



SCS: Digital First, Future Ready

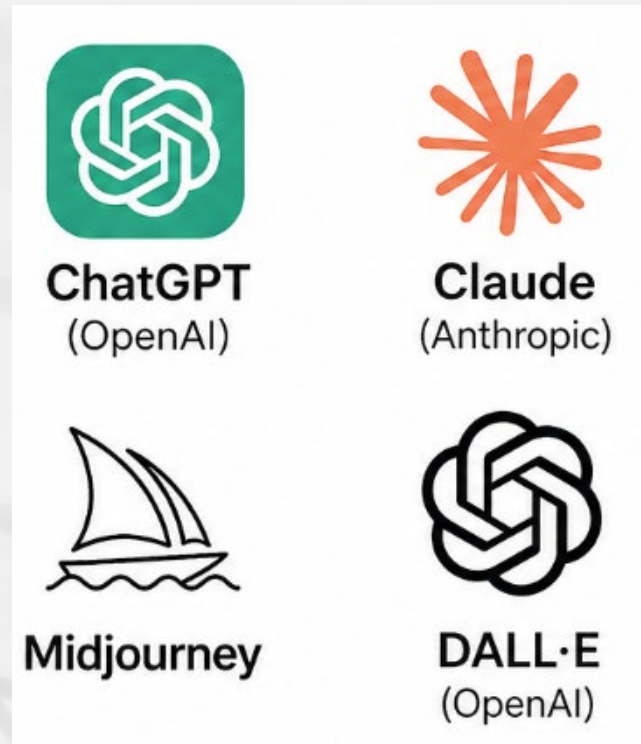
1

SCSDU Digital Awareness Talk No 1/2026

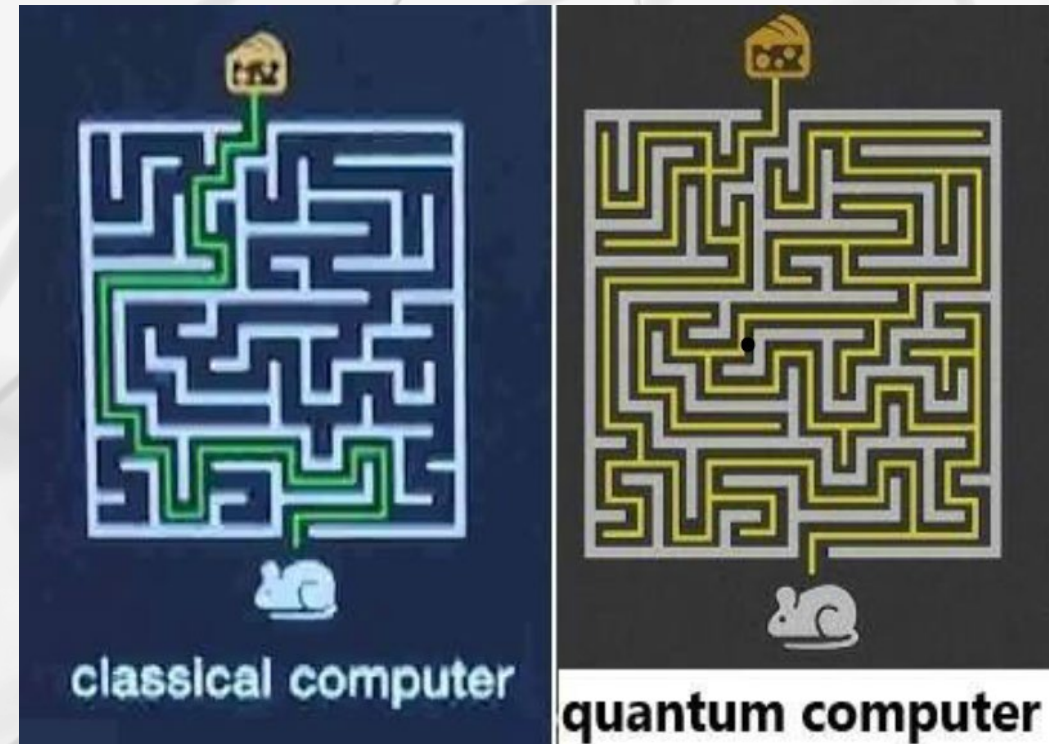
Topik : Dasar Keselamatan Siber Kerajaan Sarawak
Tarikh : 29 April 2026 (Rabu)
Masa : 10.00 pagi

