemaskini.

7.3.3 Tarikh dan masa penggunaan.

7.3.4 Alamat IP pelanggan atau stesen kerja.

7.3.5 Transaksi dan program yang dijalankan secara khusus.

7.4. Universiti akan mengambil tindakan berikut semasa penyediaan jejak audit:

7.4.1 Meneliti dan melaporkan sebarang aktiviti yang diragui dengan segera.

7.4.2 Meneliti jejak audit secara berjadual.

7.4.3 Meneliti dan melaporkan sebarang masalah keselamatan dan kejadian luar biasa.

7.4.4 Menyimpan maklumat jejak audit untuk jangka masa tertentu bagi keperluan operasi dan keselamatan.

7.4.5 Mengawal maklumat jejak audit daripada dihapus, diubahsuai, ditipu atau disusun semula.

## 8. MAKLUMAT SANDAR

8.1 Universiti bertanggungjawab memulihkan sistem sepenuhnya jika berlaku masalah atau Kerosakan.

8.2 Rancangan sandaran perlu dibuat secara berjadual dan semasa perubahan konfigurasi pada sistem. Jejak audit perlu disimpan di tempat berasingan dan selamat.

8.3. Universiti akan mengambil tindakan berikut semasa penyediaan sandaran.

8.3.1. Mendokumen prosedur sandaran dan pemulihan.

8.3.2 Menyimpan tiga (3) generasi sandar.

8.3.3 Menguji media salinan dan prosedur pemulihan dua (2) kali setahun.



## **9. PENYENGGARAAN**

- 9.1. Universiti melaksanakan kawalan dan penyenggaraan bagi memastikan integriti sistem pengoperasian daripada terdedah kepada sebarang pencerobohan keselamatan:
- 9.1.1 Tampilan dan Kelemahan Sistem - Mengemaskini tampilan dan mengatasi kelemahan sistem yang berlaku daripada agensi keselamatan berdaftar
  - 9.1.2 Naik taraf - Menaiktaraf sistem pengoperasian kepada versi terkini sesuai dengan spesifikasi peralatan ICT yang ada.

## **10. KESELAMATAN SISTEM APLIKASI**

Universiti bertanggungjawab melaksana dan mengawal tahap capaian sistem aplikasi.

## **11. PERISIAN APLIKASI**

- 11.1. Kawalan keselamatan dilaksana untuk mengelak berlakunya capaian oleh pengguna yang tidak sah, pengubahsuaian, pendedahan atau penghapusan maklumat. Universiti bertanggungjawab menyediakan kawalan dan kemudahan seperti berikut:
- 11.1.1 Sistem keselamatan berpusat dengan kawalan capaian penggunaan satu ID dan kata laluan untuk semua aplikasi.
  - 11.1.2. Profil capaian yang menghadkan tahap capaian maklumat serta fungsi berdasarkan peranan pengguna.
  - 11.1.3 Menggunakan kaedah pengesahan kedua (seperti kad pintar) untuk aplikasi kritikal misi bagi memastikan integriti dipertingkat.
  - 11.1.4 Kawalan peringkat sistem aplikasi yang menentukan akauntabiliti tertentu kepada pengguna.
  - 11.1.5 Penetapan pemilik maklumat.

## **12. PANGKALAN DATA**

- 12.1. Universiti bertanggungjawab mengadakan kawalan capaian kepada pangkalan data. Integriti maklumat yang disimpan dalam pangkalan data dikekalkan dan dijamin melalui:
- 12.1.1 Sistem pengurusan pangkalan data yang memastikan integriti dalam pengemaskinian capaian maklumat.
  - 12.1.2 Kawalan capaian kepada maklumat ditentukan oleh Pentadbir Pangkalan Data.

## **13. PENGUJIAN APLIKASI**

- 13.1. Universiti bertanggungjawab menguji atur cara, modul, sistem aplikasi dan integrasi sistem aplikasi bagi memastikan sistem berfungsi mengikut spesifikasi yang ditetapkan. Langkah berikut diambil semasa pengujian aplikasi dijalankan:
- 13.1.1 Menggunakan data dummy atau data sejarah.
  - 13.1.2 Mengawal penggunaan data sulit.
  - 13.1.3 Menghadkan capaian kepada staf yang terlibat sahaja.
  - 13.1.4 Menghapuskan maklumat yang digunakan setelah selesai pengujian (terutamanya apabila menggunakan data lapuk).
  - 13.1.5 Menggunakan persekitaran yang berasingan untuk pembangunan dan pengoperasian sistem aplikasi.

