	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI PEMBANGUNAN MAKLUMAT DAN MALAYSIA Kod Dokumen: UPM/	Halaman: 1/11
		No. Semakan: 09
		No. Isu: 01
	PELAN PEMULIHAN BENCANA	Tarikh: 31/01/2023


1.0 SKOP

Polisi ini bertujuan untuk memastikan ketahanan, ketersediaan, dan pemulihan infrastruktur dan perkhidmatan Kriptografi Pasca-Kuantum (PQC) dalam organisasi. Polisi ini terpakai untuk semua unit organisasi, kakitangan, dan penyedia pihak ketiga yang mengurus, mengekalkan, atau mengakses sistem, data, atau infrastruktur yang berkaitan dengan PQC. Polisi ini merangkumi:

- Sistem pengurusan dan penjaanaan kunci berasaskan PQC.
- Mekanisme tandatangan dan pengesahan kriptografi.
- Infrastruktur komunikasi yang dilindungi PQC (contohnya VPN, TLS, mesej terenkripsi).
- Semua sistem (berdasarkan premise dan awan) yang mengendalikan operasi PQC dan sandaran.
- Semua kakitangan, kontraktor, dan penyedia pihak ketiga yang terlibat dalam persekitaran PQC.


2.0 TANGGUNGJAWAB

PERANAN	TANGGUNGJAWAB
Pegawai PQC	Memastikan pelaksanaan PQC yang selamat dan integriti kunci kriptografi.
Pasukan Operasi IT	Melaksanakan prosedur sandaran, pemulihan, dan pemulihan bencana.
Ketua Pemulihan Bencana	Mengaktifkan dan menyelaraskan Pelan DR semasa gangguan.
Pengurus Kelangsungan Perniagaan	Mengurus dan menguji rangka kerja kelangsungan perniagaan.
Pasukan Keselamatan	Menyiasat insiden dan menguatkuasakan langkah perlindungan.
Pegawai Pematuhan	Memastikan pematuhan kepada piawaian dan polisi yang berkaitan.

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 3/11
		No. Semakan: 09
		No. Isu: 01
	POLISI XXXX	Tarikh: 31/01/2023

4.0 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	: Wakil Pengurusan
PQC	: Kriptografi Pasca-Kuantum
DRP	: Pelan untuk memulihkan sistem IT dan data selepas kejadian bencana.
BCP	: Strategi untuk mengekalkan operasi penting semasa dan selepas gangguan.
Sandaran	: Salinan data yang disimpan secara berasingan daripada data asal bagi membolehkan pemulihan.
RTO	: Masa henti maksimum yang boleh diterima.
RPO	: Kehilangan data maksimum yang boleh diterima.

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 4/11
		No. Semakan: 09
		No. Isu: 01
	POLISI XXXX	Tarikh: 31/01/2023

5.0 RISIKO

- Ketidakupayaan untuk menyambung semula operasi dalam masa yang ditetapkan
- Kehilangan data dan maklumat kritikal
- Gangguan operasi dan kehilangan kepercayaan pihak berkepentingan
- Kerugian kewangan dan kerosakan reputasi organisasi

6.0 PERNYATAAN DASAR

Dasar berikut menetapkan bagaimana PTPKM akan mengurus pemulihan bencana, sandaran data, dan kesinambungan perniagaan:

6.1 SANDARAN DATA

6.1.1 KEKERAPAN DAN SKOP SANDARAN

- Sandaran harian dan sandaran penuh mingguan untuk semua data.

6.1.2 PENYIMPANAN DAN PENYULITAN


- Semua sandaran disulitkan dengan skema penyulitan yang sejajar dengan PQC.
- Sandaran akan disimpan sekurang-kurangnya di dua lokasi yang berbeza secara geografi dan selamat (berdasarkan premise dan awan).
- Sandaran berasaskan awan mesti menggunakan kawalan akses yang dikukuhkan dengan PQC dan API *endpoint*.

6.1.3 PENYIMPANAN DAN PEMUSNAHAN

- Sandaran disimpan sekurang-kurangnya selama 12 bulan.
- Sandaran yang lebih lama dan telah tamat tempoh akan dipadamkan dengan selamat.
- Pemusnahan mesti mengikuti prosedur penghapusan yang selamat.