Emerging Technologies

AI



Quantum Computing



Application Traffic

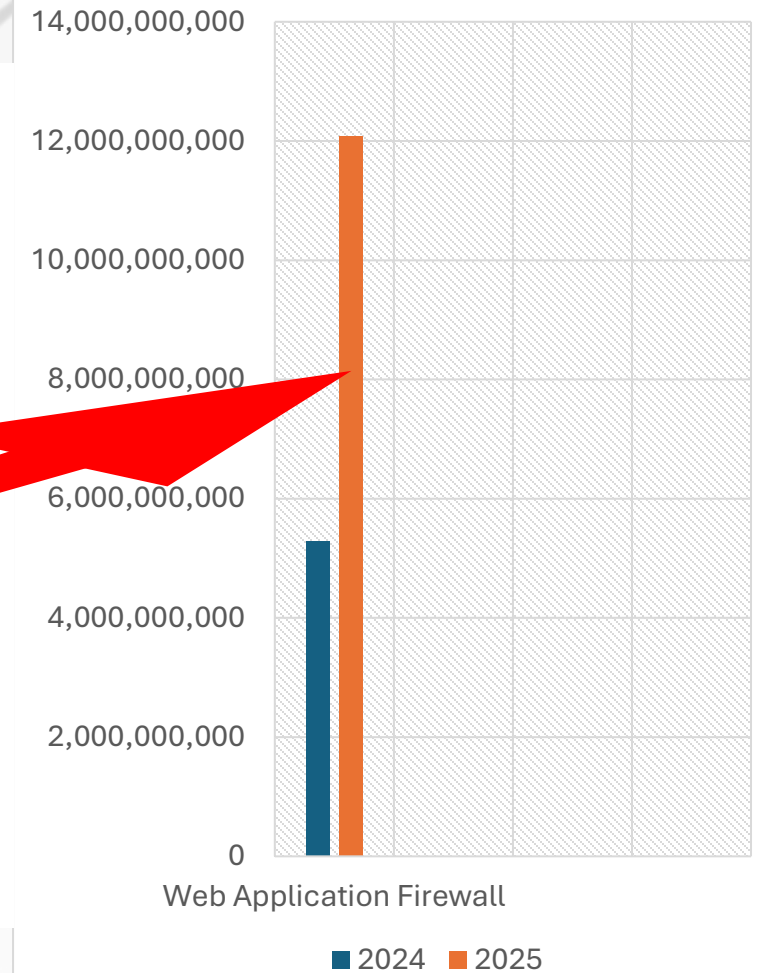


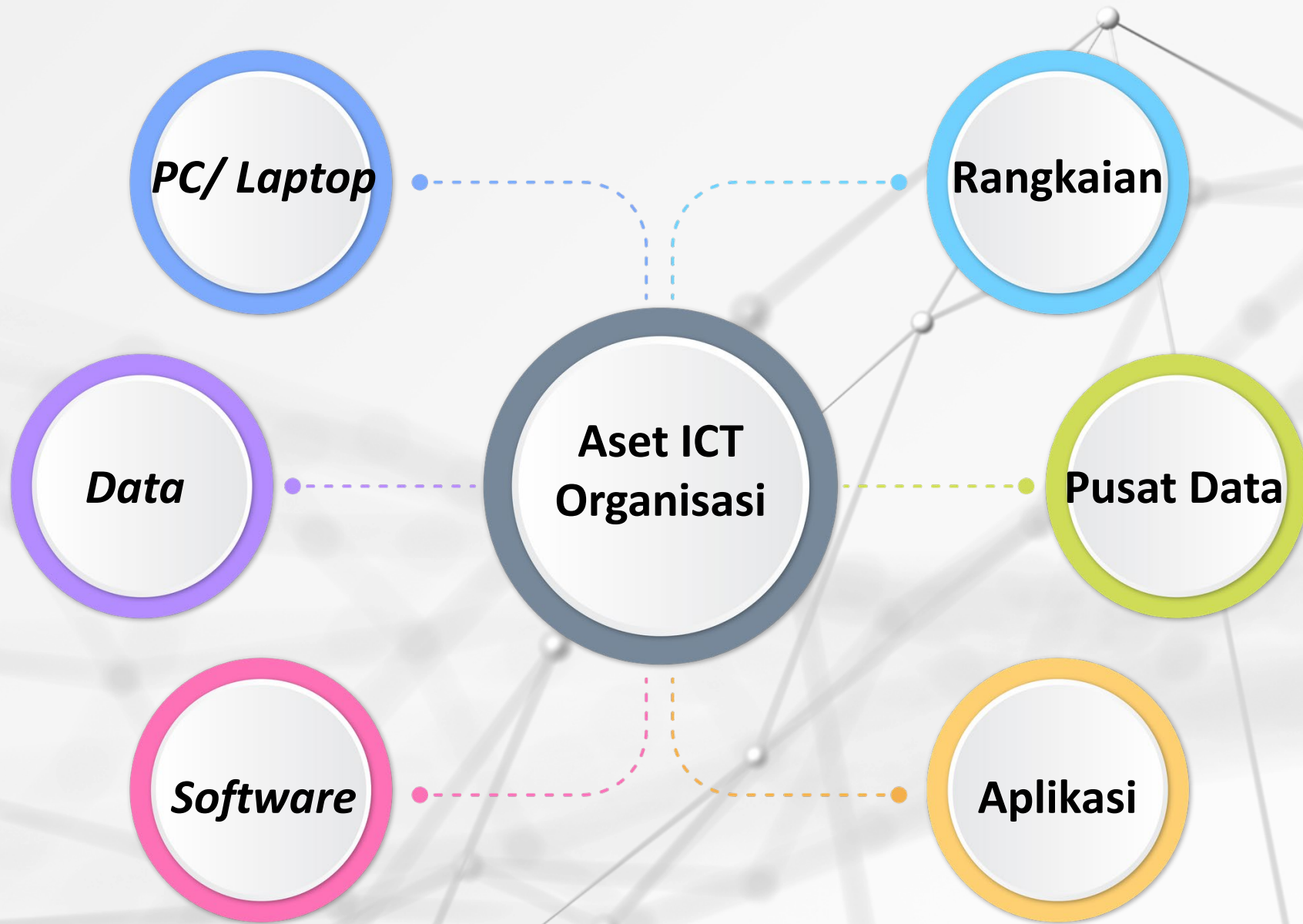
DIGITAL TRANSFORMATION

Digital transformation will empower Sarawak economic sectors to increase its efficiencies and productivity