## **14. PERISIAN BERKOD HASAD DAN CACAT**

- 14.1. Atur cara sistem aplikasi terdedah kepada kod hasad dan kod rosak. Universiti bertanggungjawab mengurangkan kemungkinan perisian yang rosak melalui kawalan berikut:

## 14. PERISIAN BERKOD HASAD DAN CACAT

- 14.1. Atur cara sistem aplikasi terdedah kepada kod hasad dan kod rosak. Universiti bertanggungjawab mengurangkan kemungkinan perisian yang rosak melalui kawalan berikut:
- 14.1.1 Kod sumber daripada pembangun sistem aplikasi yang bereputasi baik, rekod prestasi perkhidmatan yang baik dan mempunyai kepakaran teknikal yang tinggi.
  - 14.1.2 Mewujud dan melaksanakan program jaminan kualiti dan prosedur untuk semua sistem aplikasi yang dibangunkan secara dalaman dan luaran.
  - 14.1.3 Memastikan semua sistem aplikasi didokumen, diuji, disahkan fungsinya, tahan lasak dan menepati spesifikasi.

## 15. PERUBAHAN VERSI

- 15.1. Universiti bertanggungjawab mengawal versi sistem aplikasi apabila perubahan atau peningkatan dibuat dan prosedur kawalan perubahan sentiasa dipatuhi.

## 16. PENYIMPANAN KOD SUMBER

- 16.1. Universiti bertanggungjawab mengurus dan melaksanakan kawalan penyimpanan kod sumber bagi sistem aplikasi yang dibangunkan secara dalaman atau luaran untuk tujuan penyelenggaraan dan peningkatan yang merangkumi:
- 16.1.1 Mewujudkan prosedur penyenggaraan versi terkini.
  - 16.1.2 Mewujudkan perjanjian untuk keadaan di mana berlakunya kerosakan atau bencana dan kod sumber tidak ada.

## 17. PERISIAN TIDAK BERLESEN

- 17.1. Universiti bertanggungjawab memastikan semua perisian yang digunakan adalah berlesen serta mengawal dan menyimpan lesen serta kawalan fizikal ke atas lokasi perisian berlesen dan salinan lesen yang dikeluarkan.

## 18. KAWALAN KOD HASAD(MALICIOUS CODE)

- 18.1. Universiti bertanggungjawab memastikan integriti maklumat daripada pendedahan atau kemusnahan akibat kod hasad seperti berikut:
- 18.1.1 Melaksanakan prosedur untuk mengurus kod hasad.
  - 18.1.2 Mewujudkan peraturan berkaitan memuat turun, penerimaan dan penggunaan perisian percuma dan kongsi.
  - 18.1.3 Menyebarkan arahan dan maklumat untuk mengesan kod hasad kepada semua pengguna.
  - 18.1.4 Mengambil langkah pencegahan atau pemulihan serangan kod hasad
    - 18.1.4.1 Mengimbas dan menghapus kod hasad menggunakan perisian anti virus yang diluluskan
    - 18.1.4.2 Menyemak status proses imbasan dalam laporan log.
    - 18.1.4.3 Tidak melaksana atau membuka fail keipilan daripada e-mel yang meragukan.

## 19. KESELAMATAN PENGGUNAAN E-MEL

(RUJUK PADA PERATURAN PENGGUNAAN E-MEL)

## 20. KESELAMATAN PERALATAN RANGKAIAN

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

## **21. KESELAMATAN FIZIKAL**

- 21.1. Peralatan rangkaian hendaklah ditempatkan di tempat yang bebas daripada risiko luar jangkaan seperti banjir, kilat, gegaran, kekotoran dan sebagainya.
- 21.2. Suhu hendaklah terkawal di dalam had suhu peralatan rangkaian berkenaan dengan memasang sistem penghawa dingin sepanjang masa.
- 21.3. Memasang Bekalan Kuasa Tanpa Gangguan (UPS) dengan minimum 15 minit masa beroperasi jika terputus bekalan elektrik dan perlindungan daripada kilat dan menyokong penutupan pelayan secara automatik.

