PIHAK BERKUASA PEMBANGUNAN TENAGA LESTARI MALAYSIA

PEKELILING SEDA MALAYSIA BIL. 4/2024 (Pin. 1/2025)

.....

DATO' HAMZAH BIN HUSSIN
Ketua Pegawai Eksekutif
Pihak Berkuasa Pembangunan Tenaga Lestari Malaysia
Tarikh: 22 Oktober 2025

POLISI KESELAMATAN SIBER SEDA MALAYSIA

BAHAGIAN PERKHIDMATAN DIGITAL

[Untuk kegunaan dalaman sahaja]

NO. PENDAFTARAN	TARIKH KUAT KUASA
FM-01-S01	22 Oktober 2025

KAWALAN DOKUMEN

BIL.	NOMBOR RUJUKAN	TATACARA BAHAGIAN PERKHIDMATAN DIGITAL
1.	SEDA/GPD/DS/BIL.4/2024	Polisi Keselamatan Maklumat dan Siber SEDA Malaysia
2.	FM-01-S01	Polisi Keselamatan Siber SEDA Malaysia

KAWALAN VERSI DOKUMEN

VERSI	TARIKH	BUTIRAN PERUBAHAN	DISEMAK OLEH	DILULUSKAN OLEH
1.0	17/12/2024	Versi pertama dokumen	Azarulnizam Mohd Zain Pengarah, Bahagian DS	Dato' Hamzah Bin Hussin Ketua Pegawai Eksekutif, SEDA Malaysia
2.0	21/10/2025	Versi kedua dokumen untuk diseragamkan dengan skop ISMS dan keperluan ISO 27001:2022	Azarulnizam Mohd Zain Pengarah, Bahagian DS	Dato' Hamzah Bin Hussin Ketua Pegawai Eksekutif, SEDA Malaysia

ISI KANDUNGAN

1. PENGENALAN

Polisi Keselamatan Siber Pihak Berkuasa Pembangunan Tenaga Lestari (SEDA) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) Pihak Berkuasa Pembangunan Tenaga Lestari (SEDA). Polisi ini juga menerangkan kepada semua pengguna di Pihak Berkuasa Pembangunan Tenaga Lestari mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT Pihak Berkuasa Pembangunan Tenaga Lestari.

2. PENYATAAN POLISI

2.1 Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan siber adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan siber kerana ancaman dan kelemahan sentiasa berubah.

2.2 Keselamatan siber adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan siber berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan siber iaitu:

i. Melindungi maklumat rahsia rasmi dan maklumat rasmi SEDA dari capaian tanpa kuasa yang sah,
ii. Menjamin setiap maklumat adalah tepat dan sempurna
iii. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna
iv. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

2.3 Polisi Keselamatan Siber SEDA merangkumi perlindungan ke atas semua bentuk maklumat elektronik dan bukan elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan.

2.4 Ciri-ciri utama keselamatan siber adalah seperti berikut:

i. **Kerahsiaan** — Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran
ii. **Integriti** — Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan
iii. **Tidak Boleh Disangkal** — Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal
iv. **Kesahihan** — Data dan maklumat hendaklah dijamin kesahihannya
v. **Ketersediaan** — Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

3. OBJEKTIF

3.1 Polisi Keselamatan Siber SEDA diwujudkan untuk menjamin kesinambungan urusan Pihak Berkuasa Pembangunan Tenaga Lestari dengan meminimumkan kesan ancaman atau insiden keselamatan siber. Ancaman atau insiden keselamatan siber boleh memberi kesan ke atas semua pihak termasuklah aset ICT yang dikendalikan. Terdapat sembilan (9) jenis insiden keselamatan siber iaitu:

i. Pelanggaran POLISI (*Violation of Policy*)
Penggunaan aset ICT bagi tujuan kebocoran maklumat dan/atau mencapai maklumat yang melanggar Polisi Keselamatan Siber.

ii. Penghalangan Penyampaian Perkhidmatan (Denial of Service)
Ancaman terhadap keselamatan sistem di mana perkhidmatan pemprosesan maklumat sengaja disekat daripada pengguna sistem. Ia melibatkan sebarang

ancaman yang mengganggu fungsi normal system termasuk serangan Denial of Service (DoS), Distributed Denial of Service (DDoS) dan tindakan sabotaj.

iii. Pencerobohan (*Intrusion*)

Mengguna dan mengubahsuai ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak. Ia termasuk capaian tanpa kebenaran, pencerobohan laman web, melakukan kerosakan kepada sistem (*system tampering*), pindaan data (*modification of data*) dan pindaan kepada konfigurasi sistem.

iv. Pemalsuan (*Forgery*)

Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*) dan penipuan (*hoaxes*).

***v.* Spam**

Spam adalah emel yang dihantar ke akaun emel orang lain yang tidak dikenali penghantar dalam satu masa dan secara berulang-kali (kandungan emel yang sama). Ini menyebabkan kesesakan rangkaian dan tindak balas menjadi perlahan.

vi. Malicious *Code*

Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan *virus*, *trojan horse*, *worm*, *spyware* dan sebagainya.

vii. *Harrassment/Threats*

Gangguan dan ancaman melalui pelbagai cara iaitu emel dan surat yang bermotif personal dan atas sebab tertentu.

viii. *Attempts/Hack Threats/Information Gathering*

Percubaaan (samada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran termasuk *spoofing*, *phishing*, *probing*, *war driving* dan *scanning*.

ix. *Kehilangan Fizikal* (*Physical Loss*)

Kehilangan capaian dan kegunaan disebabkan kerosakan, kecurian dan kebakaran ke atas aset ICT berpunca dari ancaman pencerobohan.

4. SKOP

4.1 Polisi ini adalah terpakai oleh semua pengguna di Pihak Berkuasa Pembangunan Tenaga Lestari termasuk warga kerja SEDA Malaysia SEDA Malaysia, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT Pihak Berkuasa Pembangunan Tenaga Lestari.

4.2 Ini akan dilakukan melalui pengwujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

i. Perkakasan

Semua aset yang digunakan untuk menyokong penyediaan, pemprosesan dan kemudahan storan maklumat SEDA.

Contoh komputer, pelayan, peralatan komunikasi dan sebagainya,

ii. Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT.

Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada SEDA,

iii. Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya.

Contoh Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain,

Sistem kawalan akses (proxy) seperti sistem kad akses, dan

Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegahan kebakaran dan lain-lain.

iv. Data atau Maklumat

Data atau maklumat dalam bentuk fizikal atau elektronik, yang digunakan bagi mencapai misi dan objektif SEDA.

Contoh sistem dokumentasi, prosedur operasi, rekod-rekod SEDA, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain.

v. Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian SEDA bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan

vi. Premis

Semua kemudahan komputer dan komunikasi di premis yang digunakan untuk menempatkan perkara **(i) - (v)** di atas. Setiap perkara di atas perlu diberi perlindungan yang rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

5. PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan Siber SEDA dan perlu dipatuhi adalah seperti berikut:

5.1 Akses atas Polisi perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas POLISI “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan.

5.2 Hak akses minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/ MyPortfolio.

5.3 Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT.

5.4 Pengasingan

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

5.5 Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, router, firewall dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail.

5.6 Pematuhan

Polisi Keselamatan Siber SEDA hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan siber.

5.7 Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan.