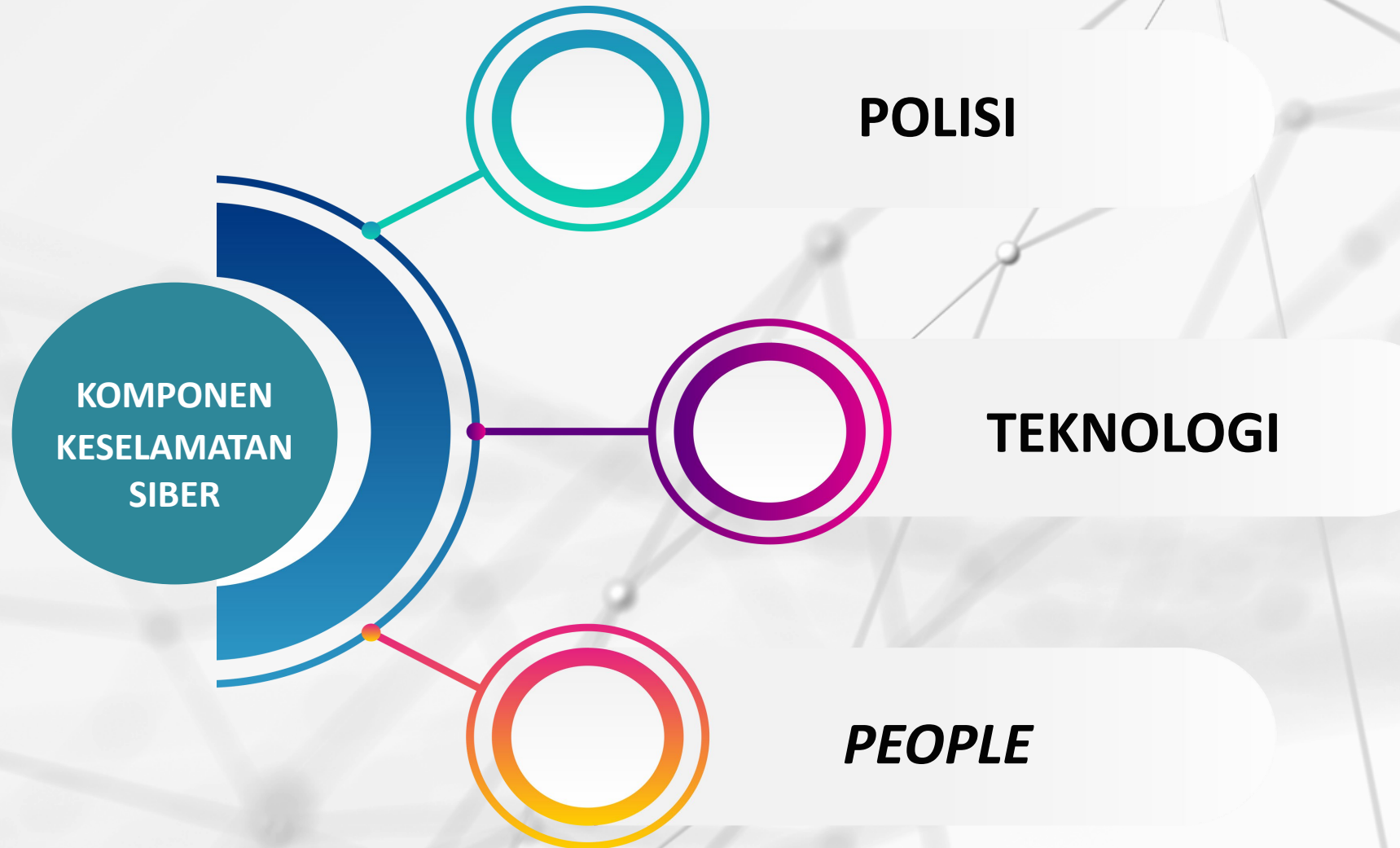
Key Outcomes

- 1 100% end-to-end digital government services
- 2 99.99% households with access to Internet connectivity
- 3 Increase Internet speed from 3 - 10 to 20 - 100 Mbps
- 4 100% of the population access to accredited STEM training and education online





Komponen Keselamatan Siber



SCS Phising Campaign

	2023 (users)	2024 (users)
<i>No. of SCS staff participate</i>	21,643	27,849
<i>No. of SCS staff click the link</i>	1,772	2,268
Kumpulan Sasaran	• Kementerian • Jabatan • R&DO	• Kementerian • Jabatan • R&DO • Badan Berkanun • PBT



DASAR KESELAMATAN SIBER

Dasar Keselamatan Siber

SURAT PEKELILING ICT NO. 1/2011

DARIPADA: Setiausaha Kerajaan Negeri

KEPADA: Semua Setiausaha Tetap Kementerian
Semua Ketua Jabatan Negeri
Semua Residen dan Pegawai Daerah
Semua Pihak Berkuasa Tempatan
Semua Ketua Badan Berkanun Negeri

PERKARA: DASAR KESELAMATAN ICT NEGERI SARAWAK

RUJ. KAMI: JKM/ICTU/100-15.02 KLT.1(2) **TARIKH:** 16 Mac 2011

1. TUJUAN

1.1 Dasar Keselamatan ICT Kerajaan Negeri diwujudkan untuk menjamin kesinambungan urusan dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi Kerajaan Negeri Sarawak. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

2. LATAR BELAKANG

2.1 Menyedari pentingnya usaha-usaha menjamin keselamatan ICT, Kerajaan Negeri Sarawak telah mengambil inisiatif untuk menghasilkan Dasar Keselamatan ICT yang menitikberatkan ciri-ciri keselamatan yang meliputi domain Keselamatan ICT yang berbeza secara menyeluruh. Polisi Keselamatan ICT telah digubal berpandukan kepada prinsip-prinsip keselamatan ICT yang kukuh, tanggungjawab terhadap keselamatan maklumat dan kesedaran terhadap ancaman serta langkah-langkah peningkatan tahap keselamatan ICT.

Surat Pekeliling ICT No. 1/2011

1



SURAT PEKELILING ICT BILANGAN 1 TAHUN 2025

DARIPADA : Setiausaha Kerajaan Sarawak
Semua Setiausaha Tetap Kementerian
Semua Ketua Jabatan Sarawak

KEPADA : Semua Residen Bahagian
Semua Ketua Badan Berkanun Sarawak
Semua Setiausaha Pihak Berkuasa Tempatan

SALINAN KEPADA : Semua Timbalan Setiausaha Kerajaan Sarawak

PERKARA : DASAR KESELAMATAN SIBER KERAJAAN SARAWAK

RUJUKAN : JPS/UDPA/100-1/2/3 JLD.1(3) **TARIKH :** 11 JULAI 2025

1.0 TUJUAN

Pekeliling ini bertujuan untuk memaklumkan dan menguatkuasakan pelaksanaan Dasar Keselamatan Siber Kerajaan Sarawak bagi menggantikan versi terdahulu yang telah dikemas kini selaras dengan keperluan semasa, teknologi terkini, serta garis panduan keselamatan digital Kerajaan Persekutuan.

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi Kerajaan Sarawak. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

2.0 LATAR BELAKANG

Seiring dengan peningkatan ancaman siber dan kebergantungan tinggi terhadap sistem teknologi maklumat dan komunikasi (ICT), keperluan untuk mewujudkan dasar keselamatan siber yang lebih komprehensif dan berdaya tahan adalah sangat penting. Justeru itu, Dasar Keselamatan ICT (DKICT) Kerajaan Sarawak telah dirangka semula untuk memastikan perlindungan menyeluruh terhadap aset digital organisasi.

