BAB 8: DASAR AKAUNTABILITI DAN KERAHSIAAN MAKLUMAT

8.1 Tujuan

Menyatakan tanggungjawab pihak yang terlibat dengan penggunaan kemudahan ICT di Universiti Malaysia Pahang (UMP) seperti berikut:

i. memelihara dan melindungi maklumat peribadi staf yang disimpan oleh UMP yang diklasifikasikan sebagai maklumat rahsia atau sulit;

ii. menyokong usaha UMP untuk menjaga kepentingan *stakeholder*; dan

iii. menerangkan aktiviti yang dilakukan oleh Jawatankuasa Pengurusan Maklumat (JKPM) atau pengguna yang melibatkan capaian data atau maklumat yang diklasifikasikan sebagai maklumat rahsia atau sulit.

8.2 Skop

Skop dasar ini meliputi tanggungjawab pengguna dan UMP berkaitan capaian maklumat rahsia atau sulit.

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

8.3 Ciri-ciri Utama Keselamatan Data & Maklumat

8.3.1 Kerahsiaan

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

8.3.2 Integriti

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

8.3.3 Kebolehsediaan

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

8.4 Penyelarasan Data & Maklumat melalui Jawatankuasa Pengurusan Maklumat (JKPM)

Peranan Jawatankuasa Pengurusan Maklumat (JKPM) adalah sebagaimana yang dinyatakan dalam **Bab 2: Dasar Pengurusan ICT**

8.5 Capaian Maklumat Rahsia Atau Sulit

8.5.1 Capaian Maklumat Rahsia Atau Sulit Oleh Pentadbir Sistem

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

8.5.1.2 Pentadbir Sistem mempunyai kuasa tanpa perlu mendapat kebenaran terlebih dahulu daripada pihak UMP untuk memantau kegiatan dan aktiviti pengguna yang melanggar Bab 9: Dasar Keselamatan ICT. Segala maklumat yang direkod boleh digunakan sebagai bukti. Sekiranya pelanggaran Dasar Keselamatan ICT tersebut serius seperti menggunakan identiti pengguna lain untuk mencuri data atau merosakkan sumber ICT. Bukti yang dikumpul akan dikemukakan kepada Jawatankuasa Penyelaras Keselamatan ICT UMP.

8.5.1.3 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 UMP boleh mencapai maklumat atau data sulit atau rahsia pengguna seperti emel atau fail yang tersimpan dalam akaunnya.

8.5.1.4 Pentadbir Sistem yang berpindah/bertukar PTJ perlu memaklumkan kepada PTMK bagi membolehkan PTMK membuat sekatan terhadap akses data atau maklumat yang sedia ada di PTJ asal bagi mengelakkan berlakunya capaian tanpa kebenaran.

8.5.2 Capaian Maklumat Rahsia Atau Sulit Oleh Pengguna

8.5.2.1 Pengguna ditegah menyimpan data atau maklumat sensitif, rahsia atau sulit di dalam komputer atau akaun pengguna tanpa kebenaran; dan

8.5.2.2 Pengguna diberi jaminan bahawa selain daripada perkara yang disebutkan di atas, 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 telah melanggar dasar ini.

8.6 Pemantauan Data Dalam Rangkaian

8.6.1 Pentadbir Rangkaian berkuasa untuk memantau dan merekodkan data-data yang berada dalam rangkaian sebagai sebahagian daripada rutin penjagaan keselamatan sumber

ICT. Peralatan rangkaian seperti *router* atau sistem komputer server yang menggunakan perisian-perisian tertentu mampu merekodkan data-data dalam rangkaian. Jaminan diberi bahawa data-data yang direkod tidak akan didedahkan melainkan jika berlaku kejadian pelanggaran Bab 10: Dasar Keselamatan ICT;

8.6.2 Sekiranya Pentadbir Rangkaian mengesyaki pengguna melanggar dasar ini, maka Pentadbir Rangkaian mempunyai mandat tanpa perlu mendapat kebenaran UMP untuk memantau dan merekodkan data-data dalam talian yang melibatkan aktiviti pengguna dengan lebih teliti. Data-data ini akan digunakan sebagai bahan bukti untuk proses pengauditan yang akan dilakukan oleh Jawatankuasa Keselamatan ICT UMP; dan

8.6.3 Pengguna diberi jaminan bahawa selain daripada perkara-perkara yang dinyatakan di atas, adalah menjadi kesalahan jika pengguna selain daripada Pentadbir Rangkaian memantau atau merekodkan data-data yang berada dalam rangkaian.

