KEMENTERIAN KEWANGAN
JABATAN AKAUNTAN NEGARA MALAYSIA

JABATAN AKAUNTAN NEGARA MALAYSIA

GARIS PANDUAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

GPTMK 2.0

GARIS PANDUAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

GPTMK 2.0

Diterbitkan oleh:
Bahagian Pengurusan Teknologi Maklumat (BPTM)
Jabatan Akauntan Negara Malaysia (JANM)
No 1, Persiaran Perdana, Presint 2, 62594 Putrajaya

E-mel: bptm@anm.gov.my
Telefon: 03-8882 1000
Laman web: www.anm.gov.my

SEJARAH DOKUMEN

GARIS PANDUAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

TAHUN	NAMA DOKUMEN	VERSI	KELULUSAN	TARIKH KUATKUASA
2022	Garis Panduan Teknologi Maklumat Dan Komunikasi	1.0	JPICT JANM	6 Julai 2022
2024	Garis Panduan Teknologi Maklumat Dan Komunikasi	1.1	JPICT JANM	4 Julai 2024
2026	Garis Panduan Teknologi Maklumat Dan Komunikasi	2.0	JPICT JANM	15 April 2026

JADUAL PINDAAN

GARIS PANDUAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

TARIKH	VERSI	JENIS PINDAAN
6 Julai 2022	1.0	Semakan mengikut dokumen Polisi Keselamatan Siber versi 1.0.
4 Julai 2024	1.1	Semakan mengikut dokumen Polisi Keselamatan Siber versi 1.1 dan tambahan melibatkan perkara baharu berdasarkan ISO/IEC27001:2022
15 April 2026	2.0	Semakan mengikut dokumen Polisi Keselamatan Siber versi 2.0 dan tambahan melibatkan perkara baharu berdasarkan Akta Keselamatan Siber 2024 dan Peraturan-peraturan (Akta 854).

ISI KANDUNGAN

PERKARA **MUKASURAT**

TUJUAN

Garis Panduan Teknologi Maklumat dan Komunikasi Jabatan Akauntan Negara Malaysia (JANM) merupakan dokumen sokongan yang perlu dibaca bersama dengan Polisi Keselamatan Siber JANM versi 2.0 Tahun 2026.

SKOP

Garis Panduan Teknologi Maklumat ini menerangkan tatacara penggunaan dan pengendalian kawalan Keselamatan yang meliputi perkara berikut:

a. Akaun dan Capaian;

b. E-mel Rasmi;

c. Rangkaian dan Keselamatan;

d. Perkakasan dan Perisian;

e. Pengurusan Keselamatan Sistem Aplikasi;

f. Perkhidmatan Prasarana Kunci Awam – *Government Public Key Infrastructure* (GPKI);

g. Pengurusan Migrasi Kriptografi Pasca Kuantum (Post-Quantum Cryptography, PQC); dan

h. Pihak Ketiga.

PENGGUNA

Pengguna meliputi:

Pengguna	Keterangan
Warga JANM	Personel kerajaan yang berkhidmat di JANM sama ada berjawatan tetap, sambilan dan kontrak yang menggunakan perkhidmatan ICT JANM.
Pihak Ketiga	Pembekal, perunding dan pihak yang berurusan dengan pihak JANM serta pengguna sistem JANM yang lain (bertujuan untuk akses data JANM).

RUJUKAN

a. Polisi Keselamatan Siber JANM versi terkini; dan

b. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) versi terkini.

AKAUN DAN CAPAIAN

AKAUN DAN CAPAIAN

Bil.	Perkara	Peranan
1	a. Penggunaan kata laluan pada setiap perkakasan ICT (*server* dan komputer) adalah diwajibkan. b. Penentuan kata laluan mesti mematuhi perkara berikut:- i. Tetapan kata laluan perlu memenuhi kerumitan (*complexity*); ii. Mempunyai huruf besar, huruf kecil, nombor dan simbol. Contohnya P@$$w0rd1234; iii. Panjang kata laluan mesti sekurang-kurangnya dua belas (12) aksara KECUALI bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; iv. Penguatkuasaan pertukaran kata laluan semasa atau selepas *login* kali pertama atau selepas reset kata laluan; v. Kata laluan yang sama boleh digunakan semula selepas tiga (3) kali pusingan; vi. Kata laluan menyerupai *username* tidak dibenarkan; vii. Kata laluan mesti ditukar dalam tempoh maksima enam (6) bulan atau 180 hari; viii. Pengguna mesti menukar kata laluan dalam kadar segera apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; dan ix. Menyimpan kata laluan menggunakan fungsi *autosave* di pelayar (*browser*) adalah tidak dibenarkan. c. Kata laluan tidak boleh ditulis, dipamer dan diletakkan pada komputer atau kawasan kerja.	– Warga JANM – Pihak ketiga