Surat Pekeliling ICT Bilangan 1 Tahun 2025

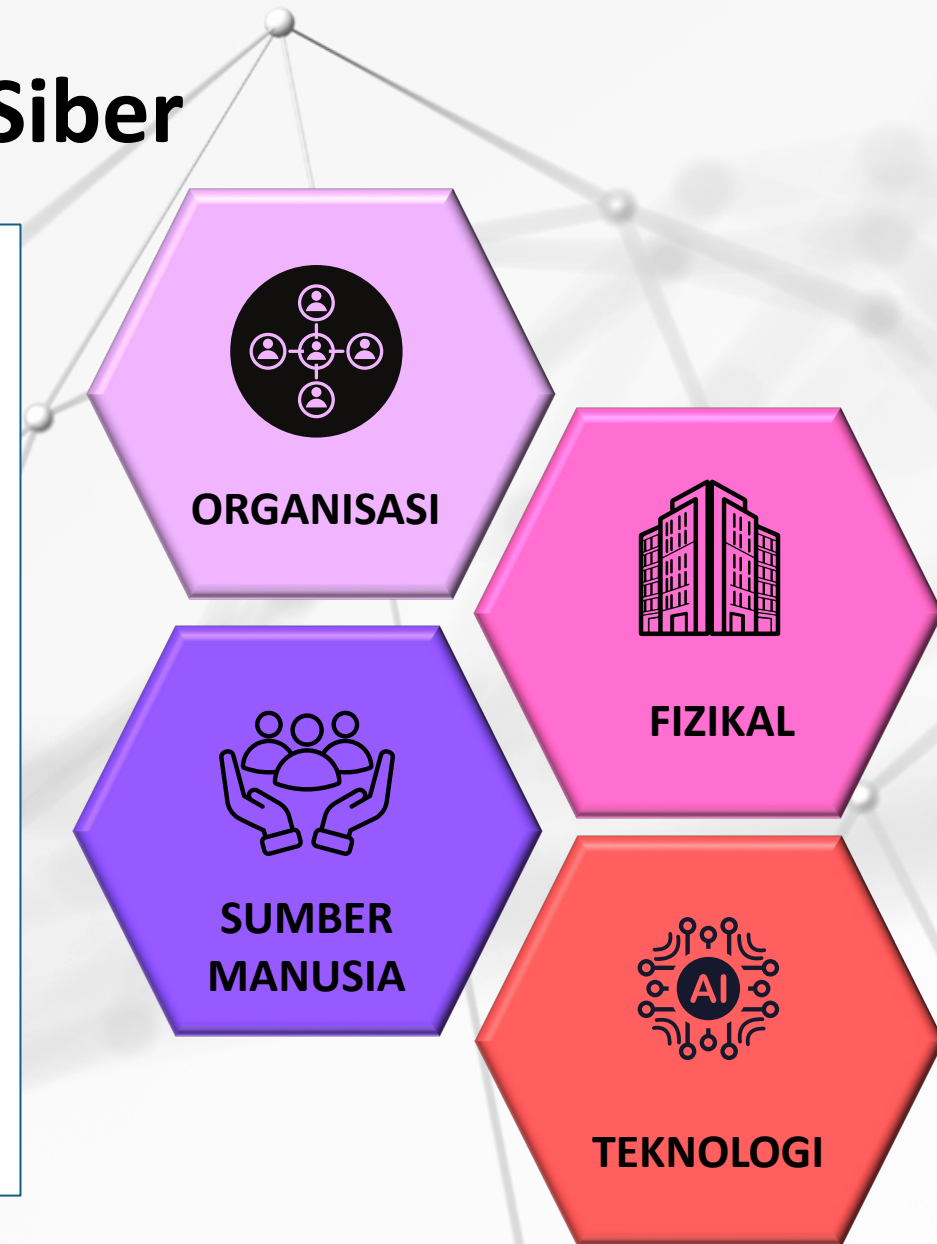
Muka surat | 1



DASAR KESELAMATAN SIBER KERAJAAN SARAWAK

VERSI 1.0 @ 2025

Dasar Keselamatan Siber



PEMAKAIAN DASAR KESELAMATAN SIBER (DKS)

3.1.4	Pemakaian dan Pengecualian Dasar Keselamatan Siber Kerajaan Sarawak Dasar Keselamatan Siber Kerajaan Sarawak adalah terpakai kepada semua penjawat awam serta mana-mana pihak berkepentingan yang berurusan dengan Kerajaan Sarawak. Tiada pengecualian bagi pematuhan dasar ini.	Agensi Pusat, Ketua Agensi, Penjawat Awam, Pihak Berkepentingan, Pembekal Perkhidmatan
--------------	---	---

PERANAN DAN TANGGUNGJAWAB

***STATE
CHIEF DIGITAL OFFICER
(CDO)***

***STATE
ICT SECURITY OFFICER
(ICTSO)***

***CHIEF DIGITAL OFFICER
(CDO)***

***ASSISTANT
CHIEF DIGITAL OFFICER
(ACDO)***



PERANAN DAN TANGGUNGJAWAB



CSIRT SARAWAK

SURAT PEKELILING ICT NO. 3/2009

DARIPADA: Setiausaha Kerajaan Negeri

KEPADA: Semua Setiausaha Tetap Kementerian Negeri
Semua Ketua Jabatan Negeri
Semua Residen dan Pegawai Daerah
Semua Ketua Badan Berkanun Negeri
Semua Pihak Berkuasa Tempatan

PERKARA: Penubuhan QCERT Dan Pengurusan Pengendalian Insiden ICT Sektor Awam di Peringkat Negeri

RUJ. KAMI: JKM/ICT/ADM04/004V.1 (41)

TARIKH: 5 November 2009

TUJUAN

Surat Pekeliling ini bertujuan memperkemas pengurusan pengendalian insiden keselamatan ICT bagi sektor awam di Peringkat Negeri supaya sebarang kejadian insiden keselamatan ICT dapat diuruskan dengan segera dan sistematik di mana kesannya dapat diminimumkan dan penyebarannya ke agensi lain dapat dibendung.

2. Kerajaan Negeri memandang berat tentang isu-isu keselamatan ICT dalam pelaksanaan Kerajaan Elektronik sebagai salah satu usaha dalam mempertingkatkan penyampaian perkhidmatan kepada rakyat. Peningkatan jenayah siber masa kini memberi kesan dan impak yang serius dalam keselamatan maklumat dan asset-asset ICT di agensi-agensi Kerajaan. Oleh yang demikian, Kerajaan memberi perhatian serius terhadap isu keselamatan ICT bagi memastikan agensi Kerajaan terus beroperasi dengan lancar.

3. Surat Pekeliling ini adalah selaras dengan suruhan Kerajaan Pusat melalui Pekeliling Am Bil. 4 Tahun 2006: "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat (ICT) Sektor Awam", di mana MAMPU menyeru Kerajaan Negeri untuk menubuhkan pasukan CERT di agensi Kerajaan untuk memperkukuh dan melancarkan lagi pengurusan insiden ICT di peringkat Negeri.

LATARBELAKANG

4. Sehubungan itu, Kerajaan Negeri telah menubuhkan pasukan CERT yang dikenali sebagai **Sarawak Computer Emergency Response Team (QCERT)**. QCERT bertindak memberi *first level support* dalam menangani insiden ICT yang berlaku di agensi-agensi Kerajaan Negeri, sebelum dilaporkan di Peringkat Kerajaan Pusat.

**SARAWAK COMPUTER EMERGENCY
RESPONSE TEAM (QCERT)**



KERAJAAN MALAYSIA

PEKELILING AM BILANGAN 4 TAHUN 2022

**PENGURUSAN DAN PENGENDALIAN INSIDEN KESELAMATAN
SIBER SEKTOR AWAM**

JABATAN PERDANA MENTERI
1 Ogos 2022

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

**CYBER SECURITY INCIDENT RESPONSE TEAM
SARAWAK (CSIRT SARAWAK)**

INSIDEN YANG DILAPORKAN KEPADA CSIRT

1

Ransomware:

Serangan yang menyebabkan sistem organisasi lumpuh sepenuhnya dan tidak boleh digunakan.

2

Kebocoran Maklumat Peribadi:

Apabila maklumat sensitif atau rahsia terlepas ke tangan pihak yang salah.

3

Penipuan E-mel (Phishing):

Percubaan menipu penjawat awam secara besar-besaran untuk mencuri maklumat log masuk.

4

Laman Web Rasmi Dirosakkan:

Penyerang mengubah rupa atau paparan laman web kerajaan secara haram.

5

Jangkitan Virus (Malware):

Penyebaran perisian berbahaya yang boleh merosakkan data dalam rangkaian organisasi.