5.8 Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

6. KAWALAN ORGANISASI

KENYATAAN	TANGGUNGJAWAB
6.1 Polisi Keselamatan Maklumat (*Policies for information security*)	
Pembangunan Polisi	
Polisi Keselamatan Siber SEDA Malaysia telah dibangunkan oleh Ketua Pengarah Eksekutif (KPE) SEDA dengan penglibatan Ketua Pegawai Digital (CDO).	Ketua Pegawai Eksekutif (KPE) Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)
Penyebaran Polisi	
Polisi ini perlu disebarkan kepada semua pengguna maklumat SEDA Malaysia (termasuk warga kerja, pembekal, pakar runding dan lain-lain pihak berkepentingan).	Pegawai Keselamatan ICT (ICTSO)
Penyelenggaraan Polisi	
Polisi Keselamatan Siber SEDA adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Polisi Keselamatan Siber SEDA:	Pengarah Bahagian Perkhidmatan Digital (DS)

KENYATAAN	TANGGUNGJAWAB
• Kenal pasti dan tentukan perubahan yang diperlukan, • Kemuka cadangan pindaan secara bertulis untuk pembentangan dan persetujuan wakil – wakil jabatan. • Perubahan yang telah dipersetujui oleh dimaklumkan kepada semua warga kerja SEDA Malaysia, pembekal dan perunding, Polisi ini hendaklah dikaji semula sekurang-kurangnya **sekali setahun**.	
Pengecualian Polisi	
Polisi Keselamatan Siber SEDA adalah terpakai kepada warga kerja SEDA Malaysia, pembekal dan perunding dan tiada pengecualian diberikan kepada mana-mana pengguna yang menggunakan kemudahan ICT SEDA.	Warga kerja SEDA Malaysia, pembekal dan perunding
6.2 Peranan dan Tanggungjawab Keselamatan Siber (*Information security role and responsibilities)* **6.3 Pengasingan Tugas (*Segregation of duties*)** **6.4 Tanggungjawab Pihak Pengurusan (*Management responsibilities*)**	
Ketua Pengarah Eksekutif (KPE)	
Peranan dan tanggungjawab Ketua Pengarah Eksekutif adalah seperti berikut: • Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Polisi Keselamatan Siber SEDA. • Memastikan semua pengguna mematuhi Polisi Keselamatan Siber SEDA.	KPE

KENYATAAN	TANGGUNGJAWAB
• Memastikan semua keperluan organisasi (sumber kewangan, sumber staff dan perlindungan keselamatan) adalah mencukupi. • Memastikan penilaian risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Polisi Keselamatan Siber SEDA • Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Polisi Keselamatan Siber SEDA.	
Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)	
Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) berperanan dan bertanggungjawab seperti berikut: • Membaca, memahami dan mematuhi Polisi Keselamatan Siber Pihak Berkuasa Pembangunan Tenaga Lestari. • Mengkaji semula dan melaksanakan kawalan keselamatan siber selaras dengan keperluan Pihak Berkuasa Pembangunan Tenaga Lestari • Menentukan kawalan akses semua pengguna terhadap aset ICT Pihak Berkuasa Pembangunan Tenaga Lestari. • Melaporkan penemuan mengenai pelanggaran Polisi Keselamatan Siber.	Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)

KENYATAAN	TANGGUNGJAWAB
• Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan siber Pihak Berkuasa Pembangunan Tenaga Lestari • Menguatkuasakan Polisi Keselamatan Siber Pihak Berkuasa Pembangunan Tenaga Lestari.	
Pegawai Keselamatan Siber (ICTSO)	
Pegawai Keselamatan Siber (ICTSO) Pihak Berkuasa Pembangunan Tenaga Lestari adalah merupakan Penolong Pengarah / Penolong Pengarah Kanan (Keselamatan Siber). Peranan dan tanggungjawab beliau adalah seperti berikut: • Mengurus keseluruhan program-program keselamatan siber SEDA. • Memberi penerangan dan pendedahan berkenaan Polisi Keselamatan Siber SEDA kepada semua pengguna. • Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi Keselamatan Siber SEDA. • Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian. • Melaporkan insiden keselamatan siber kepada Pasukan Tindak balas Insiden Keselamatan Siber Kementerian dan memaklumkannya kepada Ketua	ICTSO

KENYATAAN	TANGGUNGJAWAB
Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS). • Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera. • Menyiasat dan mengenalpasti pengguna yang melanggar Polisi Keselamatan Siber SEDA. • Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan siber.	
Pentadbir Sistem ICT	
Penolong Pengarah / Penolong Pengarah Kanan (Infra). merupakan Pentadbir Sistem ICT Pihak Berkuasa Pembangunan Tenaga Lestari. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: • Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai staff yang berhenti, bertukar, bercuti atau berlaku perubahan. • Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi Keselamatan Siber SEDA • Memantau aktiviti capaian harian pengguna. • Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta	Penolong Pengarah / Penolong Pengarah Kanan (Infra)

KENYATAAN	TANGGUNGJAWAB
• Menyimpan dan menganalisis rekod jejak audit • Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	
Pengguna	
Pengguna adalah merupakan semua warga kerja SEDA Malaysia, pembekal dan perunding. Peranan dan tanggungjawab pengguna adalah seperti berikut: • Membaca, memahami dan mematuhi Polisi Keselamatan Siber SEDA. • Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya. • Lulus tapisan keselamatan. • Melaksanakan prinsip-prinsip Polisi Keselamatan Siber dan menjaga kerahsiaan maklumat SEDA Malaysia. • Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. • Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa. • Menentukan ketersediaan maklumat untuk digunakan. • Menjaga kerahsiaan kata laluan. • Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. • Memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.	Semua Warga Kerja SEDA Malaysia, pembekal dan perunding

KENYATAAN	TANGGUNGJAWAB
• Menjaga kerahsiaan langkah-langkah keselamatan siber dari diketahui umum. • Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) dengan segera. • Menghadiri program-program kesedaran mengenai keselamatan siber bagi semua warga kerja SEDA Malaysia. • Bertanggungjawab ke atas aset-aset ICT di bawah jagaannya • Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber Pihak Berkuasa Pembangunan Tenaga Lestari. Pembekal dan perunding, memadai dengan menandatangani *Non Disclosure Agreement (NDA)* sahaja.	
Cyber Security Incident Response Team SEDA (CSIRT SEDA)	
CSIRT SEDA adalah pasukan yang bertanggungjawab dalam keselamatan siber dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan siber SEDA. **Pengerusi:** Pengarah Bahagian Perkhidmatan Digital **Ahli:** Pegawai Keselamatan Maklumat (ICTSO) Timbalan Pengarah Bahagian Perkhidmatan Digital Pegawai Bahagian Perkhidmatan Digital	CSIRT SEDA

KENYATAAN	TANGGUNGJAWAB
Ketua Bahagian/ Pegawai Bahagian (skop ISMS) **Urus Setia:** Pegawai Bahagian Perkhidmatan Digital **Perkara kuasa:** i. Memantau tahap pematuhan keselamatan siber. ii. Memperakui garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam SEDA yang mematuhi keperluan Polisi Keselamatan Siber SEDA iii. Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan siber. iv. Memastikan Polisi Keselamatan Siber SEDA selaras dengan dasar-dasar ICT kerajaan semasa. v. Menerima laporan dan membincangkan hal-hal keselamatan siber semasa. vi. Membincang tindakan yang melibatkan pelanggaran Polisi Keselamatan Siber SEDA. vii. Menerima dan mengesan aduan keselamatan siber dan menilai tahap dan jenis insiden. viii. Merekod dan menjalankan siasatan awal insiden yang diterima. ix. Menangani tindak balas (respond) insiden keselamatan siber dan mengambil tindakan baik pulih minimum. x. Menghubungi dan melaporkan insiden yang berlaku kepada National Cyber Coordination & Command Centre (NC4) dan/atau CSIRT Kementerian sama ada sebagai input atau untuk tindakan seterusnya.	

