1.0 SKOP

Polisi ini terpakai kepada sistem, aplikasi dan individu yang terlibat dalam penjanaan, pengedaran, penyimpanan, penggunaan, pembatalan dan pemusnahan kunci kriptografi.

2.0 TANGGUNGJAWAB

Polisi ini ditujukan kepada pentadbir IT, pegawai keselamatan, pembangun sistem, serta kakitangan yang terlibat dalam keselamatan sistem dan rangkaian. Ia juga terpakai kepada pasukan audit dalaman dan pihak pengurusan yang bertanggungjawab dalam perlindungan data dan mitigasi risiko.

3.0 DOKUMEN RUJUKAN

Kod Dokumen	Tajuk Dokumen

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 TeknologiMaklumat/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
HSM	:	*Hardware Security Module*
MySEAL	:	*National Trusted Cryptographic Algorithm List* (Senarai Algorithma Kriptografi Terpercaya Negara)
NIST	:	*National Institute of Standards and Technology*
CKMS	:	*Cryptographic Key Management System*
CA	:	*Certificate Authority* (Pihak Berkuasa Sijil)
FIPS	:	*Ferderal Information Processing Standards*
MFA	:	*Multi-Factor Authentication*
RBAC	:	*Role-based Access Control*

5.0 KITAR HAYAT PENGURUSAN KUNCI DAN PELAKSANAAN TEKNIKAL

5.1 Penjanaan Kunci (Key Generation)

- Kunci mestilah dijana menggunakan algoritma yang mematuhi piawaian keselamatan yang diluluskan, seperti MySEAL atau piawaian yang ditetapkan oleh Institut Piawaian dan Teknologi Kebangsaan (NIST).
- Semua kunci kriptografi mestilah dijana dalam persekitaran yang selamat seperti Hardware Security Modules (HSMs) atau melalui medium pengurusan kunci yang lain.
- Bagi pengurusan kunci, adalah disarankan untuk mengintegrasikan Cryptographic Key Management System (CKMS) dengan Hardware Security Modules (HSMs) bagi memastikan kawalan berpusat, pengurusan kitar hayat kunci secara automatik, dan tahap keselamatan yang lebih tinggi.
    - Pasangan kunci statik asimetri mestilah dijana menggunakan salah satu kaedah yang diluluskan berikut:
        - Oleh pemilik kunci yang akan menggunakan kunci peribadi tersebut.
        - Oleh fasiliti yang diberi kuasa dan dipercayai, yang bertanggungjawab terhadap penjanaan dan pengedaran kunci secara selamat.
        - Melalui proses yang diselaraskan antara pemilik kunci dan fasiliti yang dipercayai.
- Akses kepada proses penjanaan kunci mestilah dihadkan kepada pihak yang sah. Dalam persekitaran yang sensitif, kawalan dua pihak (*dual control*) adalah diwajibkan bagi meningkatkan keselamatan dan akauntabiliti.
- Metadata kunci (contohnya: tarikh penjanaan, algoritma, panjang kunci, dan tujuan penggunaan) mestilah disimpan secara selamat dalam *Cryptographic*

Key Management System (CKMS) bagi tujuan pengauditan dan rujukan keselamatan.

