# APA ITU POLISI KESELAMATAN SIBER ?


**POLISI**
**KESELAMATAN SIBER**
**KEMENTERIAN PENDIDIKAN MALAYSIA**
VERSI 1.0

1. Peraturan-peraturan yang mesti DIBACA, DIFAHAMI dan DIPATUHI oleh SEMUA WARGA KPM
2. Untuk menjamin KESINAMBUNGAN dan MEMINIMUMKAN kesan insiden keselamatan
3. ASET ICT KPM: perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia
4. Mengandungi 7 PRINSIP asas kepada Polisi Keselamatan ICT
5. Melaksanakan dan menguruskan RISIKO KESELAMATAN ICT ke atas aset ICT KPM
6. Mengandungi 14 BIDANG dan 104 KAWALAN

**Warga KPM hendaklah membaca, memahami dan akur akan peraturan-peraturan yang terkandung di dalam Polisi Keselamatan Siber KPM**

**Seksyen Risiko, Keselamatan dan Pematuhan ICT**
Bahagian Pengurusan Maklumat
Aras 3 & 4, Blok E11, Kompleks E,
Pusat Pentadbiran Kerajaan Persekutuan
62604 Putrajaya

KEMENTERIAN PENDIDIKAN MALAYSIA


# POLISI
## KESELAMATAN SIBER
### KEMENTERIAN PENDIDIKAN MALAYSIA
VERSI 1.0

# APA ITU POLISI KESELAMATAN SIBER

## PENGENALAN

Polisi Keselamatan Siber (PKS) KPM versi 1.0 telah diluluskan pada **Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KPM Bil2/2019 pada 16 April 2019** bagi menggantikan Dasar Keselamatan ICT (DKICT) KPM sedia ada.

Ianya mengandungi peraturan-peraturan yang mesti dibaca, difahami dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) KPM.

Polisi ini juga menerangkan kepada semua pengguna di KPM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KPM.

Pengemaskinian Dasar Keselamatan ICT (DKICT) KPM versi 2.0 kepada Polisi Keselamatan Siber KPM versi 1.0 adalah berdasarkan perkara-perkara berikut:

⇒Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) versi 1.0, April 2016;

⇒Pematuhan kepada *Information Security Management System (ISMS) ISO/IEC 27001:2013*; dan

⇒Selaras dengan perubahan teknologi dan perkhidmatan semasa di KPM.

## OBJEKTIF UTAMA

- Memastikan kelancaran operasi KPM dan meminimumkan kerosakan atau kemusnahan;
- Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;
- Mencegah salah guna atau kecurian aset ICT Kerajaan;
- Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan; dan
- Memperkemaskan pengurusan keselamatan ICT KPM.

## SKOP

Aset ICT KPM terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Polisi Keselamatan Siber KPM menetapkan keperluan-keperluan asas berikut:

- Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
- Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

## PRINSIP-PRINSIP

Aset ICT KPM terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Polisi Keselamatan Siber KPM menetapkan keperluan-keperluan asas seperti berikut:

1. Akses atas dasar perlu mengetahui;
2. Hak akses minimum;
3. Akauntabiliti;
4. Pengasingan;
5. Pematuhan;
6. Pemulihan; dan
7. Saling Bergantungan.

## 14 BIDANG POLISI KESELAMATAN SIBER