Bil.	Perkara	Peranan
2	Penamatan semua capaian bagi sistem, perkakasan dan perisian perlu dilaksanakan untuk warga JANM melibatkan kategori berikut: i. Tamat perkhidmatan, ii. Berpindah atau bertukar jabatan, iii. Berkursus bagi tempoh melebihi enam (6) bulan, dan; iv. Bercuti bagi tempoh tiga (3) bulan dan ke atas,	– Warga JANM
3	a. Memastikan kawalan terhadap perkakasan, perisian dan fasiliti pusat data daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan. b. Komputer mesti ditutup (*log off*) sepenuhnya pada akhir hari kerja. c. Memastikan semua maklumat sensitif atau sulit dalam bentuk salinan atau elektronik adalah selamat apabila hendak meninggalkan kawasan kerja. d. Dokumen Terhad atau Sulit yang tidak lagi diperlukan hendaklah dihapuskan secara dirincih; merujuk kepada Arkib Negara.	– Warga JANM – Pihak ketiga
4	*Content Filtering* Perisian *Content Filtering* mestilah digunakan bagi mengawal akses internet mengikut fungsi kerja dan pemantauan tahap pematuhan. Kawalan akses internet berdasarkan Garis Panduan Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan yang berkuatkuasa.	– Warga JANM – Pihak ketiga

E-MEL RASMI

E-MEL RASMI

<table>
<tr><th>Bil.</th><th>Perkara</th><th>Peranan</th></tr>
<tr><td>1</td><td>

<u>Permohonan E-mel Rasmi</u>

a. Permohonan perkhidmatan e-mel rasmi bagi pegawai baharu di JANM dilaksanakan melalui dua (2) kaedah mengikut kategori pengguna seperti berikut:

<table>
<tr><th>Bil</th><th>Kategori pengguna</th><th>Kaedah permohonan</th></tr>
<tr><td>1</td><td>Pengurusan Tertinggi
(Akauntan Negara Malaysia / Timbalan Akauntan Negara (Operasi) / Timbalan Akauntan Negara (Korporat) / Pengarah Bahagian / Pengarah JANM Negeri dan Cawangan / Timbalan Pengarah Bahagian / Pengarah JANM Negeri dan Cawangan)</td><td>Permohonan perkhidmatan e-mel rasmi bagi pegawai baharu di JANM memerlukan pengisian Borang Permohonan Perkhidmatan MyGovUC Dan Active Directory JANM bagi mewujudkan akaun pegawai baharu di JANM oleh Pentadbir UC.
Lampiran 3:
Borang Permohonan Perkhidmatan MyGovUC Dan Active Directory JANM</td></tr>
<tr><td>2</td><td>Warga JANM</td><td>Permohonan ini memerlukan pengisian Borang Permohonan Perkhidmatan MyGovUC Dan Active Directory JANM melalui Sistem iManage. (https://imanage.anm.gov.my) Pengesahan Ketua Unit/ Seksyen/ Bahagian masing-masing diperlukan bagi mewujudkan akaun pegawai baharu di JANM oleh Pentadbir UC.</td></tr>
</table>

b. Pengguna baharu perlu menukar kata laluan sementara, apabila diberikan pada login kali pertama.

c. Rahsiakan dan kukuhkan kata laluan e-mel. Penentuan kata laluan mestilah mematuhi kerumitan (*complexity*) yang telah ditetapkan.

</td><td>

– Warga JANM

– Pentadbir E-mel

</td></tr>
</table>

Bil.	Perkara	Peranan
	d. Saiz storan untuk semua pengguna adalah tertakluk kepada polisi dan ketetapan daripada pihak penyedia perkhidmatan MyGovUC iaitu Jabatan Digital Negara (JDN). e. Pengguna perlu menukar kata laluan apabila disyaki berlakunya kebocoran atau dikompromi. Kata laluan hendaklah diingat dan **TIDAK BOLEH** didedahkan dengan apa cara sekalipun. f. Pemohonan akaun e-mel akan diproses dalam tempoh **lima (5) hari bekerja**.	
2	**<u>Penggunaan E-mel</u>** a. Memastikan penghantaran e-mel rasmi menggunakan akaun e-mel rasmi JANM @anm.gov.my dan alamat penerima yang betul. b. Setiap pengguna bertanggungjawab untuk menguruskan e-mel masing-masing bagi memastikan e-mel yang disimpan tidak melebihi saiz *mailbox* yang telah diperuntukkan. Sekiranya kapasiti telah digunakan sepenuhnya, penghantaran dan penerimaan e-mel tidak boleh digunakan. Pengguna perlu melaksanakan housekeeping mengikut keperluan. c. Pengguna bertanggungjawab sepenuhnya terhadap semua kandungan e-mel dan lampiran fail. d. Akaun e-mel yang tidak aktif untuk tempoh **90 hari** akan ditamatkan kecuali perlanjutan tempoh telah dimaklumkan kepada Pentadbir e-mel.	– Warga JANM