5.2 Pengedaran Kunci (Key Distribution)

- Kunci mesti diedarkan melalui saluran yang selamat seperti komunikasi yang disulitkan
- Kunci hanya boleh diberikan kepada pihak yang mempunyai keperluan sah untuk akses.
- Kunci mesti dilindungi semasa dalam transit dan semasa dalam penyimpanan. Penyulitan (Encryption) harus digunakan ke atas kandungan dan medium penghantaran.
- Kunci hanya boleh diedarkan kepada organisasi atau peranti yang sah dan memerlukannya untuk operasi kriptografi yang diluluskan.
- Akses kepada kunci semasa pengedaran mesti dikawal, direkodkan, dan dipantau bagi memastikan pematuhan terhadap dasar keselamatan.
- Pengedaran kunci simetri dan asimetri mesti menggunakan mekanisme yang berasingan.
- Data yang disulitkan dan kunci penyulitannya tidak boleh dihantar bersama, kecuali jika kunci tersebut dilindungi melalui kaedah penyulitan tambahan seperti penyulitan kunci awam.
- Penerima mesti mengesahkan penerimaan kunci dan memastikan integriti kunci tersebut.
- Pengedaran kunci baharu mesti dilakukan secara berkala, terutamanya selepas penggiliran atau tamat tempoh dan hendaklah mengikut jadual penggiliran kunci yang telah ditetapkan.
- Pengedaran kunci baharu mesti dilakukan secara berkala selepas tamat tempoh.
- Apabila kunci dibatalkan atau terjejas, pengedaran kunci mesti dihentikan

serta-merta dan semua penerima kunci mestilah dimaklumkan sewajarnya..

5.3 Penyimpanan Kunci (Key Storage)

- Kunci mesti disimpan dalam FIPS XXXX (atau setara dengannya) Hardware Security Module (HSM) yang diperakui.
- Pangkalan data kunci mesti disulitkan menggunakan algoritma yang diluluskan secara nasional (contohnya, MySEAL) atau piawaian yang diiktiraf secara global (contohnya, NIST, FIPS XXXX).
- Kawalan akses mesti mengikuti prinsip keperluan minimum, membenarkan hanya kakitangan yang diberi kuasa. Semua akses mesti direkodkan dan boleh diaudit.
- Kunci simetri dan asimetri mesti disimpan secara berasingan menggunakan mekanisme yang berasingan untuk mengelakkan pendedahan tidak sengaja atau penyalahgunaan.
- Kunci yang digunakan untuk tujuan tidak boleh disangkal mesti dikawal sepenuhnya oleh pengguna.
- Salinan sandaran kunci mesti disulitkan dan disimpan di lokasi yang berbeza dan selamat. Proses pemulihan mestilah memastikan hanya kakitangan yang diberi kuasa sahaja boleh melaksanakan *restoration*.
- Salinan sandar *(backup copies)* mesti disulitkan dan disimpan di lokasi yang selamat dan berlainan geografi. Proses pemulihan hanya boleh dilakukan oleh kakitangan bertanggungjawab. Salinan sandar (backup copies) perlu melalui proses encryption dan disimpan di lokasi yang selamat. Proses restoration hanya boleh dilakukan oleh kakitangan yang diberi kuasa.

5.4 Penggunaan Kunci (Key Usage)

- Kunci hanya boleh digunakan untuk tujuan yang ditetapkan.

- Satu kunci hanya boleh digunakan untuk satu tujuan sahaja.
- Penggunaan kunci tanpa kebenaran adalah tidak dibenarkan sama sekali.
- Setiap kunci mesti mempunyai tempoh yang sah yang ditetapkan. Bagi kunci asimetri, kunci awam dan kunci peribadi mestilah mempunyai tempoh sah masing-masing.
- Kunci mestilah digunakan dalam persekitaran yang selamat seperti dalam peranti kriptografi selamat seperti HSM.
- Sistem automatik yang mengendalikan penggunaan kunci mesti dikonfigurasi untuk memastikan pematuhan terhadap dasar keselamatan yang diluluskan dan sekatan kawalan akses.
- Penggunaan kunci mesti dipantau secara berterusan untuk mengesan aktiviti anomali dan penyalahgunaan. Log mesti disemak secara berkala untuk tujuan pematuhan dan pengauditan keselamatan.

5.5 Pembatalan Kunci (Key Revocation)

- Kunci dibatalkan jika berlaku:
  - Pelanggaran keselamatan atau kompromi
  - Tamat tempoh kunci
  - Perubahan kakitangan atau jawatan yang memberi impak kepada akses kunci.
  - Pelanggaran polisi atau ralat dalam operasi.
- Kunci yang dibatalkan mesti:
  - Berada dalam status tidak aktif dalam *CKMS.*
  - Dikeluarkan daripada senarai kawalan akses.
  - Digantikan dengan kunci baru yang dijanakan jika perlu bagi kesinambungan operasi.
- *Certificate Revocation List (CRL)* dan *Online Certificate Status Protocol (OCSP)*

digunakan bagi menyekat penggunaan kunci yang telah tamat tempoh atau dibatalkan.