KENYATAAN	TANGGUNGJAWAB
xi. Menasihati SEDA mengambil tindakan pemulihan dan pengukuhan dengan kerjasama bersama NC4 dan/atau CSIRT Kementerian. xii. Menyebarkan makluman berkaitan dengan SEDA dengan kerjasama bersama NC4 dan/atau CSIRT Kementerian. xiii. Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan atau pengukuhan dengan kerjasama bersama NC4 dan/atau CSIRT Kementerian bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
Pengasingan Tugas	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT. ii. Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan dan bagi melindungi aset ICT daripada berlakunya kesilapan, kebocoran maklumat terperingkat atau disalahgunakan. iii. Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai "*production*". Pengasingan juga merangkumi	Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)

KENYATAAN	TANGGUNGJAWAB
tindakan memisahkan antara kumpulan operasi dan rangkaian.	
6.5 Hubungan dengan Pihak Berkuasa *(Contact with authorities)*	
Hubungan yang berkaitan urusan rasmi dengan agensi-agensi yang berkaitan dan luar dikekalkan.	KPE, Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)
6.6 Hubungan dengan Pihak Tertentu Yang Mempunyai Kepentingan (*Contact with special interest groups*)	
Hubungan yang sesuai dengan pihak tertentu yang mempunyai kepentingan atau forum keselamatan khusus *("specialist" security forums)* yang lain dan pertubuhan-pertubuhan profesional perlu dikekalkan.	KPE, Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)
6.7 Ancaman Risikan *(Threat Intelligence)*	
Maklumat berkaitan ancaman keselamatan maklumat akan dikumpulkan dan dianalisa untuk digunapakai di SEDA.	Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS), ICTSO

KENYATAAN	TANGGUNGJAWAB
6.8 Keselamatan Maklumat Dalam Pengurusan Projek ***(Information security in project management)***	
Keselamatan Maklumat perlu ditekankan dalam pengurusan projek. Adalah menjadi tanggungjawab Pengarah Bahagian Perkhidmatan Digital untuk memastikan ciri-ciri keselamatan maklumat dimasukkan ke dalam proses pengurusan projek.	Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)
6.9 Maklumat Inventori dan Aset ***(Inventory of information and other associated assets)***	
Semua aset ICT Pihak Berkuasa Pembangunan Tenaga Lestari hendaklah direkodkan dan rekod tersebut hendaklah sentiasa dikemaskini. Ini termasuklah mengenal pasti, mengkategorikan aset dan merekodkan maklumat seperti pemilik, lokasi dan sebagainya. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya. Setiap pengguna tidak dibenarkan menggunakan aset SEDA untuk tujuan peribadi.	• Pegawai Aset Bahagian • Pengguna

KENYATAAN	TANGGUNGJAWAB
6.10 Penerimaan dan Penggunaan Maklumat dan Aset (*Acceptable use of information and other associated assets)*	
Pemilikan Aset	
Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja.	• Pengarah / Ketua Bahagian dan Unit • Pegawai Aset Bahagian • Pengguna
Kepenggunaan Aset yang Dibenarkan	
Peraturan untuk penggunaan aset mengikut kaedah atau polisi kepenggunaan yang dibenarkan dan aset yang berhubungkait dengan maklumat dan kemudahan memproses maklumat perlu dikenalpasti, direkodkan dan dilaksanakan. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua Warga Kerja SEDA Malaysia
6.11 Pemulangan Aset *(Return of assets)*	
Semua warga kerja SEDA Malaysia perlu memulangkan semua aset SEDA yang ada di dalam milik mereka semasa penamatan perkhidmatan, kontrak atau perjanjian.	• Pengarah, Bahagian Pentadbiran dan Sumber Manusia • Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)

KENYATAAN	TANGGUNGJAWAB
6.12 Pengkelasan Maklumat (*Classification of information)*	
Maklumat hendaklah dikelas dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan oleh pentadbiran SEDA. Aset perlu dikendalikan sewajarnya mengikut skim klasifikasi maklumat yang digunapakai oleh SEDA.	Pengarah / Ketua Bahagian dan Unit
6.13 Penglabelan Maklumat (*Labelling of information)*	
Pelabelan diperlukan untuk menunjukkan klasifikasi maklumat yang terhasil daripada sistem yang mengandungi maklumat yang dikategorikan sebagai sensitif atau kritikal supaya boleh dikendalikan mengikut kaedah yang sepatutnya. Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan. ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa. iii. Menentukan maklumat sedia untuk digunakan. iv. Menjaga kerahsiaan kata laluan. v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan. vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan,	Pengarah / Ketua Bahagian dan Unit

KENYATAAN	TANGGUNGJAWAB
penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan. vii. Menjaga kerahsiaan langkah-langkah keselamatan siber dari diketahui umum.	
6.14 Perpindahan Maklumat (*Information transfer)*	
Memastikan keselamatan pertukaran maklumat dan perisian dalam SEDA dan mana-mana entiti luar terjamin. Perkara-perkara yang mesti dipatuhi termasuk yang berikut:- i. Polisi, prosedur dan kawalan pertukaran maklumat dilaksanakan mengikut keperluan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi. ii. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari SEDA. iii. Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubungkait dengan sistem maklumat SEDA	• KPE • Pengarah/Ketua Bahagian dan Unit
Perjanjian Dalam Pemindahan Maklumat	
Perjanjian untuk pemindahan maklumat sama ada secara elektronik atau cetakan di antara SEDA dan pihak luar perlu dilaksanakan mengikut keperluan dan ianya perlu dilakukan bergantung kepada tahap sensitiviti sesuatu maklumat yang dikendalikan.	Pengarah / Ketua Bahagian dan Unit

KENYATAAN	TANGGUNGJAWAB
Mesej Elektronik	
Maklumat yang terkandung di dalam mesej elektronik perlu dilindungi. Penggunaan mesej elektronik hanya boleh digunakan untuk aktiviti kerja harian di mana penggunaan untuk kepentingan peribadi hendaklah dilarang bagi mengelakkan daripada sebarang bentuk gangguan dan ancaman kepada keselamatan maklumat.	Pengarah / Ketua Bahagian dan Unit
Perjanjian Kerahsiaan atau Ketidaktirisan Maklumat	
Keperluan bagi perjanjian kerahsiaan atau ketidaktirisan maklumat yang mencerminkan keperluan organisasi untuk melindungi maklumat perlu dikenalpasti, dikaji secara berkala jika perlu dan didokumenkan.	Pengarah / Ketua Bahagian dan Unit
6.15 Kawalan Capaian (*Access control)*	
Bertujuan untuk mengawal capaian ke atas maklumat, kemudahan pemprosesan maklumat serta proses perkhidmatan berdasarkan keperluan perkhidmatan dan keselamatan. Peraturan kawalan capaian hendaklah juga mengambilkira penyebaran dan pengesahan maklumat. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipastikan antara lain merangkumi perkara berikut:	Pegawai Bahagian Perkhidmatan Digital (Infra)