Bil.	Perkara	Peranan
3	**<u>Keselamatan E-mel</u>** a. Pengguna tidak dibenarkan menghantar maklumat Rahsia Rasmi (Rahsia Besar dan Rahsia) melalui e-mel. b. Penghantaran maklumat Sulit dan Terhad hendaklah menggunakan Sistem Penghantaran Dokumen Sulit dan Terhad (SPDT) yang mempunyai fungsi enkripsi. Pengguna boleh merujuk kepada Garis Panduan Kawalan Dokumen E-mel dan Penghantaran Dokumen Terperingkat (Sulit dan Terhad). c. Kegiatan e-mel pengguna akan dipantau untuk tujuan penguatkuasaan dan dijadikan bahan bukti untuk kes rasmi di mahkamah. d. Memastikan setiap fail yang dimuat naik dan muat turun bebas daripada virus sebelum digunakan. e. Pengguna digalakkan membuat salinan/ arkib e-mel secara berasingan bagi tujuan *backup*. f. Membuat aduan atau laporan rasmi kepada Pentadbir e-mel jika menerima kandungan e-mel yang disertakan dengan bahan yang terlarang. g. Memaklumkan kepada pentadbir e-mel dengan segera sekiranya mengesyaki akaun telah disalahgunakan.	– Warga JANM

Bil.	Perkara	Peranan
4	**<u>Penamatan atau Nyahaktif E-mel</u>** a. Pegawai bertanggungjawab di setiap Bahagian dan JANM Negeri/ Cawangan perlu memaklumkan kepada Pentadbir e-mel **tiga (3) hari bekerja** selepas mana-mana warga JANM yang tamat perkhidmatan atau bertukar Jabatan atau cuti belajar atau kursus melebihi **enam (6)** bulan atau cuti melebihi **tiga (3)** bulan. b. Akaun e-mel bagi warga JANM yang cuti belajar atau cuti melebihi tiga (3) bulan perlu dinyahaktif (*disable*) dalam **tempoh tiga (3) hari bekerja.** c. Akaun e-mel perlu ditamatkan **30 hari dari tarikh pengguna tamat perkhidmatan di JANM.**	– Warga JANM
5	Perkara-perkara berikut adalah **<u>TIDAK DIBENARKAN:</u>** a. Penggunaan e-mel selain daripada e-mel rasmi Kerajaan bagi urusan rasmi. b. Kemudahan e-mel untuk menghantar bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian, jenayah, cetak rompak atau apa-apa maklumat yang menjejaskan reputasi JANM. c. Kemudahan e-mel rasmi untuk tujuan peribadi, komersial atau politik. d. Menyimpan, memuat turun dan memuat naik bahan yang mempunyai hakcipta, termasuk yang dimuat turun dari Internet atau menyebarkan kepada pihak lain tanpa mendapat kebenaran terlebih dahulu daripada pemilik hak cipta yang berkenaan. e. Menghantar e-mel sampah (*junk mail*) dan e-mel *spam* serta menyebarkan kod perosak seperti *virus*, *worm,* dan *trojan horse* yang boleh merosakkan sistem komputer dan maklumat pengguna lain. f. Menggunakan akaun milik orang lain, berkongsi akaun atau memberi akses akaun kepada orang lain untuk menjawab e-mel bagi pihaknya.	– Warga JANM

RANGKAIAN DAN KESELAMATAN

RANGKAIAN DAN KESELAMATAN

Bil.	Perkara	Peranan
1	**Rangkaian** Memastikan semua peranti infrastruktur Rangkaian yang disambungkan ke rangkaian JANM a. Mematuhi piawaian yang ditetapkan dalam Standard Komunikasi; b. Menggunakan protokol dan infrastruktur pengesahan yang diluluskan; c. Menggunakan protokol penyulitan JANM yang diluluskan; dan d. Peranti berupaya menyimpan alamat MAC perkakasan yang menggunakan rangkaian.	– Warga Warga JANM – Pihak ketiga
2	**Rangkaian Tanpa Wayar *(Wireless)*** Menggunakan *Service Set Identifier* (SSID) rangkaian tanpa wayar berdasarkan peranan pengguna seperti berikut: a. Pelawat JANM (JANM-GUEST-HQ); b. Pengguna dalaman (JANM-STAFF-HQ); c. Pengguna Teknikal (JANM-TECH-HQ); d. Pembekal (JANM-VENDOR-HQ); dan e. SSID Negeri dan cawangan.	– Warga JANM – Pihak ketiga
3	***Virtual Private Network* (VPN)** a. Semua capaian rasmi kepada sistem JANM secara jarak jauh hendaklah menggunakan perkhidmatan VPN yang disediakan oleh pihak BPTM. b. VPN adalah sambungan rangkaian yang dilindungi ketika menggunakan rangkaian awam. VPN menyulitkan (*encrypt*) lalu lintas internet anda dan menyamarkan identiti dalam talian anda. Ini menyukarkan pihak luar untuk mengesan aktiviti anda dalam talian dan mencuri data. Penyulitan berlaku dalam masa nyata.	– Warga JANM – Pihak ketiga