6

E-mel Rasmi Dirampas:

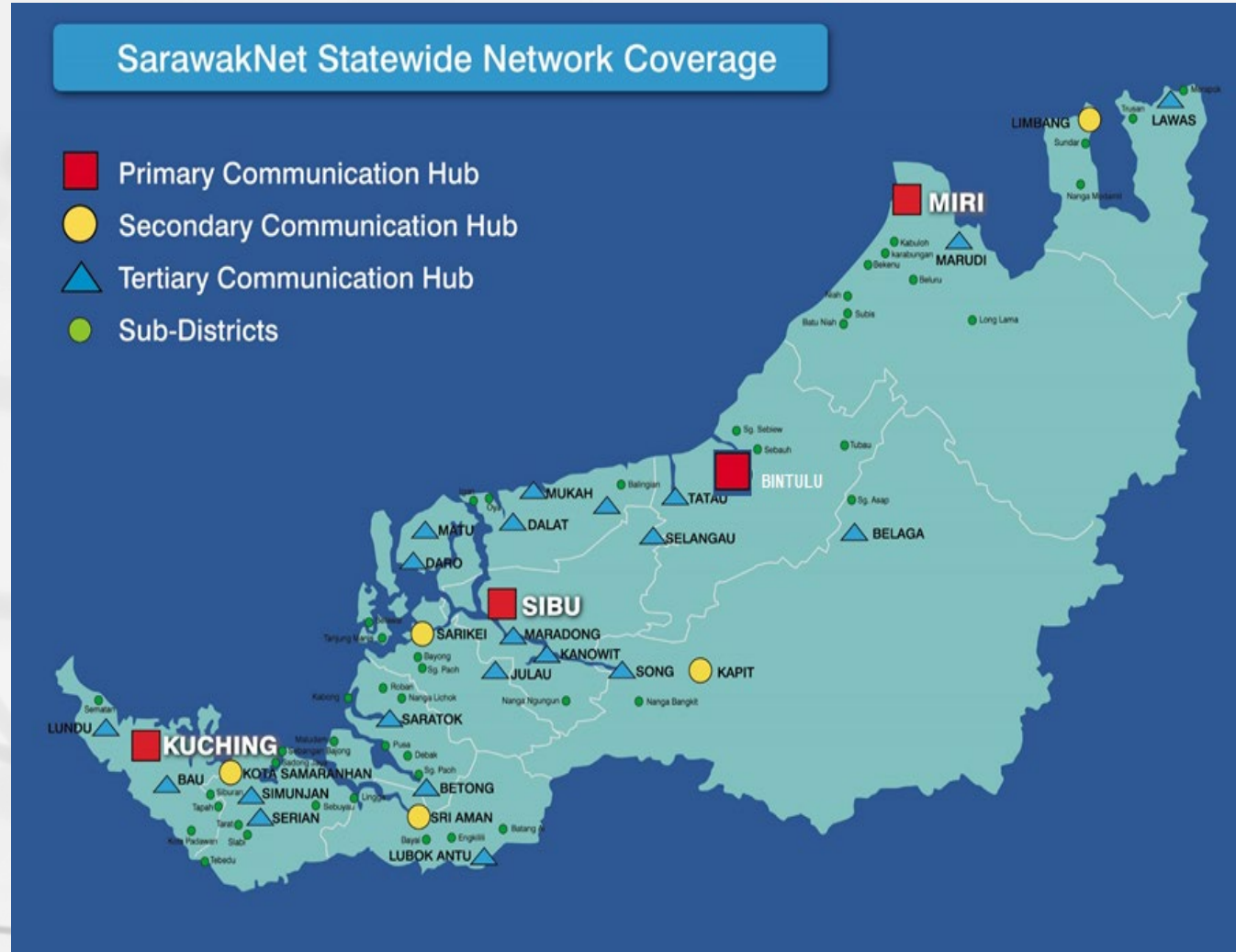
Akaun e-mel kerajaan disalahgunakan oleh penggodam untuk menghantar e-mel sampah (spam) atau penipuan.

RANGKAIAN

3.9.3 Capaian Rangkaian

Premis Kerajaan Sarawak hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian rasmi yang dibenarkan oleh Kerajaan Sarawak, iaitu Rangkaian **SarawakNet**

RANGKAIAN SARAWAKNET



WiFi Coverage

- SarawakNet WiFi
- SarawakNet Public WiFi
- SarawakNet IoT Wifi

SarawakNet Bandwidth

- Minimum of 100Mbps per site across all technology

Virtual Private Network (VPN)

- Provide OpenVPN to access restricted application that is only available in SarawakNet environment

KAWALAN SUMBER MANUSIA

1

Surat Akuan Pematuhan Dasar Keselamatan Siber

2

Surat Perakuan Akta Rahsia Rasmi

3

Tapisan Keselamatan

SURAT AKUAN PEMATUHAN DKS



SURAT AKUAN PEMATUHAN DASAR KESELAMATAN SIBER KERAJAAN SARAWAK

Nama Penuh Pegawai (Huruf Besar) :
No. Kad Pengenalan :
Jawatan / Gred :
Agensi :

Adalah dengan sesungguhnya saya memperakui bahawa: -

1. Sebagai penjawat awam Kerajaan Sarawak, saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan Siber Kerajaan Sarawak; dan
2. Sekiranya saya tidak mematuhi mana-mana perkara di dalam dasar ini, yang mana telah menyebabkan wujudnya sebarang risiko dan mendatangkan ancaman keselamatan siber kepada agensi serta Kerajaan, saya boleh dianggap cuai dan maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan Pegawai :

Tarikh :

Pengesahan Ketua Agensi

.....
(Tandatangan Ketua Agensi)

Ketua Agensi:

Tarikh :



Semua penjawat awam **WAJIB** menandatangani Surat Akuan Pematuhan Dasar Keselamatan Siber.

Bila Perlu Menandatangani Semula Surat Akuan Pematuhan?



SENARIO MASA

Saya telah berkhidmat melebihi 5 tahun di agensi ini tanpa bertukar jabatan.



SENARIO MOBILITI

Saya baru melaporkan diri di kementerian atau agensi yang baharu pada minggu lepas.



SENARIO POLISI

Kerajaan telah mengeluarkan versi baharu untuk Dasar Keselamatan Siber.

Perakuan Akta Rahsia Rasmi

Penjawat Awam	Vendor
Semua Penjawat Awam Wajib Menandatangani Borang Setiap Tahun	Menandatangani Borang Setiap Tahun
	Satu borang adalah memadai sekiranya mempunyai lebih daripada satu (1) projek bersama satu agensi
	Setiap kakitangan vendor yang terlibat wajib menandatangani surat akuan.
	Staff baru yang terlibat dengan projek harus menandatangani surat akuan
	Borang Akuan tidak perlu ditandatangani bagi vendor yang hadir ke pejabat untuk urusan mesyuarat/ courtesy visit.

Perakuan Akta Rahsia Rasmi (Penjawat Awam)

PERAKUAN UNTUK DITANDATANGANI OLEH PEGAWAI AWAM BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan surat rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan surat rasmi yang saya peroleh dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila meninggalkan Perkhidmatan Kerajaan.