KENYATAAN	TANGGUNGJAWAB
i. Kawalan capaian ke atas maklumat dan proses perkhidmatan mengikut keperluan keselamatan dan peranan pengguna; ii. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; iii. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan iv. Kawalan ke atas kemudahan pemprosesan maklumat	
6.16 Pengurusan Identiti (*Identity management)*	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh SEDA seperti berikut: i. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; ii. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi; iii. Panjang kata laluan mestilah sekurang-kurangnya 12 aksara (gabungan nombor, huruf besar dan huruf kecil, tanda atau simbol). Contoh: P4s$w0rclSEDA; iv. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun;	• Pengarah/Ketua Bahagian dan Unit • Pegawai Bahagian Perkhidmatan Digital (Infra) • Pengguna

KENYATAAN	TANGGUNGJAWAB
v. Kata laluan windows dan screen saver hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; vi. Kata laluan tidak boleh dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; vii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; dan viii. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa bersesuaian.	
6.17 Pengesahan Maklumat *(Authentication information)*	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin agar ianya selamat berdasarkan garis panduan berikut: i. Mewujudkan dan menguatkuasakan mekanisma untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan ii. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pegawai Bahagian Perkhidmatan Digital (Infra)
6.18 Peruntukan Akses Pengguna (*Access rights)*	
Hak akses pengguna kepada maklumat dan aset berkaitan hendaklah diperuntukkan, disemak, diubahsuai dan dialih keluar mengikut dasar khusus topik organisasi dan peraturan untuk kawalan akses. Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi:	• Pegawai Bahagian Perkhidmatan Digital (Infra) • Pengguna

KENYATAAN	TANGGUNGJAWAB
i. Akaun yang diperuntukkan sahaja boleh digunakan; ii. Akaun pengguna mestilah unik; iii. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; iv. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; dan v. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang. Pentadbir Sistem ICT akan membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: • Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan. • Bertukar ke agensi lain. • Bersara atau ditamatkan perkhidmatan. Walaubagaimanapun, jika terdapat permohonan atas kepentingan dan keperluan Bahagian, Pentadbir Sistem ICT boleh mengaktifkan semula akaun pengguna dengan pertimbangan.	

KENYATAAN	TANGGUNGJAWAB
Pendaftaran dan Nyahdaftar Pengguna	
Proses pendaftaran dan nyahdaftar pengguna perlu dilaksanakan berdasarkan kepada tugas pemberian dan pengambilan semula capaian ke atas segala sistem dan perkhidmatan ICT mengikut keperluan semasa SEDA.	Pegawai Bahagian Perkhidmatan Digital (Infra)
Pengurusan Keutamaan Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pegawai Bahagian Perkhidmatan Digital (Infra)
Pengurusan Pengesahan Maklumat Rahsia Pengguna	
Pemberian maklumat rahsia pengguna yang telah disahkan perlu dikawal melalui proses pengurusan yang rasmi dan merujuk kepada Polisi Katalaluan.	Pegawai Bahagian Perkhidmatan Digital (Infra)
Semakan Hak Capaian Pengguna	
Pentadbir Sistem perlu semak dan kemaskini ke atas hak capaian pengguna.	Pegawai Bahagian Perkhidmatan Digital (Infra)
Penyahaktifan atau Pelarasan Hak Capaian Pengguna	
Hak akses untuk maklumat dan kemudahan pemprosesan maklumat bagi semua warga kerja SEDA Malaysia, pembekal, perunding perlu dinyahaktifkan selepas penamatan	Pegawai Bahagian Perkhidmatan Digital (Infra)

KENYATAAN	TANGGUNGJAWAB
perkhidmatan, kontrak atau perjanjian atau diselaraskan jika ada perubahan.	
6.19 Polisi Keselamatan Maklumat Berhubung Dengan Pembekal *(Information security in supplier relationships)*	
Keperluan untuk mengurangkan risiko yang berkaitan dengan keselamatan maklumat akses pembekal kepada aset SEDA harus dipersetujui dengan pembekal dan didokumenkan. Perkara yang perlu dipatuhi termasuk yang berikut: • Membaca, memahami dan mematuhi Polisi Keselamatan Siber SEDA; dan • Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Infra)
6.20 Elemen Keselamatan Dalam Perjanjian Dengan Pembekal (*Addressing* information *security within supplier agreements)*	
Keperluan keselamatan siber mestilah diambilkira secara menyeluruh di dalam perjanjian dengan Pihak Ketiga sebelum mereka dibenarkan mencapai aset ICT SEDA. Memastikan semua syarat keselamatan maklumat dan siber dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut boleh dimasukkan di dalam perjanjian yang dimeteraikan jika perlu:	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Infra)

KENYATAAN	TANGGUNGJAWAB
• Polisi Keselamatan Siber Pihak Berkuasa Pembangunan Tenaga Lestari; • Tapisan Keselamatan; • Perakuan Akta Rahsia Rasmi 1972; dan • Hak Harta Intelek.	
6.21 Mengurus Keselamatan Maklumat Siber Terhadap Rantaian Pembekal (*Managing information security in the information and communication technology (ICT) supply chain*)	
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: • Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; • Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan • Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Ketua Bahagian

KENYATAAN	TANGGUNGJAWAB
6.22 Memantau dan Menyemak Perkhidmatan Pembekal (*Monitoring, review and change management of supplier services)*	
SEDA hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: • Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; • Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan • Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	Pengarah / Ketua Bahagian dan Unit
Mengurus Perubahan untuk Perkhidmatan Pembekal	
Sebarang perubahan skop perkhidmatan yang diberikan oleh pihak ketiga perlu diurus mengikut keperluan semasa. Ianya termasuklah bekalan, perubahan terhadap perkhidmatan sedia ada dan pertambahan perkhidmatan baru. Penilaian risiko perlu dilakukan berdasarkan tahap kritikal sesuatu sistem dan impak yang wujud terhadap perubahan tersebut.	Pengarah / Ketua Bahagian dan Unit

KENYATAAN	TANGGUNGJAWAB
6.23 Keselamatan Maklumat dalam Perkhidmatan Awan (*Information security for use of cloud services)*	
Keperluan keselamatan dalam perkhidmatan awan mestilah diambilkira secara menyeluruh di dalam perjanjian dengan Pihak Ketiga sebelum mereka dibenarkan beroperasi. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga seperti penggunaan, pengurusan dan penamatan dengan pihak perkhidmatan awan.	• KPE • Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Ketua Undang-Undang
6.24 Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Siber (Information *security incident management planning and preparation)*	
Tanggungjawab dan Prosedur	
Prosedur pelaporan insiden keselamatan siber perlu dilaksanakan berdasarkan Prosedur Pengurusan Insiden Keselamatan Siber Prosedur pelaporan insiden keselamatan siber hendaklah berdasarkan Pekeliling / arahan kerajaan yang berkuat kuasa dari semasa ke semasa.	CSIRT SEDA
Melaporkan Peristiwa Keselamatan Maklumat	
Insiden keselamatan siber seperti berikut hendaklah dilaporkan kepada CSIRT SEDA, CSIRT Kementerian dan portal NC4 dengan kadar segera:	• Semua Warga kerja SEDA Malaysia • CSIRT SEDA