Bil.	Perkara	Peranan
	c. Warga JANM yang menggunakan VPN perlu mematuhi peraturan berikut: i. Menggunakan komputer hak milik kerajaan SAHAJA yang dilengkapi dengan kata laluan (*password*); ii. Memastikan perisian *antivirus* berlesen; atau perisian keselamatan enkripsi atau dekripsi; dan iii. Status Polisi Keselamatan Siber JANM telah disahkan. d. Borang Permohonan Pendaftaran VPN Jabatan Akauntan Negara Malaysia adalah diisi di dalam https://imanage.anm.gov.my; e. Permohonan VPN akan diproses dan diluluskan dalam tempoh tiga (3) hari berkerja. f. Perkongsian ID VPN untuk sebarang capaian adalah tidak dibenarkan sama sekali. g. Pengguna adalah dilarang untuk mengakses VPN bagi kaedah berikut: i. Menggunakan akses internet percuma atau kemudahan rangkaian awam; ii. Mengakses VPN dari luar negara sama ada semasa bercuti atau bertugas disana; dan iii. Menggunakan pelayan proxy yang terletak di luar negara. h. Akses VPN dari kemudahan internet awam dan dari luar negara adalah tidak dibenarkan sebagai mana yang dinyatakan di dalam Garis Panduan Akauntan Negara Malaysia Bil 1 2020 (GPANM Bil 1 Tahun 2020) - Pelaksanaan Tugasan Kewangan Dan Perakaunan Melalui Penggunaan Virtual Private Network (VPN) Oleh Pusat Tanggungjawab (PTJ). Penyalahgunaan dalam penggunaan kemudahan VPN ini boleh mengakibatkan kemudahan ini ditarik balik.	

Bil.	Perkara	Peranan
	VPN – Pihak Ketiga Pihak ketiga yang menggunakan VPN perlu mematuhi peraturan berikut: a. Status *Non-Disclosure Agreement* dan Polisi Keselamatan Siber JANM telah disahkan. b. Menggunakan VPN bagi pelaksanaan kerja di JANM; c. Memastikan perisian *antivirus* berlesen. **VPN - bertempoh** VPN (Bertempoh) Akses kepada rangkaian dalaman JANM diberikan kepada warga JANM dan pihak ketiga yang tidak berdaftar bagi keperluan situasi kritikal seperti bencana alam, pandemik dan sebagainya.	
4	a. Penamatan atau Nyahaktif VPN b. ID VPN bagi kakitangan akan dinyahaktifkan sekiranya tidak diakses selama enam (6) bulan berturut-turut dan ID akan dipadamkan pada bulan berikutnya. c. ID VPN bagi pihak ketiga akan dinyahaktifkan sekiranya tidak diakses selama tiga (3) bulan berturut-turut dan ID akan dipadamkan pada bulan berikutnya. d. Borang Permohonan Penamatan VPN JANM adalah menggunakan sistem iManage . e. Bagi ID VPN (bertempoh) akan ditamatkan serta merta selepas situasi kritikal telah tamat.	– Warga JANM – Pihak ketiga – Pentadbir Rangkaian dan Keselamatan

Bil.	Perkara	Peranan
5	**Perlindungan Rangkaian Daripada Perisian Berbahaya** a. Mengimbas semua kandungan storan luaran dengan perisian *antivirus*. b. Memastikan tiada sambungan perkakasan yang mencurigakan pada port *Universal Serial Bus* (USB) komputer yang digunakan.	– Warga JANM – Pihak ketiga
6	***Windows Encryption Technology*** a. Komputer riba yang dibekalkan perlu dipasang dengan *Windows Encryption* untuk menghalang dari akses yang tidak dibenarkan bagi melindungi data dan maklumat JANM. b. Memastikan *Windows Encryption* adalah terkini.	– Warga JANM
7	**Kawalan Akses** Penguatkuasaan kawalan akses berdasarkan prinsip pengesahan (*authentication*) dan *least privilege principle*, menggunakan model seperti: a. Role-based Access Control (RBAC); b. Attribute-based Access Control (ABAC); atau c. Pendekatan lain yang relevan dan sesuai dengan keperluan JANM.	– Warga JANM – Pihak ketiga – Pentadbir Rangkaian dan Keselamatan
8	**Pengemaskinian Gambar Rajah Rangkaian Fizikal dan Logikal** Menyediakan dan mengemaskini gambar rajah rangkaian fizikal dan logikal yang merangkumi: a. Gambar rajah fizikal: Perkakasan (*hardware*), perkabelan (*cabling*), dan lokasi peranti. b. Gambar rajah logikal: Segmentasi rangkaian, pengalamatan IP (*IP addressing*), dan aliran data (*data flows*).	– Pentadbir Rangkaian dan Keselamatan

Bil.	Perkara	Peranan
	Gambar rajah rangkaian hendaklah merangkumi kawalan keselamatan lanjutan yang berkaitan, seperti: a. *Next-generation firewalls* (NGFW): Untuk *application-aware traffic filtering*. b. *Intrusion Detection and Prevention Systems* (IDPS): Untuk mengesan dan mengurangkan ancaman. c. *Security Information and Event Monitoring* (SIEM): Untuk pemantauan secara *real-time* dan analisis.	
9	**Pengurusan *Firewall*** Melaksanakan peraturan *firewall* untuk mengawal trafik antara segmen rangkaian dengan: a. Menguatkuasakan segmentasi trafik antara zon rangkaian yang berbeza. b. Menyekat *ports* dan protokol yang tidak dibenarkan c. Mengemaskini peraturan *firewall* secara berkala untuk menangani ancaman. Melaksanakan keupayaan pengesanan ancaman rangkaian untuk memastikan pengesanan dan tindak balas yang tepat pada masanya terhadap aktiviti rangkaian yang mencurigakan bagi mencegah dan mengurangkan ancaman siber. Ini termasuk penggunaan *Web Application Firewall* (WAF) untuk semua aplikasi yang menghadap luaran (*external-facing*) bagi mengurangkan vektor serangan biasa. Melaksanakan penyelesaian *Network Access Control* (NAC) di seluruh organisasi untuk menguatkuasakan dasar akses, termasuk: a. Pengesahan dan kebenaran peranti sebelum memberikan akses rangkaian b. Pengkuarantinan peranti c. Segmentasi berdasarkan tahap risiko peranti	– Pentadbir Rangkaian dan Keselamatan – Pentadbir ICT – Pihak ketiga