6.1.4 UJIAN DAN PENGESAHAN

- Proses sandaran hendaklah dipantau dan disahkan secara berkala untuk memastikan integriti dan kelengkapan.
- Ujian pemulihan hendaklah dilakukan setiap suku tahun bagi mengesahkan kebolegunaan data sandaran.

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 5/11
		No. Semakan: 09
		No. Isu: 01
	POLISI XXXX	Tarikh: 31/01/2023

6.2 PEMULIHAN BENCANA (DR)

6.2.1 OBJEKTIF DR

- **Objektif Masa Pemulihan (RTO):** 4 jam untuk sistem PQC kritikal.
- **Objektif Titik Pemulihan (RPO):** 15 minit untuk penjanaan dan pengesahan kunci.

6.2.2 KRITERIA PENGAKTIFAN

- Bencana alam
- Gangguan perkhidmatan yang berpanjangan
- Pelanggaran keselamatan yang mempengaruhi sistem PQC
- Kegagalan perkakasan atau perisian yang melibatkan infrastruktur PQC.

6.2.3 *FAILOVER* DAN *REDUNDANCY*

- Pemindahan automatik ke sistem sekunder dengan konfigurasi PQC yang digandakan.
- Perkhidmatan PQC akan dikontainerkan dan mampu melakukan *failover* tanpa status melalui platform orkestrasi (contohnya, Kubernetes).
- Tapak sejuk, suam, atau panas akan tersedia berdasarkan keutamaan sistem.

6.2.4 UJIAN DAN SEMAKAN DRP

- Ujian DR akan dijalankan setiap enam bulan.
- Penilaian pasca-ujian dan pelajaran yang diperoleh akan didokumenkan dan digunakan untuk mengemas kini prosedur.
- Kemudahan alternatif, pemulihan awan, atau sistem berlebihan beban (*overload*) hendaklah digunakan apabila perlu.

6.3 KESINAMBUNGAN PERNIAGAAN (BC)

6.3.1 FUNGSI PQC KRITIKAL

- Penjanaan dan pengedaran kunci.
- Pengesahan sijil dan operasi tandatangan digital.
- Komunikasi selamat berasaskan PQC.

6.3.2 LANGKAH KELANGSUNGAN

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 6/11
		No. Semakan: 09
		No. Isu: 01
	POLISI XXXX	Tarikh: 31/01/2023

- Kemampuan kerja jarak jauh menggunakan penyelesaian akses jauh (*remote access*) yang dilindungi PQC.
- Lokasi operasi alternatif yang telah dikonfigurasi dengan aset kriptografi.
- Replikasi konfigurasi dan kawalan akses dalam persekitaran sekunder.

6.3.3 KESIAPSIAGAAN TENAGA KERJA

- Kakitangan utama dilatih dalam tindak balas kecemasan dan pemulihan kriptografi.
- Pelan penggantian disediakan untuk peranan kepimpinan teknikal PQC.
- Prosedur kelangsungan dimasukkan dalam program latihan semasa pengambilan dan tahunan.

7.0 PEMATUHAN DAN PIAWAIAN

- **ISO/IEC 27001:** Pengurusan Keselamatan Maklumat
- **ISO/IEC 22301:** Pengurusan Kelangsungan Perniagaan
- **NIST SP 800-160:** Kejuruteraan Keselamatan Sistem
- **NIST SP 800-208:** Syor bagi Skim Tandatangan Digital Berdasarkan Fungsi Hash
- **Piawaian PQC NIST:** Piawaian kriptografi yang tahan terhadap kuantum yang sedang berkembang

8.0 PEMATUHAN DAN PEMANTAUAN

Audit dalaman akan dilaksanakan secara berkala (cth: tahunan atau separuh tahunan) bagi memastikan pmatuhan terhadap polisi ini. Audit akan merangkumi aspek dokumentasi semakan kod, pmatuhan terhadap senarai semakan pengekodan selamat, penggunaan alat automasi keselamatan, dan rekod latihan pembangun.

