MALAYSIAN STANDARD

MS ISO/IEC 27002:2013 (BM)

Teknologi maklumat - Teknik keselamatan - Kod amalan untuk kawalan keselamatan maklumat
(Semakan pertama)
(ISO/IEC 27002:2013, IDT)
(Diterbitkan oleh Jabatan Standard Malaysia pada tahun 2017)

ICS: 35.040

Perihal: teknologi maklumat, teknik keselamatan, kod amalan, kawalan keselamatan maklumat

JABATAN STANDARD MALAYSIA

PEMBANGUNAN *MALAYSIAN STANDARD*

Jabatan Standard Malaysia (STANDARDS MALAYSIA) ialah badan standard dan akreditasi kebangsaan.

Fungsi utama Jabatan Standard Malaysia adalah untuk merangsang dan menggalakkan standard, penstandardan dan akreditasi sebagai cara bagi memajukan ekonomi negara, menggalakkan kecekapan dan pembangunan industri yang bermanfaat kepada kesihatan dan keselamatan awam, melindungi pengguna, memudahkan perdagangan dalam negeri dan antarabangsa serta melanjutkan kerjasama antarabangsa berhubung dengan standard dan penstandardan.

Malaysian Standard (MS) dibangunkan melalui sepersetujuan jawatankuasa-jawatankuasa yang dianggotai oleh perwakilan yang seimbang daripada pengeluar, pengguna dan pihak lain yang kepentingannya relevan, sebagaimana yang sesuai dengan perkara yang sedang diusahakan. *Malaysian Standard* adalah sejajar atau diterima guna daripada standard antarabangsa, seboleh mungkin. Kelulusan sesuatu standard sebagai *Malaysian Standard* ditentukan oleh Akta Standard Malaysia 1996 [Akta 549]. *Malaysian Standard* dikaji semula secara berkala. Penggunaan *Malaysian Standard* adalah secara sukarela, melainkan diwajibkan oleh pihak berkuasa yang mengawal selia melalui peraturan, undang-undang kecil tempatan atau apa-apa cara lain yang serupa.

Untuk tujuan *Malaysian Standard*, definisi-definisi berikut diguna pakai:

Semakan: Proses di mana *Malaysian Standard* yang sedia ada dikaji semula dan dikemaskini yang menjurus kepada penerbitan edisi baharu *Malaysian Standard*.

MS yang disahkan: *Malaysian Standard* yang telah dikaji semula oleh jawatankuasa yang bertanggungjawab dan mengesahkan bahawa kandungannya adalah terkini.

Pindaan: Proses di mana peruntukan-peruntukan dalam *Malaysian Standard* sedia ada diubah. Perubahan-perubahan dinyatakan dalam halaman pindaan yang dimasukkan ke dalam *Malaysian Standard* sedia ada. Pindaan-pindaan boleh dalam bentuk teknikal atau editorial.

***Corrigendum* teknikal:** Cetakan semula yang telah dibetulkan bagi edisi terkini yang dikeluarkan untuk membuat pembetulan kepada kesilapan teknikal atau kekeliruan dalam *Malaysian Standard* yang diwujudkan dengan tidak sengaja semasa mendraf atau percetakan yang menyebabkan penggunaan *Malaysian Standard* yang tidak betul atau tidak selamat.

NOTA: *Corrigendum* teknikal bukan untuk membetulkan kesilapan yang boleh dianggap mendatangkan akibat semasa penggunaan *Malaysian Standard*, sebagai contoh kesilapan kecil percetakan.

Jabatan Standard Malaysia melantik **SIRIM Berhad** sebagai ejen bagi membangunkan *Malaysian Standard*. Jabatan itu juga melantik SIRIM Berhad sebagai ejen pengedaran dan penjualan *Malaysian Standard*.

Untuk maklumat lanjut berkaitan dengan *Malaysian Standard*, sila hubungi:

Jabatan Standard Malaysia
Kementerian Sains, Teknologi dan Inovasi
Aras 1 & 2, Blok 2300, Century Square
Jalan Usahawan
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel.: 60 3 8318 0002
Faks: 60 3 8319 3131
http://www.jsm.gov.my
E-mel: central@jsm.gov.my

ATAU

SIRIM Berhad
(No. Syarikat 367474-V)
1, Persiaran Dato' Menteri
Seksyen 2, Peti Surat 7035,
40700 Shah Alam
Selangor Darul Ehsan
MALAYSIA

Tel.: 60 3 5544 6000
Faks: 60 3 5510 8095
http://www.sirim.my
E-mel: msonline@sirim.my

Kandungan

Muka surat

Perwakilan jawatankuasa

Jawatankuasa Standard Perindustrian mengenai Teknologi Maklumat, Komunikasi dan Multimedia (ISC G) yang di bawah kuasanya *Malaysian Standard* ini diterima pakai, dianggotai oleh wakil daripada organisasi yang berikut:

CyberSecurity Malaysia
Dewan Perdagangan dan Industri Antarabangsa Malaysia
Gabungan Komputer Nasional Malaysia
Institut Jurutera Malaysia
Institut Penyelidikan Sains dan Teknologi Pertahanan
Institut Tadbiran Awam Negara, Malaysia
Jabatan Standard Malaysia
Kementerian Komunikasi dan Multimedia
Kementerian Perdagangan Antarabangsa dan Industri
Kementerian Sains, Teknologi dan Inovasi
Kementerian Tenaga, Teknologi Hijau dan Air
Majlis Keselamatan Negara
Malaysia Digital Economy Corporation Sdn Bhd
Malaysian Technical Standards Forum Bhd
MIMOS Berhad
Multimedia University
Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
Persatuan Industri Komputer dan Multimedia Malaysia
Persatuan Jurutera Perunding Malaysia
Persekutuan Pekilang-Pekilang Malaysia
SIRIM Berhad (Sekretariat)
Suruhanjaya Komunikasi dan Multimedia Malaysia
Telekom Malaysia Berhad
Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
Universiti Teknologi Malaysia