Bil.	Perkara	Peranan
10	Perkara-perkara berikut adalah **TIDAK DIBENARKAN:** Penggunaan peralatan rangkaian persendirian yang dihubungkan dengan rangkaian JANM tanpa kebenaran.	– Warga JANM – Pihak ketiga
11	Keselamatan Rangkaian dan Sistem ICT mesti dilaksanakan mengikut Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang berkuatkuasa.	– Warga JANM – Pihak ketiga

PERKAKASAN DAN PERISIAN

PERKAKASAN DAN PERISIAN

Bil.	Perkara	Peranan
1	a. Komputer riba mestilah dikunci dengan *cable lock* yang dibekalkan atau disimpan dalam kabinet berkunci. b. Pengguna digalakkan membuat salinan atau penduaan (*backup*) pada maklumat yang disimpan dalam perkakasan bagi tujuan keselamatan dan bagi mengelakkan kehilangan data. Maklumat yang disimpan adalah mengikut prosedur *backup* yang telah ditetapkan.	– Warga JANM
2	Perkara-perkara berikut adalah **TIDAK DIBENARKAN:** a. Meninggalkan cetakan yang mengandungi maklumat Terhad atau Sulit di mesin pencetak atau penyalin atau ditinggalkan di mana-mana lokasi yang terdedah dan tidak selamat; b. Meletakkan atau menyimpan sebarang maklumat rahsia rasmi di skrin *desktop* komputer atau komputer riba; c. Membuat penambahan, menanggal atau mengganti perkakasan ICT yang telah ditetapkan; d. Mengubah kedudukan perkakasan dari tempat asal kecuali telah mendapat kebenaran Pengurus ICT dan dimaklumkan kepada Pegawai Aset; e. Menampal sebarang pelekat atau melakukan sebarang instalasi dan modifikasi pada perkakasan dan perisian selain untuk tujuan rasmi kecuali mendapat kebenaran Pentadbir ICT dan dimaklumkan kepada Pegawai Aset; dan f. Sekiranya pegawai bertukar tempat bertugas ke pejabat atau lokasi yang baharu, pegawai tidak dibenarkan untuk membawa perkakasan ICT dan mesti dikembalikan mengikut tatacara atau prosedur yang ditetapkan.	– Warga JANM

PENGURUSAN KESELAMATAN SISTEM APLIKASI

PENGURUSAN KESELAMATAN SISTEM APLIKASI

Bil.	Perkara	Peranan
Pembangunan Sistem		
1	Menyediakan dokumen pembangunan sistem berdasarkan garis panduan Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA), Pengurusan Projek ICT Sektor Awam (PPrISA), Garis Panduan Pembangunan Sistem dan Keperluan Infrastruktur ICT JANM (GPPS) atau prosedur dalaman JANM.	– Pemilik Sistem – Pentadbir Sistem ICT
2	Menentukan dan mengesahkan peranan dan tahap capaian penggunaan sistem.	– Pemilik Sistem – Pentadbir Sistem ICT
3	Membuat dan mengemaskini konfigurasi peranan dan tahap capaian pengguna sistem.	– Pentadbir Sistem ICT
4	Maklumat kata laluan pengguna disimpan dalam bentuk *encrypted* di dalam pangkalan data.	– Pentadbir Sistem ICT
5.	Memastikan perlindungan ke atas data terperingkat menggunakan *Secure Sockets Layer* (SSL), *Secure Shell* (SSH), *Public Key Infrastructure* (PKI) atau Enkripsi.	– Pentadbir Sistem ICT
6	Memastikan sistem mempunyai *session termination* (*frontend/backend*).	– Pentadbir Sistem ICT
7	Menyekat paparan *Directory Listing*.	– Pentadbir Sistem ICT
8.	Mengkhususkan satu *drive/volume/directory* secara berasingan untuk Sistem Pengoperasian (OS), Pangkalan Data (DB) dan Aplikasi mengikut kesesuaian dan keperluan.	– Pentadbir Sistem ICT
9	Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang berkuatkuasa mesti dipatuhi untuk mengelak pencerobohan data dan sistem.	– Pemilik sistem – Pentadbir Sistem ICT