KENYATAAN	TANGGUNGJAWAB
• Maklumat yang didapati hilang, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; • Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; • Kata laluan atau mekanisma kawalan akses yang didapati hilang, dicuri atau didedahkan; • Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan • Berlaku percubaan pencerobohan, penyelewengan dan insiden-insiden yang tidak dijangka	
Melaporkan Kelemahan Keselamatan Maklumat	
Pelaporan juga perlu dilakukan sekiranya terdapat kelemahan keselamatan di dalam sistem atau perkhidmatan.	• Semua Warga kerja SEDA Malaysia • CSIRT SEDA
6.25 Penilaian dan Keputusan Peristiwa Keselamatan Maklumat (*Assessment and decision on information security events)*	
Kejadian keselamatan maklumat perlu dinilai dan diklasifikasikan sebagai insiden keselamatan maklumat.	CSIRT SEDA
6.26 Tindakbalas Terhadap Insiden Keselamatan Maklumat (*Response to information security Incidents)*	
Insiden keselamatan maklumat perlu diberi tindakbalas sewajarnya mengikut prosedur yang telah didokumenkan.	CSIRT SEDA

KENYATAAN	TANGGUNGJAWAB
6.27 Mengambil Pengajaran Dari Insiden Keselamatan Maklumat (*Learning from* information *security incidents)*	
Maklumat mengenai insiden keselamatan siber yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga perlulah digunakan untuk mengenal pasti insiden yang kerap berlaku atau insiden yang memberi kesan serta impak yang tinggi kepada SEDA.	CSIRT SEDA
6.28 Pengumpulan Bahan Bukti (*Collection of evidence)*	
Bahan-bahan bukti berkaitan insiden keselamatan siber hendaklah direkod, disimpan dan dikemaskini. Kawalan-kawalan yang perlu diambilkira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: • Menyimpan jejak audit, penduaan secara berkala dan melindungi integriti semua bahan bukti; • Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; • Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; • Menyediakan tindakan pemulihan segera; dan • Memaklumkan atau mendapatkan nasihat pihak berkuasa berkaitan perundangan sekiranya perlu.	CSIRT SEDA

KENYATAAN	TANGGUNGJAWAB
6.29 Melaksanakan Kesinambungan Keselamatan Maklumat (*Information security during Disruption)*	
Pelan kesinambungan perkhidmatan hendaklah dilaksanakan mengikut keperluan semasa bagi menentukan agar suatu pendekatan yang menyeluruh dapat diambil bagi mengekalkan kesinambungan perkhidmatan. Ini juga bertujuan untuk memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan SEDA dan menjamin keselamatan maklumat ICT SEDA.	• Pasukan Pelaksana ISMS • Bahagian DS
6.30 Kemudahan Kesediaan Pemprosesan Maklumat (*ICT readiness for business continuity)*	
Kemudahan pemprosesan maklumat perlu dilaksanakan dengan redundansi yang mencukupi untuk memenuhi keperluan ketersediaan, bergantung kepada keperluan.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)
Mengesah, Menyemak dan Menilai Kesinambungan Keselamatan Maklumat	
Pengesahan kawalan kesinambungan keselamatan maklumat perlu dilaksanakan secara berkala untuk memastikan bahawa ianya adalah sah dan berkesan semasa keadaan tidak diingini berlaku.	• Pasukan Pelaksana ISMS • Bahagian DS

KENYATAAN	TANGGUNGJAWAB
6.31 Undang-Undang, Statutori, Kawal Selia dan Kontrak Perjanjian (*Legal, statutory, regulatory and contractual requirements)*	
Mengenalpasti Keperluan Perundangan dan Kontrak	
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di SEDA: • Arahan Keselamatan; • Akta Rahsia Rasmi 1972; • Akta Siber Sekuriti 2024; dan • Akta Keselamatan Siber yang berkuat kuasa.	• KPE • Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)
6.32 Hak Harta Intelek (*Intellectual property rights)*	
Prosedur yang sesuai perlulah dilaksanakan untuk memastikan pematuhan kepada keperluan perundangan, kawalselia dan kontrak yang berkaitan dengan hak harta intelektual dan penggunaan produk perisian hak milik.	Pengarah / Ketua Bahagian dan Unit
6.33 Kawalan Rekod (*Protection of records)*	
Setiap rekod perlu dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses dan pendedahan yang tidak dibenarkan mengikut keperluan perundangan, peraturan, kontrak dan perkhidmatan.	Pengarah / Ketua Bahagian dan Unit

KENYATAAN	TANGGUNGJAWAB
6.34 Privasi dan Perlindungan Data Peribadi (*Privacy and protection of personal identifiable information (PII)*	
Privasi dan perlindungan maklumat peribadi yang boleh dikenalpasti perlu dilaksanakan mengikut keperluan semasa bagi menjamin tahap keselamatan maklumat berada dalam keadaan terkawal dan selamat pada setiap masa.	Pengarah / Ketua Bahagian dan Unit
6.35 Semakan Semula Keselamatan Maklumat (*Independent review of information security)*	
Pendekatan SEDA untuk menguruskan keselamatan maklumat dan pelaksanaan hendaklah dikaji secara berkala atau apabila perubahan ketara berlaku pada sebarang maklumat ICT SEDA dan ianya perlu dilakukan oleh pihak berkecuali atau pihak bebas.	Pengarah / Ketua Bahagian dan Unit
6.36 Pematuhan kepada Polisi, Peraturan dan Standard (*Compliance with policies, rules and standards for information security)*	
Setiap pengguna di Pihak Berkuasa Pembangunan Tenaga Lestari hendaklah membaca, memahami dan mematuhi Polisi Keselamatan Siber SEDA dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di Pihak Berkuasa Pembangunan Tenaga Lestari termasuk maklumat yang disimpan di dalamnya adalah hak milik SEDA dan KPE berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) perlu memastikan semua prosedur	Semua Warga kerja SEDA Malaysia, Pembekal dan Perunding.

KENYATAAN	TANGGUNGJAWAB
keselamatan dalam MyPortfolio masing-masing mematuhi polisi, piawaian dan keperluan teknikal.	
Semakan Semula Pematuhan Teknikal	
Sistem ICT mestilah diperiksa secara berkala untuk memastikan ianya mematuhi standard keselamatan yang sedia ada. Sebarang pematuhan teknikal mestilah dijalankan oleh individu yang kompeten yang diberi kebenaran.	Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)
6.37 Prosedur Operasi Didokumenkan (*Documented operating procedures*)	
Semua prosedur Keselamatan siber hendaklah diwujudkan disimpan dan dikawal. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (DS)

7. KAWALAN SUMBER MANUSIA

KENYATAAN	TANGGUNGJAWAB
7.1 Penyaringan (*Screening*)	
Menyatakan dengan lengkap dan jelas tentang peranan dan tanggungjawab setiap semua warga kerja SEDA Malaysia, pembekal dan perunding dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan. Tapisan keselamatan perlu dilaksanakan selaras dengan keperluan perkhidmatan di SEDA.	Pengarah Bahagian Pentadbiran dan Sumber Manusia
7.2 Terma dan Syarat Perkhidmatan (*Terms and conditions of employment)*	
Semua warga kerja SEDA Malaysia yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa serta mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh SEDA.	• Pengarah Bahagian Pentadbiran dan Sumber Manusia • Semua Warga kerja SEDA Malaysia
Tanggungjawab Pengurusan	
Pihak pengurusan perlu memastikan setiap warga kerja SEDA Malaysia, pembekal, perunding dan pihak yang berkepentingan dalam memberikan perkhidmatan dan menguruskan keselamatan aset ICT berdasarkan kepada perundangan dan peraturan yang telah ditetapkan oleh organisasi sama ada dari segi dasar, polisi, prosedur dan panduan. Semua warga kerja SEDA Malaysia, pembekal, perunding dan pihak berkepentingan yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	• KPE • Pengarah / Ketua-Ketua Bahagian dan Unit

