1.0 TUJUAN

Garis panduan ini bertujuan untuk menerangkan cara mengendalikan insiden keselamatan ICT untuk menangani insiden ICT atau pelanggaran keselamatan dan meminimumkan kerosakan akibat insiden keselamatan dan kegagalan fungsi (*malfunction*).

2.0 SKOP

Merangkumi semua *server* yang berada di Pusat Data (DC) dan Pusat Pemulihan Bencana (DRC) Universiti Putra Malaysia.

3.0 PANDUAN

Bil	Tindakan	Tanggungjawab
1.	Menerima aduan daripada saluran yang betul atau daripada Pentadbir Sistem.	PYB
2.	2.1 Menjalankan siasatan terhadap kes insiden ICT yang diterima dengan menggunakan perisian sokongan untuk menganalisa log yang berkaitan. 2.2 Langkah siasatan terhadap kes adalah seperti berikut: i. Menganalisis dan mengenal pasti punca kejadian; dan ii. Mengumpul jejak audit dan bukti berkaitan.	Pekerja ICT Pekerja ICT

3.	3.1 Melaporkan hasil penemuan siasatan kepada UPMCERT, JKKTMK dan Pentadbir Sistem dengan menyertakan laporan insiden ICT dan laporan imbasan. 3.2 Langkah laporan insiden ICT adalah seperti berikut: i. Pekerja ICT perlu mengisi Laporan pada Borang Maklumat Pengendalian Insiden Keselamatan ICT (UPM/ISMS/OPR/IRH 1.0); dan ii. Pentadbir Sistem perlu mengisi Borang Maklumbalas Tindakan Susulan dari Pengendalian Insiden Keselamatan ICT (UPM/ISMS/OPR/IRH 1.1). 3.3 Langkah laporan imbasan adalah seperti berikut: i. Pekerja ICT perlu mengisi Borang Maklumat Imbasan *Server/Host* (UPM/ISMS/OPR/IRH 2.0); dan ii. Pentadbir Sistem perlu mengisi Borang Maklumbalas Tindakan Susulan Imbasan *Server/Host* (UPM/ISMS/OPR/IRH 2.1).	Penyelia/ Pentadbir Sistem / Pekerja ICT Pekerja ICT/ Pentadbir Sistem Pekerja ICT / Pentadbir Sistem
4.	4.1 Semua insiden ICT yang berlaku hendaklah direkodkan ke dalam Log Pengendalian Insiden (UPM/ISMS/OPR/IRH 1.2). 4.2 Semua insiden keselamatan ICT yang dikesan hendaklah mempunyai sekurang-kurangnya maklumat seperti berikut: i. Tarikh dan masa insiden ICT; ii. Menyenaraikan sistem yang terjejas akibat Insiden ICT atau kejadian tersebut; iii. Ringkasan insiden ICT; iv. Tindakan yang diambil untuk membetulkan insiden ICT; dan v. Senarai bukti yang diperolehi semasa siasatan	Pekerja ICT Pekerja ICT