## **22. KESELAMATAN CAPAIAN FIZIKAL**

- 22.1. Langkah yang perlu diambil untuk melindungi kabel rangkaian daripada dicapai oleh mereka yang tidak berkenaan:
  - 22.1.1 Melindungi kabel di dalam kawasan awam dengan cara memasang conduit atau lain-lain mekanisma perlindungan.
  - 22.1.2 Pusat dan punca pendawaian terletak di dalam ruang atau bilik yang berkunci dan hanya boleh dicapai oleh staf yang dibenarkan sahaja.

## **23. KESELAMATAN CAPAIAN PERALATAN RANGKAIAN**

- 23.1. Peralatan rangkaian hendaklah ditempatkan di tempat yang selamat dan terkawal.
- 23.2. Peralatan rangkaian hanya boleh dicapai oleh staf yang dibenarkan sahaja.

## **24. KESELAMATAN CAPAIAN LOGIKAL**

- 24.1. ID dan kata laluan sah diperlukan untuk mencapai perisian rangkaian. Capaian hanya boleh dibuat oleh staf yang dibenarkan sahaja.
- 24.2. Komposisi kata laluan mestilah konsisten dengan garis panduan yang telah ditetapkan.
- 24.3. Maklumat capaian ke router hendaklah direkodkan (pegawai, tarikh, masa dan aktiviti). Maklumat mestilah disimpan sekurang-kurangnya selama 90 hari.
- 24.4. 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.
- 24.5. Perubahan perisian konfigurasi mestilah direkodkan.
- 24.6. Perubahan konfigurasi hendaklah dikendalikan secara berpusat.

## **25. PENGGUNAAN PERALATAN TANPA KEBENARAN**

- 25.1. Dilarang menyambung sebarang peralatan selain daripada yang dibenarkan
- 25.2. Bilik pendawaian atau almari pendawaian hanya boleh dicapai oleh pegawai yang dibenarkan sahaja.

## **26. KONFIGURASI PERALATAN**

- 26.1. Mengaktifkan perkhidmatan yang diperlukan sahaja.
- 26.2. Menghadkan capaian konfigurasi kepada nod atau alamat IP yang dibenarkan.
- 26.3. Mematikan penyiaran trafik.
- 26.4. Menggunakan kata laluan yang selamat.
- 26.5. Dilaksanakan oleh staf yang terlatih dan dibenarkan sahaja.

## **27. PENYELENGGARAAN PERALATAN**

- 27.1 Peralatan hendaklah dipasang, dioperasi dan diselenggara mengikut spesifikasi pengilang.
- 27.2 Peralatan dibaiki dan diselenggara hanya oleh staf yang terlatih dan dibenarkan sahaja.
- 27.3. Mengemaskini rekod penyenggaraan.

# Polisi & Peraturan

Teknologi Maklumat & Telekomunikasi (ICT)

---

## 28. KEBOLEHCAPAIAN PENGGUNA MELAKUKAN PENGINTIPAN DATA RANGKAIAN UNIVERSITI

- 28.1. Perisian pengintip atau penganalisis tidak dibenar digunakan pada sebarang komputer kecuali setelah mendapat kebenaran daripada Pengarah CICT atau Pegawai Keselamatan ICT

## 29. PROTOKOL RANGKAIAN YANG TIDAK DIGALAKKAN

- 29.1. Penggunaan protokol rangkaian yang mengambil bandwidth yang tinggi seperti NetBIOS dan IPX/SPX.
- 29.2. Penggunaan workgroup kerana menyokong share-level security.

## 30. FIREWALL

- 30.1. Semua trafik rangkaian dari dalam ke luar UTM dan sebaliknya mestilah melalui firewall dan hanya trafik yang disahkan sahaja dibenarkan untuk melepasi.
- 30.2. Reka bentuk firewall hendaklah mengambilkira perkara berikut:
  - 30.2.1 Keperluan audit dan arkib.
  - 30.2.2 Kebolehsediaan.
  - 30.2.3 Kerahsiaan.
  - 30.2.4 Melindungi maklumat UTM.
- 30.3. Pusat Tanggungjawab (PTJ) yang mempunyai pelayan komputer sendiri boleh menyediakan firewall khusus untuk tujuan keselamatan.