KENYATAAN	TANGGUNGJAWAB
7.3 Kesedaran, Pendidikan dan Latihan Berkaitan Keselamatan Maklumat (*Information security awareness, education and training)*	
Memastikan latihan kesedaran dan perkara-perkara yang berkaitan dengan pengurusan keselamatan maklumat diberikan kepada semua warga kerja SEDA Malaysia dari semasa ke semasa sekiranya perlu.	Pengarah Bahagian Pentadbiran dan Sumber Manusia
7.4 Proses Tatatertib (*Disciplinary process)*	
Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas semua warga kerja SEDA Malaysia, pembekal dan perunding sekiranya berlaku perlanggaran berkaitan perundangan dan peraturan yang telah ditetapkan oleh organisasi	• Pengarah Bahagian Pentadbiran dan Sumber Manusia • Jawatankuasa Berkaitan tatatertib
7.5 Penamatan dan Perubahan Perkhidmatan (*Responsibilities after termination or change of employment)*	
Memastikan semua aset ICT dikembalikan kepada SEDA mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan. Membatalkan semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan SEDA dan/atau terma perkhidmatan.	• Pengarah Bahagian Pentadbiran dan Sumber Manusia • Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)
7.6 Perjanjian NDA (*Confidentiality or Non-Disclosure Agreements)*	
Perjanjian dengan pembekal/individu harus merangkumi keperluan untuk menangani sebarang risiko keselamatan maklumat yang berkaitan dengan teknologi maklumat dan komunikasi dan rantaian bekalan produk/perkhidmatan.	Pengarah / Ketua-Ketua Bahagian dan Unit

KENYATAAN	TANGGUNGJAWAB
Tanggungjawab kerahsiaan atau ketakdedahan hendaklah diperuntukkan di dalam sesuatu perjanjian atau perjanjian kerahsiaan - *Non Disclosure Agreement (NDA)* yang ditandatangani antara SEDA dan pihak luar yang berkaitan mengikut dasar, prosedur dan keperluan organisasi serta hendaklah dikenalpasti, disemak dan didokumentasikan. Tanggungjawab kerahsiaan tersebut hendaklah dipersetujui dan dipatuhi oleh semua pihak bagi memenuhi keperluan keselamatan maklumat yang relevan.	
7.7 Bekerja Jarak Jauh (*Remote Working*)	
Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan. Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi telekerja. Berikut adalah langkah-langkah yang perlu dipatuhi: • Memastikan proses pengesahan pengguna remote digunakan untuk mengawal capaian logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh. • Sebarang capaian ke dalam operasi teknikal dari luar SEDA hanya dibenarkan dengan akses melalui VPN (Virtual Private Network) rasmi SEDA dan perlu mendapat kelulusan ICTSO. • Pihak ketiga yang perlu melaksanakan kerja menggunakan VPN untuk memberi perkhidmatan sokongan atau bantuan teknikal hendaklah dipantau sepanjang masa sehingga tugas berkenaan selesai.	• Semua Warga kerja SEDA Malaysia • Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Infra)

KENYATAAN	TANGGUNGJAWAB
• Sebarang perkara berkaitan pengurusan akaun VPN perlu merujuk kepada prosedur yang sedang berkuatkuasa.	
7.8 Laporan Peristiwa Keselamatan Maklumat (*Information security event reporting*)	
Insiden keselamatan siber seperti berikut hendaklah dilaporkan kepada CSIRT SEDA dengan kadar segera: • Maklumat yang didapati hilang, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; • Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; • Kata laluan atau mekanisma kawalan akses yang didapati hilang, dicuri atau didedahkan; • Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan • Berlaku percubaan pencerobohan, penyelewengan dan insiden-insiden yang tidak dijangka.	Semua Warga kerja SEDA Malaysia

8. KAWALAN FIZIKAL

KENYATAAN	TANGGUNGJAWAB
8.1 Sempadan Keselamatan Fizikal (*Physical security perimeters*)	
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut: • Kawasan keselamatan fizikal hendaklah di kenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal	• Pengarah Bahagian Pentadbiran dan Sumber Manusia • Semua Warga kerja SEDA Malaysia

KENYATAAN	TANGGUNGJAWAB
hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; • Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; • Memperkukuhkan dinding dan siling; • Menghadkan jalan keluar masuk; • Mengadakan kaunter kawalan jika perlu; • Menyediakan tempat atau bilik khas untuk pelawat jika perlu; • Mewujudkan perkhidmatan kawalan keselamatan jika perlu; dan • Kawasan akses awam, penghantaran dan pemunggahan mesti dikawal, dipantau dan diasingkan daripada kemudahan pemprosesan maklumat untuk menghalang capaian yang tidak dibenarkan.	
8.2 Kawalan Kemasukan Fizikal (*Physical entry)*	
Setiap warga kerja SEDA Malaysia di Pihak Berkuasa Pembangunan Tenaga Lestari hendaklah memakai kad ID atau sebarang pengenalan diri sepanjang waktu bertugas Setiap pelawat perlu mendaftar di pintu masuk ke kawasan atau tempat berurusan. Hanya pegawai, staff dan pelawat yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT.	• Pengarah Bahagian Pentadbiran dan Sumber Manusia • Semua Warga kerja SEDA Malaysia
8.3 Kawalan Pejabat, Bilik dan Kemudahan (*Securing offices, rooms and facilities)*	
Keselamatan fizikal untuk pejabat, bilik dan kemudahan perlu dilaksanakan mengikut keperluan SEDA bagi memastikan maklumat dan kemudahan pemprosesan maklumat tidak dapat dicapai tanpa kebenaran yang disahkan dan juga bagi	• Pengarah Bahagian Pentadbiran dan Sumber Manusia

KENYATAAN	TANGGUNGJAWAB
menghalang sebarang bentuk kemusnahan dan ganggu gugat yang boleh memberi ancaman kepada keselamatan.	• Semua Warga kerja SEDA Malaysia
8.4 Pemantauan Keselamatan Fizikal (*Physical security monitoring)*	
Keselamatan fizikal hendaklah sentiasa dipantau daripada akses fizikal yang tidak dibenarkan.	Pengarah / Ketua-Ketua Bahagian dan Unit
8.5 Perlindungan Terhadap Ancaman Luaran dan Persekitaran (*Protecting against physical and environmental threats)*	
Perlindungan fizikal terhadap kejadian bencana alam, serangan berbahaya atau insiden seperti kebakaran, banjir, gempa bumi, letupan, rusuhan awam dan lain-lain bentuk bencana alam atau perbuatan manusia perlu dilaksanakan mengikut keperluan semasa	Semua Warga kerja SEDA Malaysia
8.6 Bekerja di Kawasan Larangan (*Working in secure areas)*	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan staff yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Contoh kawasan larangan di SEDA adalah Bilik Server, Bilik UPS dan Bilik Fail. Memastikan peralatan ICT dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai dan	Semua Warga kerja SEDA Malaysia