Tandatangan : _____
Nama (huruf besar) : _____
No. Kad Pengenalan : _____
Jawatan : _____
Jabatan : _____
Tarikh : _____
Disaksikan oleh _____

(Tandatangan)

Nama (huruf besar) : _____
No. Kad Pengenalan : _____
Jawatan : _____
Jabatan : _____
Tarikh : _____
Cap Jabatan _____

PERAKUAN UNTUK DITANDATANGANI OLEH PEGAWAI AWAM APABILA MENINGGALKAN PERKHIDMATAN KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan surat rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Dengan ini menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa rahsia rasmi atau surat rasmi kepada mana-mana orang lain, sama ada atau tidak orang itu memegang jawatan dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau mana-mana Kerajaan Malaysia, dan sama ada di Malaysia atau di negara luar, sebelum dan selepas saya berhenti memegang jawatan dalam perkhidmatan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia.

Saya mengaku bahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyarat timbal, atau kata laluan rasmi yang rahsia, atau apa-apa benda, surat atau maklumat, anak kunci, rencana, alat meteri, atau cap bagi atau yang dipunyai, atau diguna, dibuat atau diadakan oleh mana-mana jabatan Kerajaan atau oleh mana-mana pihak berkuasa diplomat yang dilantik oleh atau yang bertindak di bawah kuasa Kerajaan Malaysia atau Seri Paduka Baginda Yang di-Pertuan Agong yang tidak dibenarkan berada dalam milik atau kawalan saya.

Tandatangan : _____
Nama (huruf besar) : _____
No. Kad Pengenalan : _____
Jawatan : _____
Jabatan : _____
Tarikh : _____

Disaksikan oleh _____

(Tandatangan)

Nama (huruf besar) : _____
No. Kad Pengenalan : _____
Jawatan : _____
Jabatan : _____
Tarikh : _____
Cap Jabatan _____

Perakuan Akta Rahsia Rasmi (Vendor/ Pembekal Perkhidmatan)

**PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN
ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN
PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN
RASMI KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972
[AKTA 88]**

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan surat rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan surat rasmi yang saya peroleh semasa berurusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, sama ada dalam masa atau selepas berurusan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis daripada pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu auan selanjutnya bagi maksud ini apabila urusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia telah selesai.

Tandatangan	:	
Nama (huruf besar)	:	
No. Kad Pengenalan	:	
Jawatan	:	
Jabatan / Organisasi	:	
Tarikh	:	
Disaksikan oleh	:	
		(Tandatangan)
Nama (huruf besar)	:	
No. Kad Pengenalan	:	
Jawatan	:	
Jabatan / Organisasi	:	
Tarikh	:	
Cap Jabatan / Organisasi	:	

**PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN
ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN
PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN
RASMI KERAJAAN APABILA TAMAT KONTRAK PERKHIDMATAN
DENGAN KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972
[AKTA 88]**

Perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan surat rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Dengan ini menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa rahsia rasmi atau surat rasmi kepada mana-mana orang lain, sama ada atau tidak orang itu memegang jawatan dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau mana-mana Kerajaan Malaysia, dan sama ada di Malaysia atau di negara luar, sebelum dan selepas saya tamat kontrak perkhidmatan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia.

Saya mengaku bahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyarat timbal, atau kata laluan rasmi yang rahsia, atau apa-apa benda, surat atau maklumat, anak kunci, rencana, alat meteri, atau cap bagi atau yang dipunyai, atau diguna, dibuat atau diadakan oleh mana-mana jabatan Kerajaan atau oleh mana-mana pihak berkuasa diplomat yang dilantik oleh atau yang bertindak di bawah kuasa Kerajaan Malaysia atau Seri Paduka Baginda Yang di-Pertuan Agong yang tidak dibenarkan berada dalam milikan atau kawalan saya.

Tandatangan	:	
Nama (huruf besar)	:	
No. Kad Pengenalan/ Pasport	:	
Jawatan	:	
Jabatan/Organisasi	:	
Tarikh	:	
Disaksikan oleh	:	
		(Tandatangan)
Nama (huruf besar)	:	
No. Kad Pengenalan/ Pasport	:	
Jawatan	:	
Jabatan/Organisasi	:	
Tarikh	:	
Cap Jabatan / Organisasi	:	

Tapisan Keselamatan

Penjawat Awam	Vendor/ Pembekal Perkhidmatan
1. Tapisan Keselamatan di buat melalui sistem eVetting 3.0 oleh pegawai pengesah yang telah dilantik.	
2. Pegawai Pengesah Vendor & Penjawat awam hendaklah berbeza	
3. Tapisan keselamatan perlu dibuat setiap lima (5) tahun	

Tapisan Keselamatan

Log Masuk

ID Pengguna



→ Slaid ke kanan untuk mengisi

[Lupa ID Pengguna ?](#)

[Lupa Kata Laluan ?](#)

Log Masuk

Bukan Pengguna ? [Akaun Baharu](#)

[Log Masuk](#)

[Soalan Lazim](#)

[Aduan](#)

[Manual Pengguna](#)

[Hubungi Kami](#)



KAWALAN FIZIKAL



1. Memastikan premis dan aset kerajaan dilindungi



2. Memastikan penjawat awam dan pelawat menggunakan pas sepanjang berada di dalam premis



3. Menyediakan ruang tertutup untuk mesin penyalin



4. Penggunaan CCTV dan kad akses sebagai alat pemantauan



5. Tidak mendedahkan bahan-bahan sensitif di atas meja atau paparan skrin semasa ketiadaan pengguna



6. Memastikan perkakasan ICT hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja



7. Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan



KAWALAN TEKNOLOGI (INISIATIF KERAJAAN)

SCS Mobile +



SCS applications are being enhanced with Multi Factor Authentication (MFA) for secured login. All users are required to install [SCS Mobile+](#).

Login to applications is easy by using SCS Mobile+ scan to login. Or login with user name and password plus the OTP obtained in SCS Mobile+.

SCS Mobile+ is available on App Store, Google Play, or Huawei AppGallery.



Login



Time Left: 50 seconds

OR

Login with Password

If you have any queries, you can contact SAINS Call Centre (24 x 7).

Tel: 1-300-88-SAINS or 1-300-88-7246

DSign Platform



MENU

Dashboard

Documents

Activity History

Settings

Help

English Muhammad Zakaria Sahputra Bin Azlan

Dashboard

New Document

0 Pending My Signature

0 Waiting for others

0 Draft

Document(s) Pending Signature

Select All

* Documents containing comments, initials, stamps, checkboxes, or password protection are not allowed for batch signing.