Bil.	Perkara	Peranan
10	Mesej ralat tidak boleh memaparkan mesej dalaman sistem seperti nama *table, prosedur, error code* dan sebagainya kepada pengguna bagi mengelakkan risiko digodam.	– Pentadbir Sistem ICT
11	URL *query string* tidak boleh memaparkan sebarang maklumat session pengguna. Contoh: https://www.example.net/sAervlet/login?userid=abu&password=abu	– Pentadbir Sistem ICT
12	Sistem aplikasi mestilah berupaya menyemak dan memastikan *data input* yang dimasukkan betul bagi menjamin ketepatan dan integriti maklumat.	– Pentadbir Sistem ICT
13	Memastikan ketersediaan sistem dengan menyediakan persekitaran *High Availability* (jika berkaitan).	– Pentadbir Sistem ICT
14	Memastikan dokumentasi sistem, *Standard Operating Procedure* (SOP), dan manual panduan pengguna yang lengkap serta terkini.	– Pemilik Sistem – Pentadbir Sistem ICT
15	Memastikan dengan jelas kriteria dan keperluan bagi penerimaan sistem, didokumenkan dan diuji sebelum sistem diterima.	– Pemilik Sistem – Pentadbir Sistem ICT
16	Membuat konfigurasi dan pelarasan terhadap OS, perisian pembangunan sistem dan DB untuk memberi perlindungan kepada sistem yang akan digunakan supaya keselamatan dan prestasi sistem di tahap yang optimum.	– Pentadbir Sistem ICT
17	Memastikan sistem mempunyai jejak audit (*audit trail*) dan mengaktifkan fail log.	– Pentadbir Sistem ICT
18	Melaksanakan aktiviti *Security Posture Assessment* (SPA) dan pengukuhan sebelum sistem *Go Live* mengikut Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam.	– Pentadbir Sistem ICT

Bil.	Perkara	Peranan
19	Melakukan pengujian iaitu *functional, non-functional* termasuk *stress test* dan *performance testing* untuk *validate and verify* sistem yang dibangunkan atau dinaiktaraf bagi memenuhi keperluan dan rekabentuk sistem.	– Pemilik Sistem – Pentadbir Sistem ICT
20	Pengujian sistem hendaklah dilaksanakan di persekitaran pengujian (*Development/Staging)* terlebih dahulu bagi meminimakan risiko dan gangguan kepada operasi sistem di *Production*.	– Pemilik Sistem – Pentadbir Sistem ICT
21	Melakukan pengujian sistem setiap kali selepas proses *restore* dijalankan.	– Pemilik Sistem – Pentadbir Sistem ICT
Pengoperasian, Penyenggaraan dan Pemantauan Sistem		
1	Memastikan sistem mempunyai khidmat sokongan dan penyenggaraan.	– Pemilik Sistem
2	Penyenggaraan sistem hanya boleh dilakukan oleh kakitangan atau pihak yang dibenarkan sahaja. Semua aktiviti penyenggaraan hendaklah disemak dan diuji sebelum dan selepas aktiviti tersebut dilaksanakan.	– Pentadbir Sistem ICT – Pihak Ketiga
3	Sebarang penyenggaraan yang memerlukan sistem ditutup (*shutdown*) dan tidak boleh dicapai dalam tempoh tertentu perlu dirancang, dipersetujui dan dimaklumkan kepada pengguna.	– Pentadbir Sistem ICT – Pihak Ketiga – Pengguna
4	Mengurus dan memantau aktiviti penyenggaraan sistem mengikut jadual yang telah ditetapkan.	– Pemilik Sistem – Pentadbir Sistem ICT – Pihak Ketiga

Bil.	Perkara	Peranan
5	Melaporkan sebarang insiden keselamatan berkaitan sistem ke pihak yang bertanggungjawab.	– Pentadbir sistem ICT – Pemilik sistem
6	Memastikan dan memantau sistem boleh dicapai dan digunakan pada setiap masa.	– Pemilik sistem – Pentadbir sistem ICT
7	Melaksanakan aktiviti SPA dan pengukuhan mengikut Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam.	– Pentadbir sistem ICT – Pemilik sistem
8	Memastikan setiap masalah aplikasi diselesaikan di dalam tempoh *Service Level Agreement* (SLA) yang ditetapkan di dalam kontrak atau Surat Setuju Terima (SST).	– Pemilik Sistem – Pihak Ketiga
9	Perubahan sistem yang dibuat hendaklah mengikut tatacara proses yang dinyatakan di KRISA atau PPrISA atau Prosedur Kawalan Perubahan.	– Pemilik – Pentadbir sistem ICT
10.	Merekod dan menyimpan dokumentasi pembangunan sistem termasuk *source code* selepas *project hand-over* dilaksanakan.	– Pemilik sistem – Pentadbir sistem ICT
Source Code		
1	*Source code* atau *Intellectual Property Right* (IPR) bagi pembangunan sistem aplikasi dan serahan-serahan lain menjadi hak milik JANM kecuali *source code* yang telah dipatenkan oleh pihak prinsipal (*commercial of the shelf*).	– Pemilik sistem
2	Sekiranya terdapat penambahbaikkan yang baharu (*change request*) pada sistem, *source code* perlu dikemaskini dan disimpan mengikut keperluan JANM.	– Pentadbir sistem ICT – Pihak Ketiga

