# Borang IRH 1.0:

**Maklumat Pengendalian Insiden Keselamatan ICT**

Tarikh Pengendalian: Masa Pengendalian:

| **A. *Computer Emergency Response*** | |
|---|---|
| *No. Insiden | Tahun/Bulan/Kod Kategori/Bil insiden dalam tahun semasa (Sila rujuk Lampiran A) |
| *Tarikh & Masa Dikesan | |
| **B. Maklumat Jabatan/ Agensi** | |
| ICTSO<br>1. Nama<br>2. E-mel<br>3. Jawatan dan Gred<br>4. No. Telefon Pejabat<br>5. No. Telefon Bimbit | |
| Pentadbir Sistem<br>1. Nama<br>2. E-mel<br>3. Jawatan dan Gred<br>4. No. Telefon Pejabat<br>5. No. Telefon Bimbit | |
| Pegawai Perhubungan<br>1. Nama<br>2. E-mel<br>3. Jawatan dan Gred<br>4. No. Telefon Pejabat<br>5. No. Telefon Bimbit | |
| Alamat Penuh Agensi | |
| Bahagian/Unit Yang Melapor | |
| No. Telefon Agensi | |
| No. Faks | |

| **C. Maklumat Perkakasan dan Perisian Yang Terlibat** |
|---|
| Hostname |
| Domain |
| DNS |
| Alamat IP<br>1. Internal<br>2. External |
| Sistem Pengoperasian<br>1. Jenis<br>2. Versi<br>3. Service pack |
| Kapasiti Disk |
| Jenis *Hard Disk* |
| Sistem Aplikasi / Perkhidmatan lain |
| **D. Maklumat Insiden** |
| Alamat IP Penyerang |
| Jenis Insiden (cth: pelanggaran dasar, pencerobohan) : |
| Jenis Serangan |
| **E. Tindakan Yang Diambil Oleh Unit ICT** |
| |

**Lampiran A**

## Jenis Insiden Keselamatan ICT

| Kod Kategori | Jenis Insiden | Penerangan |
|---|---|---|
| 01 | Pelanggaran Dasar (Violation of Policy) | Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar Dasar Keselamatan ICT. |
| 02 | Penghalangan Penyampaian Perkhidmatan (Denial of Service) | Ancaman ke atas keselamatan sistem komputer di mana perkhidmatan pemprosesan maklumat sengaja dinafikan terhadap pengguna sistem. Ia melibatkan sebarang tindakan yang menghalang sistem daripada berfungsi secara normal. Termasuk *denial of service* (DoS), *distributed denial of service* (DDoS) dan *sabotage*. |
| 03 | Pencerobohan (Intrusion) | Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem (system tampering), pindaan data (modification of data) dan pindaan kepada konfigurasi sistem. |
| 04 | Pemalsuan (Forgery) | Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage) dan penipuan (hoaxes). |
| 05 | Spam | Spam adalah emel yang dihantar ke akaun emel orang lain yang tidak dikenali penghantar dalam satu masa dan secara berulang-kali (kandungan emel yang sama). Ini menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan. |
| 06 | Malicious Code | Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya. |
| 07 | Harrassment/Threats | Gangguan dan ancaman melalui pelbagai cara iaitu emel dan surat yang bermotif personal dan atas sebab tertentu. |
| 08 | Attempts/Hack Threats/Information Gathering | Percubaan (samada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran. Termasuk *spoofing, phishing, probing, war drivin*g dan *scanning*. |
| 09 | Kehilangan Fizikal (Physical Loss) | Kehilangan capaian dan kegunaan disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT berpunca daripada ancaman pencerobohan. |