9.0 SEMAKAN DAN KEMASKINI POLISI

Polisi ini akan disemak sekurang-kurangnya sekali setahun atau apabila berlaku perubahan ketara dalam teknologi, peraturan atau sistem dalaman. Sebarang perubahan yang diluluskan mesti dimaklumkan kepada semua pihak yang berkaitan dan didokumentasikan secara rasmi.

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 7/11
		No. Semakan: 09
		No. Isu: 01
	POLISI XXXX	Tarikh: 31/01/2023

10.0 MAKLUMAT PERHUBUNGAN

NAMA	JAWATAN	EMEL	NO. TELEFON
	Ketua Pemulihan Bencana		
	Pegawai PQC		
	Pasukan Operasi IT		
	Pengurus Kelangsungan Perniagaan		
	Pasukan Keselamatan		
	Pegawai Pematuhan		

KELULUSAN

Nama:


Jawatan:

Tandatangan:

Tarikh:

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 8/11
		No. Semakan: 09
		No. Isu: 01
	POLISI XXXX	Tarikh: 31/01/2023

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 9/11
		No. Semakan: 09
		No. Isu: 01
	POLISI XXXX	Tarikh: 31/01/2023

	POLISI, PERUNDANGAN DAN KESEDARAN		Halaman: 10/11
	PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA		No. Semakan: 09
	Kod Dokumen: UPM/		No. Isu: 01
	POLISI XXXX		Tarikh: 31/01/2023

11.0 LAMPIRAN


Dokumen Operasi dan Pengurusan PQC

1. Jadual Senarai Sistem PQC Kritikal

Tujuan:

Jadual ini menyenaraikan sistem yang menggunakan atau akan menggunakan algoritma Kriptografi Pascakuantum (PQC) dan dikategorikan sebagai sistem kritikal berdasarkan impak kepada keselamatan dan operasi organisasi.

Bil	Nama Sistem	Jenis Algoritma PQC	Tahap Kritikaliti	Tarikh Penilaian Terakhir	Status Terkini	Catatan
1	Sistem E-Mel Rasmi (SecureMail)	Kyber (Key Encapsulation)	Tinggi	01/03/2025	Dalam Operasi	Tiada insiden
2	Sistem Tandatangan Digital	Dilithium (Signature)	Tinggi	15/02/2025	Dalam Pemantauan	Ujian kestabilan berterusan
3	Rangkaian VPN Organisasi	BIKE	Sederhana	20/01/2025	Diperlukan Naik Taraf	Algoritma sedang dinilai
4	Sistem Penyimpanan Awan (CloudSafe)	FrodoKEM	Tinggi	10/03/2025	Stabil	Audit dijadualkan Mei 2025

	POLISI, PERUNDANGAN DAN KESEDARAN PUSAT TEKNOLOGI DAN PENGURUSAN KRIPTOLOGI MALAYSIA Kod Dokumen: UPM/	Halaman: 11/11
		No. Semakan: 09
		No. Isu: 01
	POLISI XXXX	Tarikh: 31/01/2023

2. Prosedur Pemulihan Kunci Kriptografi PQC

1. Pengenalpastian Insiden Kerosakan atau Pendedahan Kunci:

- Analisis audit log dan pemantauan tingkah laku abnormal dalam sistem PQC.

2. Penahanan Sementara Sistem Terjejas:

- Gantung sementara sambungan PQC
- Alihkan kepada mod fallback dengan kriptografi hibrid (jika tersedia)

3. Pemulihan Kunci:

- Buang kunci terjejas secara selamat
- Jana dan edarkan kunci baharu menggunakan HSM atau modul keselamatan lain
- Daftarkan semula kunci baharu dalam sistem verifikasi pihak ketiga (jika digunakan)

4. Dokumentasi & Pengesahan:

- Catat semua langkah pemulihan dalam log pemulihan
- Jalankan audit keselamatan segera selepas pemulihan

5. Notifikasi Kepada Pihak Berkaitan:

- Pihak pengurusan keselamatan
- Pusat Respons Insiden Siber (CSIRT)
- Pihak pengguna terjejas (jika perlu)