* 1. **PENGENALAN**

Kriptografi moden kini menghadapi ancaman serius daripada kemunculan teknologi pengkomputeran kuantum. Agensi-agensi seperti *National Institute of Standards and Technology* (NIST) dan *European Union Agency for Cybersecurity* (ENISA) telah menggariskan keperluan untuk pemindahan daripad algoritma kriptografi klasik kepada algoritma kriptografi pascakuantum (PQC). PTPKM bertanggungjawab memastikan semua sistem kriptografi yang digunakan di Malaysia bersedia dan selamat dalam meghadapi ancaman kuantum ini.

1. **TUJUAN**

Polisi ini bertujuan untuk:

1. Menyediakan rangka kerja bagi pelaksanaan dan pemindahan kepada algoritma PQC.
2. Memastikan sistem maklumat negara kekal terlindung daripada ancaman komputer kuantum.
3. Menetapkan keperluan pematuhan kepada piawaian antarabangsa dalam pelaksanaan PQC.
4. **SKOP**

Polisi ini terpakai kepada:

1. Semua sistem kerajaan dan organisasi yang bergantung pada kriptografi untuk perlindungan data.
2. Vendor dan pembekal yang terlibat dengan pembangunan, intergrasi dan penyelenggaraan sistem berkaitan keselamatan.
3. Semua produk keselamatan siber ynag digunakan oleh agensi awam dan swasta yang berkaitan dengan infrastruktur kritikal.
4. **TANGGUNGJAWAB**
5. **DOKUMEN RUJUKAN**

|  |  |
| --- | --- |
| **Kod Dokumen** | **Tajuk Dokumen** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. **TERMINOLOGI DAN SINGKATAN**

|  |  |  |
| --- | --- | --- |
| PTPKM | : | Pusat Teknologi dan Pengurusan Kriptologi Malaysia |
| KS | : | Ketua Seksyen yang bertugas di Seksyen iDEC yang  dipertanggungjawabkan |
| Pembekal | : | Pembekal sah yang dilantik oleh iDEC untuk kerja-kerja perkhidmatan dan penyelenggaraan |
| PYB | : | Pekerja Yang Bertanggungjawab |
| Pekerja ICT | : | Pegawai Teknologi Maklumat/Jurutera/Penolong Pegawai  Teknologi Maklumat/Penolong Jurutera/Juruteknik Komputer/Pekerja lain yang dilantik untuk mengurus ICT |
| Pentadbir Sistem | : | Pegawai Teknologi Maklumat/Jurutera/Penolong Pegawai Teknologi Maklumat/Penolong Jurutera/Juruteknik Komputer/Pekerja lain yang mengurus operasi atau aktiviti berkaitan  pengoperasian aplikasi, telekomunikasi serta pengurusan sistem pangkalan data Universiti. |
| TPKD | : | Timbalan Pegawai Kawalan Dokumen |
| TWP | : | Timbalan Wakil Pengurusan |
| WP  PQC | :  : | Wakil Pengurusan  *Post-Quantum Cryptography* – algoritma tahan serangan komputer kuantum. |

1. **KENYATAAN POLISI**
   1. **INVENTORI KRIPTOGRAFI**
2. Melaksanakan inventori menyeluruh terhadap system yang menggunakan kriptografi.
3. Klasifikasikan mengikut tahap kepekaan dan kepentingan.
   1. **PENILAIAN RISIKO**
4. Jalankan analisis risiko terhadap algoritma kriptografi sedia ada.
5. Kenal pasti sistem yang paling terdedah kepada ancaman kuantum.
   1. **PEMILIHAN ALGORITMA**
6. Gunakan algoritma yang telah diluluskan oleh NIST seperti CRYSTALS-Kyber dan Dilithium.
7. Elakkan penggunaan hibrid melainkan dengan kelulusan keselamatan rasmi.
   1. **PELAN MIGRASI**

Menyediakan pelan migrasi terperinci yan meliputi:

* 1. Penemuan
  2. Ujian
  3. Integrasi
  4. Pengeluaran
  5. Pemantauan

* 1. **UJIAN DAN PENGESAHAN**

1. Menyediakan persekitaran ujian untuk menilai prestasi algoritma PQC.
2. Mengesahkan pematuhan kepada piawaian keselamatan yang berkenaan.
   1. **PENGURUSAN VENDOR**
3. Mewajibkan vendor menyatakan kesiapsiagaan mereka terhadap PQC.
4. Memasukkan keperluan sokongan PQC dalam perolehan baru.
   1. **KOMUNIKASI SELAMAT**

Tingkatkan kepada TLS yang menyokong PQC.

Ubah suai saluran komunikasi selamat seperti VPN, emel dan pengesahan pengguna.

* 1. **KESEDARAN DAN LATIHAN**

Memberi latihan berkala kepada staf teknikal dan pentadbir sistem.

Dokumentasikan proses dan kemas kini prosedur operasi.

1. **PENGUATKUASAAN**

Kegagalan mematuhi polisi ini boleh dikenakan tindakan tatatertib, termasuk penggantungan akses system atau tindakan undang-undang mengikut keseriusan pelanggaran.

1. **SEMAKAN SEMULA**

Polisi ini akan disemak setiap tahun atau apabila berlaku perubahan besar dalam terknologi kuantum atau piawaian PQC dan NIST.

1. **LAMPIRAN**