KENYATAAN	TANGGUNGJAWAB
Semua penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada KPE.	
Kawasan Penghantaran dan Pemunggahan	
Semua akses yang melibatkan kawasan penghantaran dan pemunggahan dan kawasan lain di mana orang yang tidak dibenarkan boleh memasuki premis organisasi perlulah dikawal dan diasingkan dari kemudahan pemprosesan maklumat bagi menghalang sebarang kemungkinan akses yang tidak dibenarkan.	Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)
8.7 Meja dan Skrin Bebas daripada Maklumat Sensitif (*Clear desk and clear screen)*	
Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. ***Clear Desk*** bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci.	Semua Warga kerja SEDA Malaysia
8.8 Penempatan Peralatan dan Perlindungan (*Equipment siting and protection)*	
Peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu.	Semua Warga kerja SEDA Malaysia

KENYATAAN	TANGGUNGJAWAB
Setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya. Sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan adalah dilarang. Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (activated) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan. Peralatan-peralatan kritikal perlu disokong oleh Uninterruptable Power Supply (UPS). Semua peralatan di SEDA yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai. Peralatan ICT yang hendak dibawa keluar dari premis SEDA perlulah mendapat kelulusan Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) dan direkodkan bagi tujuan pemantauan kecuali komputer riba dan tablet yang dibekalkan kepada setiap pengguna. Peralatan ICT yang hilang hendaklah dilaporkan kepada	Semua Warga kerja SEDA Malaysia

KENYATAAN	TANGGUNGJAWAB
Bahagian Teknologi Maklumat dan Pegawai Aset dengan segera. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal. Pengguna dilarang sama sekali mengubah katalaluan *administrator* yang telah ditetapkan oleh Pentadbir Sistem ICT. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS). Hanya peralatan ICT yang dibekalkan dan dibenarkan oleh Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) sahaja boleh diguna pakai di SEDA.	Semua Warga kerja SEDA Malaysia
8.9 Keselamatan Peralatan dan Aset di Luar Kawasan (*Security of assets off premises*)	
Bagi perkakasan yang dibawa keluar dari premis Pihak Berkuasa Pembangunan Tenaga Lestari, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan Pihak Berkuasa Pembangunan Tenaga Lestari. Peralatan perlu dilindungi dan dikawal sepanjang masa. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua Warga kerja SEDA Malaysia

KENYATAAN	TANGGUNGJAWAB
8.10 Pengurusan Media Boleh Alih (*Storage media)*	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: • Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; • Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; • Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; • Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan • Menyimpan semua media di tempat yang selamat.	Pengarah / Ketua-Ketua Bahagian dan Unit
8.11 Utiliti Sokongan (*Supporting utilities)*	
Peralatan yang kritikal perlu dilindungi dari kegagalan kuasa elektrik dan sebarang gangguan lain yang disebabkan oleh kegagalan utiliti sokongan.	Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)
8.12 Keselamatan Pengkabelan (*Cabling security)*	
Kabel elektrik dan telekomunikasi yang menyalurkan data atau menyokong sistem penyampaian perkhidmatan hendaklah dilindungi kerana ianya boleh menjadi punca terdedahnya maklumat dan mengganggu kebolehsediaan perkhidmatan. Antara langkah-langkah keselamatan yang boleh diambil untuk memastikan keselamatan pengkabelan adalah seperti berikut:	Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)

KENYATAAN	TANGGUNGJAWAB
• Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; • Kabel hendaklah dilindungi daripada kerosakan yang disengajakan atau tidak disengajakan; • Laluan pemasangan kabel hendaklah dilindungi sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan • Membuat pelabelan kabel menggunakan kod tertentu.	
8.13 Penyelenggaraan Peralatan (*Equipment maintenance)*	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan keintegritian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: • Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; • Memastikan perkakasan hanya boleh diselenggara oleh staff atau pihak yang dibenarkan sahaja; • Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; • Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; • Memaklumkan kepada pengguna sebelu melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan • Semua penyelenggaraan mestilah mendapat kebenaran daripada Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS).	Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)

KENYATAAN	TANGGUNGJAWAB
8.14 Pelupusan (*Secure disposal or re-use of equipment)*	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada ianya aset harta modal atau inventori yang dibekalkan oleh SEDA dan ditempatkan di SEDA Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan SEDA. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: • Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui shredding, grinding, degauzing atau pembakaran; • Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; • Peralatan ICT yang akan dilupuskan sebelum dipindahmilik hendaklah dipastikan agar maklumat-maklumat dalam penyimpanan telah dihapuskan dengan cara yang selamat; • Pegawai aset hendaklah mengenalpasti sama ada peralatan tersebut boleh dilupuskan atau sebaliknya; • Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; • Pegawai aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam sistem inventori; dan	Pegawai Aset Bahagian

KENYATAAN	TANGGUNGJAWAB
• Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuatkuasa. Semua warga kerja SEDA Malaysia SEDA adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut: • Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; • Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, harddisk, motherboard dan sebagainya; • Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di SEDA; • Memindah keluar dari SEDA mana-mana peralatan ICT yang hendak dilupuskan; dan • Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan aset adalah di bawah tanggungjawab SEDA.	
Pelupusan yang Selamat atau Penggunaan Semula Peralatan	
Semua peralatan yang mengandungi media penyimpanan (storan) perlu diperiksa untuk memastikan sebarang maklumat sensitif dan perisian berlesen telah dimusnahkan dengan selamat sebelum dilupuskan atau digunakan semula. Semua warga kerja SEDA Malaysia SEDA bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media penyimpanan kedua seperti thumb drive, external harddisk, CD dan media lain yang berkenaan sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	Semua Warga kerja SEDA Malaysia

KENYATAAN	TANGGUNGJAWAB
Peralatan Gunasama ICT	
Pengguna perlu memastikan peralatan yang dikongsi bersama perlu diawasi dan diberi perlindungan sewajarnya.	Semua Warga kerja SEDA Malaysia

9. KAWALAN TEKNOLOGI

KENYATAAN	TANGGUNGJAWAB
9.1 Prosedur "Log-on" yang Selamat *(User end point devices)*	
Akses kepada sistem dan aplikasi perlu dikawal oleh prosedur "*log-on*" (prosedur keselamatan sistem aplikasi) yang selamat mengikut keperluan keselamatan yang sesuai.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Pentadbir Sistem)
9.2 Mengehadkan Capaian Maklumat (*Privileged access rights)*	
Capaian sistem dan aplikasi di SEDA adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: • Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; • Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Pentadbir Sistem)

KENYATAAN	TANGGUNGJAWAB
• Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan • Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimana pun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja	
9.3 Sekatan Akses Maklumat (*Information access restriction)*	
Penggunaan program utiliti khas yang berkemungkinan mampu untuk mengatasi kawalan sistem dan aplikasi perlu dihadkan dan dikawal ketat.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Infra)
9.4 Kawalan Capaian kepada Kod Sumber Program (*Access to source code)*	
Capaian kepada kod sumber program mestilah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: • Log audit perlu dikekalkan kepada semua akses kepada kod sumber; • Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan • Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik SEDA.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Pentadbir Sistem)

KENYATAAN	TANGGUNGJAWAB
9.5 Pengurusan Kunci Digital (*Secure authentication)*	
Pengurusan kunci digital hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci digital berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci digital tersebut.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Pentadbir Sistem)
9.6 Pengurusan Kapasiti (*Capacity management)*	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Pentadbir Sistem)
9.7 Kawalan Terhadap Perisian Berisiko (*Protection against malware*)	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: Memasang sistem keselamatan seperti antivirus untuk mengesan perisian atau program berbahaya, serta mengikut prosedur penggunaan yang betul dan selamat. Hanya memasang dan menggunakan perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa.	Semua warga kerja SEDA Malaysia