Bil.	Perkara	Peranan
3	Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Log audit perlu dikekalkan kepada semua akses kepada kod sumber; dan b. Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan.	– Pentadbir sistem – Pemilik sistem – Pihak ketiga

PERKHIDMATAN PRASARANA KUNCI AWAM (PKI)

PERKHIDMATAN PRASARANA KUNCI AWAM – *GOVERNMENT PUBLIC KEY INFRASTRUCTURE* (GPKI)

Bil.	Perkara	Peranan
1	Pentadbir GPKI perlu dilantik bagi mengurus sijil digital pengguna.	– Pentadbir GPKI
2	Permohonan pembaharuan, pembatalan dan semakan status sijil digital pengguna hendaklah melalui portal atau *mobile* GPKI.	– Pentadbir dan Pengguna GPKI
3	Pemegang sijil digital perlu mematuhi Garis Panduan dan merujuk Portal MyGPKI JDN yang dikemaskini dari semasa ke semasa.	– Pentadbir dan Pengguna GPKI
4	Pemegang sijil digital perlu memaklumkan kepada pentadbir GPKI berkenaan penggantian dan pembatalan sijil digital pengguna mengikut keperluan berikut: a. Sijil digital yang tidak berfungsi; b. Sijil digital yang disalahguna oleh pihak ketiga; c. Penyalahgunaan oleh pemegang sijil digital pengguna; dan d. Pengguna yang tamat perkhidmatan atau bersara.	– Pentadbir dan Pengguna GPKI

PENGURUSAN MIGRASI KRIPTOGRAFI PASCA KUANTUM (PQC)

PENGURUSAN MIGRASI KRIPTOGRAFI PASCA KUANTUM

Kriptografi Pasca Kuantum atau *Post Quantum Cryptography* (PQC) adalah kaedah penyulitan dan tandatangan digital yang direka untuk melindungi data, komunikasi, dan sistem IT daripada ancaman komputer kuantum pada masa hadapan. PQC melindungi transaksi digital kritikal dan maklumat sensitif, serta memastikan keselamatan jangka panjang tanpa memerlukan perisian kuantum. Peranan dan tanggungjawab dalam pelaksanaan migrasi PQC adalah seperti berikut.

Bil.	Perkara	Peranan
1	**Fasa 1: Persediaan (Nilai)** Menilai landskap kriptografi semasa, mengenal pasti sistem kritikal, dan menjalankan penilaian risiko yang menyeluruh. Aktiviti – aktiviti yang perlu dilaksanakan adalah seperti berikut: a. Mengenal pasti sistem yang paling berisiko terhadap operasi dan keselamatan organisasi apabila wujudnya pengkomputeran kuantum. b. Membuat inventori semua aset kriptografi (protokol penyulitan, sistem pengurusan kunci dan maklumat sulit). c. Melakukan penilaian risiko secara menyeluruh bagi menentukan tahap kerentanan sistem terhadap serangan kuantum. d. Menilai tahap kebergantungan terhadap organisasi luar.	– Pengurus ICT – Pentadbir ICT
2	**Fasa 2: Pemilihan Dan Penyeragaman Algoritma (Pilih)** Memastikan pemilihan algoritma PQC yang selamat dan berkesan untuk menggantikan protokol kriptografi yang rentan terhadap ancaman kuantum. Aktiviti – aktiviti yang perlu dilaksanakan adalah seperti berikut: a. Menerima, mengikuti, dan menggunakan piawaian yang telah ditetapkan secara antarabangsa (NIST/ETSI/ISO). b. Memilih algoritma PQC yang sesuai untuk proses *enkripsi*, tandatangan digital dan pertukaran kunci rahsia. c. Menguji dan menilai kesesuaian algoritma dengan sistem dalam pelbagai konfigurasi.	– Pengurus ICT – Pentadbir ICT

Bil.	Perkara	Peranan
	d. Memperoleh pengiktirafan piawaian keselamatan di peringkat nasional dan antarabangsa.	
3	**<u>Fasa 3 : Pembuktian Dan Pengujian Kebolehlaksanaan Awal (Mengesahkan)</u>** Membuktikan keberkesanan algoritma dalam persekitaran sebenar dengan menguji kebolehlaksanaannya pada skala kecil sebelum migrasi secara menyeluruh dilaksanakan. Aktiviti – aktiviti yang perlu dilaksanakan adalah seperti berikut: a. Menguji kebolehlaksanaan awal algoritma PQC ke atas sistem yang kritikal dalam organisasi dan seterusnya mengenal pasti cabaran serta kesukaran yang timbul. b. Mengguna pakai algoritma PQC hibrid bagi menyokong peralihan sistem ke arah PQC secara berperingkat. c. Melakukan analisis secara menyeluruh terhadap sistem serta mengumpul maklum balas untuk tujuan penambahbaikan. d. Mengoptimumkan kecekapan algoritma PQC berdasarkan prestasi awal serta maklum balas yang diperoleh.	– Pengurus ICT – Pentadbir ICT
4	**<u>Fasa 4: Pelaksanaan (Melaksanakan)</u>** Memastikan penggunaan algoritma PQC secara menyeluruh pada sistem organisasi yang kritikal. Aktiviti – aktiviti yang perlu dilaksanakan adalah seperti berikut: a. Melaksanakan pelan migrasi PQC untuk sistem kritikal, termasuk naik taraf infrastruktur dan penggantian protokol kriptografi tradisional kepada algoritma PQC. b. Menguji keberkesanan algoritma PQC bagi memastikan fungsi dan prestasi memenuhi keperluan. c. Memastikan pematuhan algoritma PQC kepada piawaian nasional dan antarabangsa (NIST/ISO/ETSI/MySEAL).	– Pengurus ICT – Pentadbir ICT