Jawatankuasa Teknikal mengenai Keselamatan Maklumat yang mengawal selia penerimagunaan Standard ISO/IEC sebagai *Malaysian Standard* ini terdiri daripada perwakilan organisasi yang berikut:

CyberSecurity Malaysia
Kementerian Sains, Teknologi dan Inovasi
Malaysia Digital Economy Corporation Sdn Bhd
MIMOS Berhad
Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
Persatuan Industri Komputer dan Multimedia Malaysia
POS Malaysia Berhad
PricewaterhouseCoopers Risk Services Sdn Bhd
SIRIM Berhad (Sekretariat)
SIRIM QAS International Sdn Bhd
Suruhanjaya Komunikasi dan Multimedia Malaysia
TM Applied Business Sdn Bhd
Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia

Perwakilan jawatankuasa *(sambungan)*

Kumpulan Kerja mengenai Sistem Pengurusan Keselamatan Maklumat yang mengesyorkan penerimagunaan Standard ISO/IEC sebagai *Malaysian Standard* ini dianggotai oleh wakil daripada organisasi yang berikut:

CyberSecurity Malaysia
Malaysian Electronic Payment System Sdn Bhd
PricewaterhouseCoopers Risk Services Sdn Bhd
Scope International (M) Sdn Bhd
SIRIM Berhad (Sekretariat)
SIRIM QAS International Sdn Bhd
Suruhanjaya Komunikasi dan Multimedia Malaysia
TM Applied Business Sdn Bhd
Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
Universiti Islam Antarabangsa Malaysia
Universiti Malaya
Universiti Pertahanan Nasional Malaysia
VADS Berhad

Ahli ambilan:

RHB Bank Berhad

Prakata kebangsaan

Penerimagunaan Standard ISO/IEC sebagai *Malaysian Standard* telah disyorkan oleh Kumpulan Kerja mengenai Sistem Pengurusan Keselamatan Maklumat di bawah kuasa Jawatankuasa Standard Perindustrian mengenai Teknologi Maklumat, Komunikasi dan Multimedia.

Malaysian Standard ini serupa dengan ISO/IEC 27002:2013, *Information technology - Security techniques - Code of practice for information security controls*, yang diterbitkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC). Walau bagaimanapun, bagi maksud *Malaysian Standard* ini, perkara yang berikut terpakai:

a) dalam teks sumber, "Standard Antarabangsa ini" hendaklah dibaca sebagai "*Malaysian Standard* ini"; dan

b) tanda koma yang digunakan sebagai titik perpuluhan (jika ada), hendaklah dibaca sebagai noktah.

Malaysian Standard ini membatalkan dan menggantikan MS ISO/IEC 27002:2005, *Information technology - Security techniques - Code of practice for information security management*.

Versi bahasa Malaysia ini adalah terjemahan daripada versi asal dalam bahasa Inggeris, iaitu MS ISO/IEC 27002:2013, *Information technology - Security techniques - Code of practice for information security controls*. Jika terdapat sebarang pertikaian semasa penggunaan standard ini, versi bahasa Inggeris mengatasi versi ini.

Pematuhan kepada *Malaysian Standard* tidak dengan sendirinya memberikan kekebalan daripada obligasi undang-undang.

NOTA. IDT pada kulit depan menunjukkan standard yang serupa, iaitu standard dengan kandungan, struktur dan perkataan teknikal (atau terjemahan yang serupa) bagi *Malaysian Standard* adalah benar-benar sama dengan yang terdapat dalam Standard Antarabangsa atau serupa dari segi kandungan dan struktur teknikal, walaupun ia mungkin mengandungi perubahan editorial yang minimum seperti yang dinyatakan dalam klausa 4.2 ISO/IEC Guide 21-1.

Prakata

ISO (International Organization for Standardization) dan IEC (International Electrotechnical Commission) membentuk sistem khusus penstandardan bagi seluruh dunia. Badan kebangsaan yang menjadi ahli ISO atau IEC turut serta dalam pembangunan Standard Antarabangsa melalui jawatankuasa teknikal yang ditubuhkan oleh organisasi masing-masing untuk menangani aktiviti teknikal dalam bidang tertentu. Jawatankuasa teknikal ISO dan IEC bekerjasama dalam beberapa bidang yang melibatkan kepentingan bersama. Organisasi antarabangsa yang lain, kerajaan atau bukan kerajaan, dengan kerjasama ISO/IEC, juga turut serta dalam usaha tersebut. Dalam bidang teknologi maklumat, ISO dan IEC telah menubuhkan jawatankuasa teknikal bersama, iaitu ISO/IEC JTC 1.

Standard Antarabangsa telah digubal menurut peraturan yang ditetapkan dalam ISO/IEC Directives, Part 2.

ISO/IEC 27002 disediakan oleh Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC27, IT Security techniques.

Perlu ditegaskan bahawa terdapat kemungkinan sesetengah unsur dokumen ini tertakluk kepada hak paten. ISO dan IEC tidak boleh dipertanggungjawabkan untuk mengenal pasti mana-mana atau kesemua hak paten tersebut.

Edisi kedua ini membatalkan dan menggantikan edisi pertama (ISO/IEC 27002:2005), yang telah disemak semula dari segi teknikal dan struktur.

