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

2. Laporan Insiden PQC – Rekod Terkini

Maklumat Insiden:
- Tarikh & Masa: 4 April 2025, 11:43 pagi
- Sistem Terjejas: SecureMail (Sistem E-Mel Rasmi)
- Jenis Insiden: Gagal rundingan kunci PQC (Kyber) akibat ralat konfigurasi
- Deskripsi: Kegagalan dalam pengesahan kunci awam menyebabkan kegagalan penghantaran mesej terenkripsi selama 47 minit.

Tindakan Segera:
- Konfigurasi semula parameter kunci
- Penyelarasan semula modul PKI dalaman
- Pelaksanaan ujian menyeluruh selepas pembetulan

Punca Insiden:
Kesalahan semasa integrasi modul PQC baru dengan sistem penghantaran e-mel.

Dampak:
Gangguan komunikasi kepada 3 jabatan utama. Tiada kehilangan data.

Langkah Pencegahan:
- Latihan teknikal lanjutan untuk kakitangan keselamatan siber
- Prosedur pengujian regresi wajib bagi setiap kemas kini

3. 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)

4. Senarai Kontak Pasukan DRP PQC

Nama	Jawatan	Telefon	E-mel	Tanggungjawab
Azmi Zakaria	Ketua DRP PQC	012-3456789	azmi.z@ptpkm.gov.my	Koordinasi keseluruhan pemulihan

Nur Aisyah Halim	Pegawai Keselamatan Siber	019-8765432	aisyah.h@ptpkm.gov.my	Audit & pemantauan sistem
Farid Johan	Jurutera Kriptografi	013-1234567	farid.j@ptpkm.gov.my	Pemulihan & konfigurasi kunci
Lim Wei Shen	Sokongan Infrastruktur	016-7890123	lim.w@ptpkm.gov.my	Sambungan rangkaian & sistem sokongan
Rosnah Mohd Ali	Wakil CSIRT	017-4567890	rosnah.ma@csirt.gov.my	Pengesanan insiden & eskalasi