Bil.	Perkara	Peranan
	<u>Fasa 5: Pemantauan Dan Memastikan Ketahanan (Pantau)</u> Mengekalkan kelangsungan, keselamatan dan fungsi jangka panjang sistem PQC selepas pelaksanaannya. Aktiviti – aktiviti yang perlu dilaksanakan adalah seperti berikut: a. Menjalankan audit secara berkala. b. Memantau prestasi dan keselamatan sistem secara berterusan. c. Memantau perkembangan semasa pengkomputeran kuantum atau penyelidikan kriptografi, dan mengambil tindakan apabila wujudnya ancaman baru. d. Sentiasa menambah baik dan mengemas kini sistem.	– Pengurus ICT – Pentadbir ICT


PIHAK KETIGA

PIHAK KETIGA

Bil.	Perkara	Peranan
1	Pihak ketiga yang dilantik yang memerlukan akaun bagi mendapat capaian ke sistem-sistem di JANM perlu melengkapkan dokumen seperti di bawah: a. Salinan borang permohonan ke sistem e-Vetting, Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) - https://evetting.cgso.gov.my; b. Akuan Pematuhan Polisi Keselamatan Siber JANM (rujuk PKS versi terkini) di isi di dalam https://imanage.anm.gov.my; c. Borang Permohonan Pendaftaran VPN JANM di isi di dalam https://imanage.anm.gov.my – jika perlu; d. Borang 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] seperti di **Lampiran 1;** dan e. Borang 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] seperti di **Lampiran 2** (untuk penamatan pembekal).	– Pihak ketiga – Pentadbir Sistem
2	Pentadbir sistem bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pihak ketiga.	– Pentadbir ICT
3	Pihak ketiga hendaklah menyerahkan kod sumber (*source code*) sistem enam (6) bulan sebelum kontrak tamat kepada pihak JANM.	– Pihak ketiga – Pemilik Sistem
4	Penilaian prestasi pihak ketiga perlu dilaksanakan secara berkala atau mengikut keperluan.	– Pihak ketiga – Pemilik Sistem

GLOSARI

TERMA	PENERANGAN
ABAC	*Attribute-based Access Control*
BPTM	Bahagian Pengurusan Teknologi Maklumat
CGSO (Chief Government Security Office)	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia, iaitu sebuah unit di bawah Jabatan Perdana Menteri, Malaysia.
DB	*Database* (Pangkalan Data)
GPKI	*Government Public Key Infrastructure*
ICT	*Information and Communication Technology*
IDPS	*Intrusion Detection and Prevention Systems*
iGFMAS	*integrated Government Financial and Management Accounting System*
IPR	*Intellectual Property Right*
ISO/IEC27001:2022	*International Standard 27001:2022 – Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*
JANM	Jabatan Akauntan Negara Malaysia
JDN	Jabatan Digital Negara
KRISA	Kejuruteraan Sistem Aplikasi Sektor Awam (KRISA)
NAC	*Network Access Control*

TERMA	PENERANGAN
NGFW	*Next-generation Firewalls*
OS	*Operating System* (Sistem Pengoperasian)
PKI	*Public Key Infrastucture*
PKS	Polisi Keselamatan Siber
PPrISA	Pengurusan Projek ICT Sektor Awam
PQC	*Post Quantum Cryptography* (Kriptografi Pasca Kuantum)
RAKKSSA	Rangka Kerja Keselamatan Siber Sektor Awam
RBAC	*Role-based Access Control*
SIEM	*Security Information and Event Monitoring*
SLA	*Service Level Agreement*
SOP	*Standard Operating Procedure*
SPA	*Security Posture Assessment*
SPDT	Sistem Penghantaran Dokumen Sulit dan Terhad
SSH	*Secure Shell*
SSID	*Service Set Identifier*
SSL	*Secure Socket Layer*
SST	Surat Setuju Terima
USB	*Universal Serial Bus*

TERMA	PENERANGAN
VPN	*Virtual Private Network*
WAF	*Web Application Firewall*

LAMPIRAN 1

Borang 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]

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 suratan 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 suratan 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 akuan 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 .....

LAMPIRAN 2

Borang Perakuan Untuk Ditandatangani oleh Komuniti Keselamatan Atau Mana-Mana Pihak Lain yang Berurusan Dengan Perkhimatan Awam atau Yang Berkhidmat di Kediaman Rasmi Kerajaan Apabila Tamat Kontrak Perkhidmatan Dengan Kerajaan Berkaitan dengan Akta Rahsia Rasmi 1972 [Akta 88]

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 suratan 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 suratan 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, suratan atau maklumat, anak kunci, lencana, 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 .....