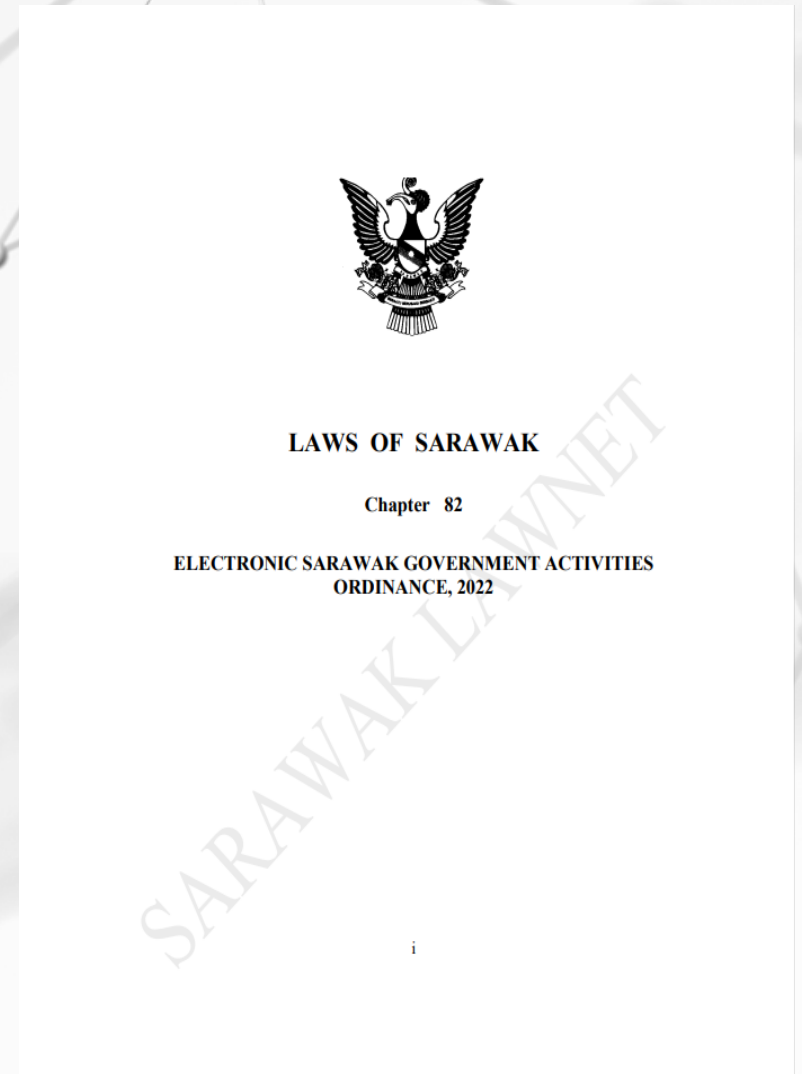
Document Download: For iOS users (Iphone, Ipad) Safari/Firefox: Share > Save to Files

Document	Progress	Release Date	Expiry Date	Action
No Data Available				

<

>

© Support



Official platform for electronic and digital signing

Anti Virus



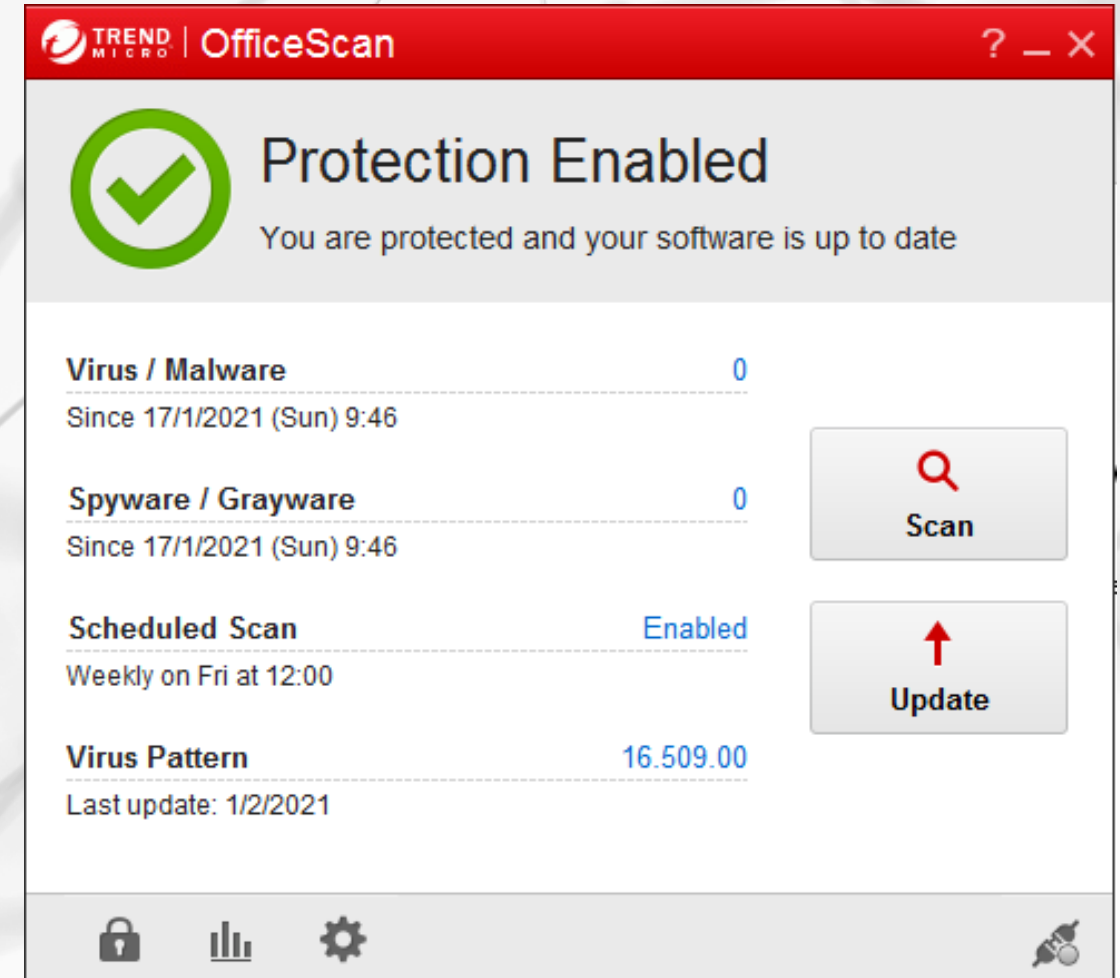
Trend Micro (Apex One) as a standard anti virus for all pc and laptop.



Update schedule is on every Friday afternoon from 12:00 pm – 2:00 pm



User are require to turn on the laptop/pc during that period.



Pusat Data Negeri



JABATAN PREMIER SARAWAK
(UNIT DIGITALISASI PERKHIDMATAN AWAM)
TINGKAT 4 (SAYAP KIRI), WISMA BAPA MALAYSIA, PETRA JAYA,
93502 KUCHING, SARAWAK.