8.7 Larangan Terhadap Pengambilan Maklumat Sensitif

8.7.1 Sebarang keperluan data dan maklumat yang ingin dicapai dan diambil bagi tujuan mengguna, menghebah ataupun untuk tujuan prosedur di mana-mana keperluan yang dikenal pasti, perlu dimohon kepada pemilik data dan ia adalah tertakluk di bawah bidang kuasa Jawatankuasa Pengurusan Maklumat (JKPM).

8.7.2 Semua keperluan data dan maklumat yang sensitif hendaklah dinyatakan dengan jelas tujuan penggunaannya semasa permohonan mendapatkan maklumat dilakukan.

8.7.3 Maklumat kesihatan hanya boleh diambil oleh Pegawai Perubatan yang bertauliah namun masih tertakluk kepada kelulusan JKPM.

8.8 Maklumat Peribadi Yang Boleh Diambil Daripada Tuan Punya Maklumat

8.8.1 Maklumat peribadi berikut atau pun yang bersamaan dengannya boleh diambil:

i. Nama

ii. Gelaran

iii. Pusat Tanggungjawab (PTJ)

iv. Nombor Telefon

v. Alamat

8.8.2 Tujuan pengambilan dan penggunaan maklumat hendaklah di maklumkan kepada Tuan Punya Maklumat jika maklumat tersebut perlu dihebahkan untuk tujuan tertentu.

8.8.3 Hak untuk meminta capaian kepada maklumat peribadi dan hak untuk membuat pindaan atau pembetulan jika terdapat kesilapan hendaklah dimaklumkan kepada pemilik data tersebut.

8.9 Had Penggunaan Maklumat Peribadi

Maklumat peribadi mestilah digunakan untuk tujuan yang dinyatakan ketika maklumat itu diperoleh daripada Pemberi Maklumat dalam skop yang dibenarkan oleh UMP:

Penggunaan maklumat peribadi yang telah diambil mestilah mengikut syarat berikut:

i. Tuan Punya Maklumat telah memberi kebenaran menggunakan maklumat tersebut; maklumat boleh digunakan sebagai pengesahan sesuatu kontrak.

ii. maklumat boleh digunakan untuk tujuan mahkamah atau perundangan.

iii. maklumat boleh digunakan untuk melindungi tuan punya maklumat dalam semua perkara.

8.10 Penyelenggaraan Penggunaan Maklumat Peribadi

8.10.1 Universiti Malaysia Pahang (UMP) bertanggungjawab memastikan ketepatan maklumat peribadi semasa dalam simpanan dan sentiasa dikemas kini untuk tujuan yang diperlukan. Maklumat rahsia atau sulit perlu dikemas kini dari semasa ke semasa mengikut keperluan.

8.10.2 Universiti Malaysia Pahang (UMP) bertanggungjawab menjamin keselamatan maklumat yang disimpan dengan mematuhi Dasar Keselamatan ICT.

8.10.3 UMP bertanggungjawab menjamin kerahsiaan maklumat peribadi. Individu yang bertanggungjawab menyimpan, mengumpul atau memproses data mestilah memastikan maklumat peribadi tidak disebarkan kepada pihak lain, selain daripada mereka yang mempunyai hak untuk mengetahui maklumat tersebut.

8.10.4 Permintaan untuk mencapai maklumat peribadi oleh tuan punya maklumat untuk tujuan pengesahan mestilah diberi untuk satu tempoh yang berpatutan. Jika terdapat kesilapan maklumat ketika diperiksa oleh Tuan Punya Maklumat, pemilik data tersebut hendaklah diberitahu.

8.10.5 Pengurus maklumat mestilah memahami dan mematuhi Dasar ini dan bertanggungjawab untuk memaklumkan kepada pemberi maklumat tentang dasar ini.

8.10.6 Pemakluman oleh pemilik sistem perlu dilakukan kepada pihak PTMK sebelum proses pertukaran pemilik sistem berlaku.