- Semua sistem dan pengguna yang mempunyai akses kepada kunci yang telah dibatalkan mesti dihentikan aksesnya secara serta-merta.

  Kakitangan yang diberi kuasa mesti dimaklumkan serta-merta apabila sesuatu kunci dibatalkan, dan pembatalan tersebut hendaklah didokumenkan bagi tujuan pengauditan.

5.6 Pemusnahan Kunci (Key Destruction)

- Kunci mesti dimusnahkan apabila:
  - Ia tidak lagi diperlukan.
  - Tempoh sah kriptografi telah tamat.
  - Ia telah dibatalkan dan tidak akan digunakan.
- Kunci yang disimpan dalam HSM atau storan selamat perlu dimusnahkan menggunakan menggunakan kaedah yang selamat dan arahan atau fungsi di dalam peranti tersebut.
- Mekanisme kriptografi selamat yang menjana kunci juga mesti dimusnahkan sekiranya kunci tersebut telah diedarkan secara *secret shares* atau fragmen.
- Maklumat yang diperlukan untuk mencipta semula kunci masih disimpan di lokasi operasi sehingga ia dihentikan atau dipadamkan.
- Pemusnahan bagi *master key* mesti dilaksanakan melalui kawalan *dual control.*
- Proses pemusnahan mesti direkod dengan tarikh, ID kunci dan kakitangan yang bertanggungjawab.
- Process pemusnahan ini perlu diaudit secara berkala bagi memastikan pematuhan kepada keperluan standard yang telah ditetapkan.

5.7 Kawalan Akses Kunci

- Pengesahan berbilang faktor *(MFA)* mesti dilaksanakan untuk semua pengguna dan sistem yang mengakses kunci kriptografi.
- Kawalan akses berasaskan peranan *(RBAC)* dan prinsip keperluan minimum *(Principle of Least Privilege)* dikuatkuasakan supaya hanya pengguna dan sistem yang sah memiliki akses kepada kunci yang disimpan.
- Akses kepada kunci yang sensitif seperti *master key* atau kunci *CA* persendirian mesti menggunakan kawalan dua pihak untuk memastikan kunci sensitif tidak boleh diakses dan digunakan oleh salah satu pihak tanpa pengetahuan pihak lain.
- Semua akses kepada kunci kriptografi perlu direkodkan termasuk identiti pengguna/sistem, cap masa dan tindakan yang diambil.
- Semakan berkala perlu dilaksanakan bagi memastikan hanya individu yang sah mempunyai akses.
- Hak akses kunci mesti dibatalkan serta-merta jika berlaku perubahan peranan kakitangan, penamatan perkhidmatan, terdapat kecurigaan kompromi.
- Akses secara remote diberikan dengan menggunakan protokol selamat seperti VPN atau TLS.

6.0 PEMATUHAN DAN PEMANTAUAN

6.1 Audit Berkala

Audit dalaman akan dilaksanakan secara berkala (cth: tahunan atau separuh tahunan) bagi memastikan pematuhan terhadap polisi ini. Audit akan merangkumi aspek penjanaan, kawalan akses dan pemusnahan kunci serta integriti log audit.

6.2 Latihan

Kakitangan yang berkaitan mesti menjalani latihan berkala mengenai amalan terbaik pengurusan kunci, tanggungjawab peranan dan prosedur pengendalian. Latihan ini juga perlu dimasukkan dalam proses pengambilan staf baru dalam bidang keselamatan IT, dan dikemaskini selaras dengan perubahan dasar atau peraturan.

7.0 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.

8.0 LAMPIRAN