Telefon Am : 082- 441957 | 082-319443 (Pengarah) Faks : 082-449002
Laman Web : <https://premierdept.sarawak.gov.my>



SURAT PEKELILING ICT BILANGAN 1 TAHUN 2023

DARIPADA : Setiausaha Kerajaan Sarawak

KEPADA : Semua Setiausaha Tetap Kementerian
Semua Ketua Jabatan Negeri
Semua Residen Bahagian
Semua Ketua Badan Berkanun Negeri
Semua Pihak Berkuasa Tempatan Negeri
Semua Ketua Syarikat Milik Kerajaan (*Government Linked Company*)

SALINAN : Semua Timbalan Setiausaha Kerajaan Sarawak
KEPADA : Pengarah Audit Dalam

PERKARA : KONSOLIDASI PERKHIDMATAN DI BAWAH PUSAT DATA NEGERI
(*STATE DATA CENTER*)

RUJUKAN : JPS/UDPA/100-1.01 JLD.7 (83) TARIKH : 02 MAY 2023

1.0 TUJUAN

Pekeliling ini bertujuan untuk memaklumkan kepada semua Kementerian, Jabatan dan agensi Kerajaan Sarawak termasuk agensi Badan Berkanun, Pihak Berkuasa Tempatan dan Syarikat Milik Kerajaan (agensi Kerajaan Sarawak) berkenaan pelaksanaan polisi pemusatan semua perkhidmatan di bawah Pusat Data Negeri (*State Data Center*).



2201

DIVISION V—CLOUD ACT

SEC. 101. SHORT TITLE.

This division may be cited as the “Clarifying Lawful Overseas Use of Data Act” or the “CLOUD Act”.

SEC. 102. CONGRESSIONAL FINDINGS.

Congress finds the following:

(1) Timely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime, including terrorism.

(2) Such efforts by the United States Government are being impeded by the inability to access data stored outside the United States that is in the custody, control, or possession of communications-service providers that are subject to jurisdiction of the United States.

(3) Foreign governments also increasingly seek access to electronic data held by communications-service providers in the United States for the pur-

SCS Cloud Storage







 All files

 Recent

 Favorites

 Shared with you

 Shared with others

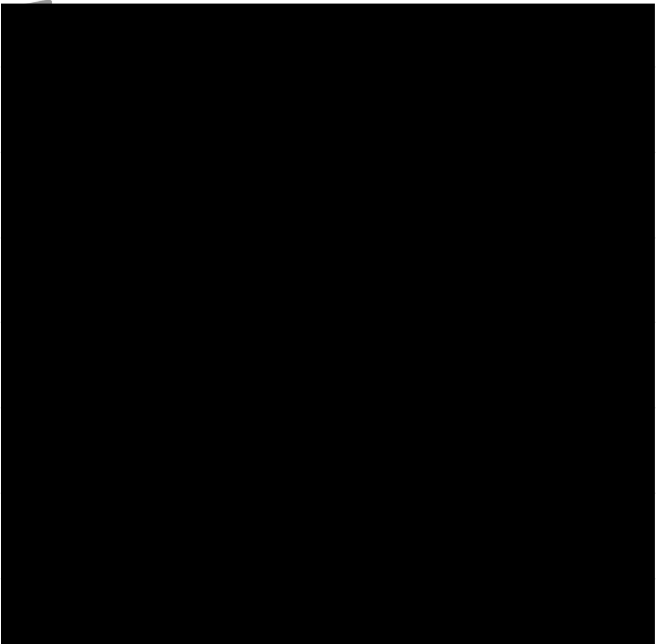
 Shared by link

 Tags

 Deleted files

 337.3 MB of 10 GB used

 Settings

☐	Name ▾		Size	Modified	
☐		 Shared	...	55 KB	2 years ago
☐		 Shared	...	336.4 MB	2 years ago
☐		 Shared	...	887 KB	2 years ago
☐		 Shared	...	4.8 MB	2 years ago
☐		 Shared	...	262 KB	2 years ago
☐		 Shared	...	928 KB	2 years ago
☐		 Shared	...	881.2 MB	2 years ago
☐		 Shared	...	1.2 GB	2 years ago

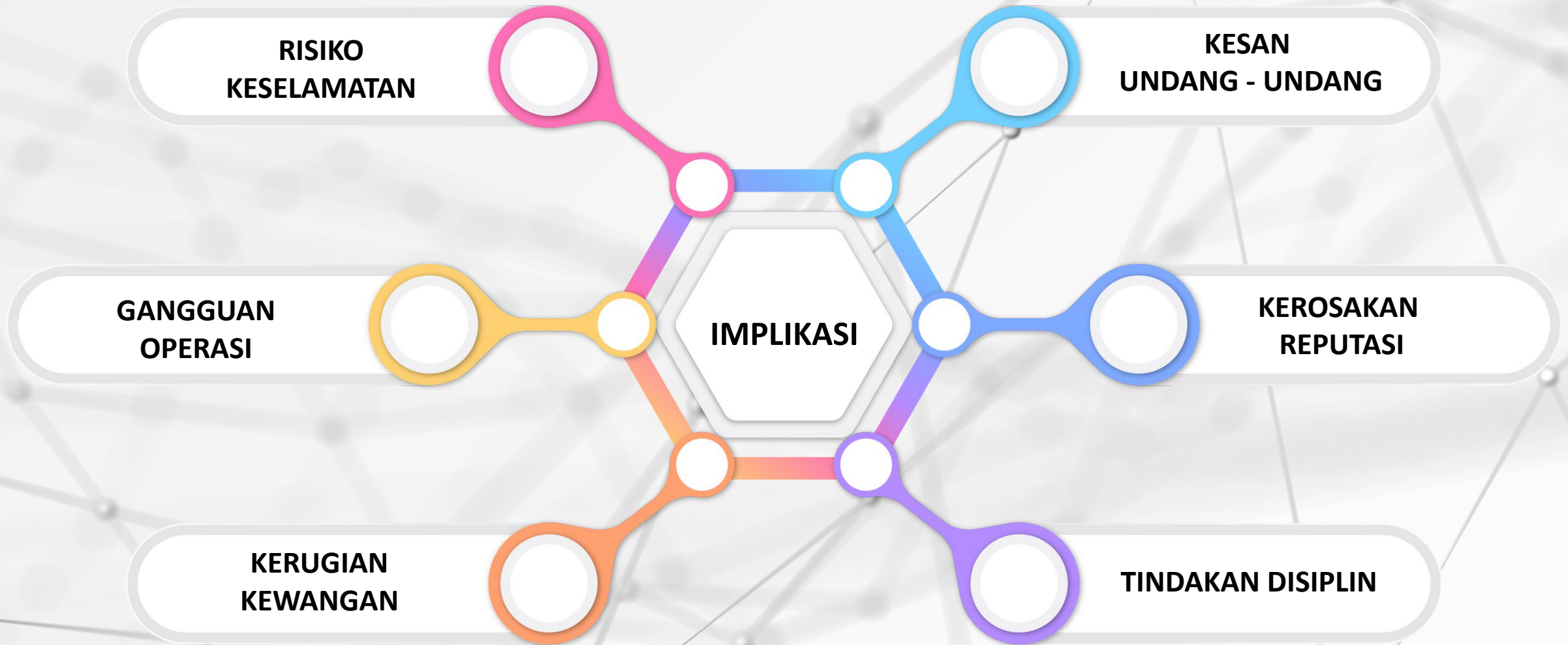
Security Operation Centre (SOC)



SCSdu



IMPLIKASI KETIDAKPATUHAN DKS





THANK YOU