KENYATAAN	TANGGUNGJAWAB
Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya. Mengemaskini antivirus dengan pattern antivirus yang terkini. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya. Memasukkan klausa waranti di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baikpulih sekiranya perisian tersebut mengandungi program berbahaya. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan. Memberi amaran mengenai ancaman keselamatan siber seperti serangan virus.	
9.8 Pengurusan Kelemahan Teknikal (*Management of technical vulnerabilities)*	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut : • Mendapatkan maklumat teknikal berkaitan keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Pentadbir Sistem)

KENYATAAN	TANGGUNGJAWAB
• Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan • Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	
9.9 Pengurusan Konfigurasi (*Configuration management)*	
Pengurusan konfigurasi yang merangkumi konfigurasi keselamatan, perkakasan, perisian, perkhidmatan dan rangkaian hendaklah diwujudkan, didokumenkan, dilaksanakan, dipantau dan dikaji semula.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Pentadbir Sistem)
9.10 Pemadaman Maklumat (*Information deletion)*	
Maklumat yang disimpan dalam sistem maklumat, peranti atau dalam mana-mana media storan lain perlu dipadamkan apabila tidak lagi diperlukan. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Semua warga kerja SEDA Malaysia
9.11 *Data Masking*	
Data masking hendaklah digunapakai sewaktu pengujian sistem mengikut peraturan organisasi dan kawalan akses dengan mengambil kira prosedur yang berkaitan.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan

KENYATAAN	TANGGUNGJAWAB
	Digital (Pentadbir Sistem)
9.12 *Pencegahan* Kebocoran Data *(Data leakage prevention)*	
Langkah-langkah pencegahan kebocoran data hendaklah dilaksanakan bagi memastikan sistem aplikasi, rangkaian dan mana-mana peranti lain yang memproses, menyimpan atau menghantar maklumat sensitif dilindungi. Pemasangan perisian ke atas sistem yang sedang beroperasi perlu dikawal untuk memastikan tiada sebarang gangguan yang boleh menjejaskan integriti daripada berlaku semasa dan/atau selepas pemasangan perisian.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Pentadbir Sistem)
9.13 Penduaan Maklumat (*Information Backup*)	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan di simpan di *off site.* Membuat salinan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaharu. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian Perkhidmatan Digital (Pentadbir Sistem)

KENYATAAN	TANGGUNGJAWAB
Menyimpan sekurang-kurangnya tiga (3) generasi backup. Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.	
9.14 Redundansi (*Redundancy of information processing facilities*)	
Kemudahan pemprosesan maklumat perlu dilaksanakan dengan redundansi yang mencukupi untuk memenuhi keperluan ketersediaan, bergantung kepada keperluan.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Infra)
9.15 Pengrekodan Log (*Logging*) **9.16 Aktiviti Pemantauan (*Monitoring activities*)**	
Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan. Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti yang berikut:	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem) • Pegawai Bahagian DS (Infra)

KENYATAAN	TANGGUNGJAWAB
• Fail log sistem pengoperasian; • Fail log servis (contoh: web); • Fail log aplikasi (audit trail); dan • Fail log rangkaian (contoh: firewall) Pemantauan sistem, rangkaian dan aplikasi hendaklah sentiasa dilakukan dengan tindakan yang sesuai perlu diambil untuk menilai insiden keselamatan maklumat	
9.17 Penyeragaman Jam (*Clock synchronization)*	
Waktu server dan peralatan ICT yang berpusat dan kritikal perlu diselaraskan dengan satu sumber waktu yang piawai. Server yang bukan di bawah kawalan PTMK digalakkan untuk menggunakan Network Time Protocol (NTP) Server. Masa yang berkaitan dengan sistem pemprosesan maklumat ICT SEDA mestilah diseragamkan mengikut rujukan punca masa yang sama yang digunakan oleh organisasi. Ini untuk memastikan ketepatan masa log yang disimpan serta bertujuan untuk mengawal integriti log tersebut bagi kegunaan masa hadapan.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Infra)
9.18 Penggunaan program utiliti khas (*Use of privileged utility programs*)	
Penggunaan program utiliti khas yang berkemungkinan mampu untuk mengatasi kawalan sistem dan aplikasi perlu dihadkan dan dikawal ketat.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Infra)

KENYATAAN	TANGGUNGJAWAB
9.19 Sekatan ke atas Pemasangan Perisian *(Installation of software on* operational *systems)*	
Pemasangan perisian oleh pengguna perlu dikawal dan disemak secara berkala bagi memastikan tiada sebarang bentuk ancaman atau gangguan ke atas sistem yang beroperasi.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Infra)
9.20 Keselamatan Rangkaian (*Networks security)* **9.21 Keselamatan Perkhidmatan Rangkaian (*Security of network services)*** **9.22 Pengasingan Dalam Rangkaian (*Segregation of networks)*** **9.23 Tapisan Web *(Web filtering)***	
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk. *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan Pihak Berkuasa Pembangunan Tenaga Lestari.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem) • Pegawai Bahagian DS (Infra)

KENYATAAN	TANGGUNGJAWAB
Akses secara fizikal dan logikal ke atas port diagnostik dan port konfigurasi perlu dikawal. Sebarang penyambungan rangkaian yang bukan di bawah kawalan Pihak Berkuasa Pembangunan Tenaga Lestari hendaklah mendapat kebenaran Pengurus Teknologi Maklumat. Semua pengguna hanya dibenarkan menggunakan rangkaian Pihak Berkuasa Pembangunan Tenaga Lestari sahaja. Penggunaan “mobile broadband” peribadi adalah dilarang sama sekali. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum. Sebarang penyambungan rangkaian daripada pihak ketiga (remote tunneling) ke dalam sistem rangkaian Pihak Berkuasa Pembangunan Tenaga Lestari hendaklah mendapat kebenaran Pengurus Teknologi Maklumat, sekiranya ada. Rangkaian untuk pengguna, sistem perkhidmatan dan sistem maklumat juga perlulah diasingkan.	
9.24 Peraturan Kawalan Kriptografi *(Use of cryptography)*	
Kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang dan peraturan yang relevan mengikut keperluan semasa. Pengguna hendaklah membuat enkripsi (encryption) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Infra)

KENYATAAN	TANGGUNGJAWAB
9.25 Kitar Hayat Keselamatan Pembangunan (*Secure development life cycle)*	
Kaedah untuk pembangunan perisian dan sistem yang selamat hendaklah diwujudkan dan digunakan SEDA hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: • Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; • Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan • Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian. Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. SEDA perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira perkara-perkara berikut: • Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; • Patuh kepada keperluan undang-undang dan peraturan dalaman dan luaran; • Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; • Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem;	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem) • Pegawai Bahagian DS (Infra)

KENYATAAN	TANGGUNGJAWAB
• Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan • Kawalan ke atas capaian kepada persekitaran pembangunan sistem	
9.26 Kawalan Keselamatan Aplikasi (*Application security requirements)*	
Keperluan keselamatan maklumat hendaklah dikenalpasti, ditentukan dan diluluskan semasa membangunkan atau memperoleh permohonan Kawalan keselamatan aplikasi di rangkaian awam perlu dikawal dan disemak secara berkala untuk memastikan kawalan keselamatan yang sesuai dapat diolah dan diterapkan ke dalam aplikasi bagi menghalang sebarang bentuk kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat daripada berlaku kepada aplikasi Perkara-perkara yang perlu dipatuhi adalah seperti berikut: • Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin kesahihan dan ketepatan; • Menggabungkan semakan pengesahan ke dalam aplikasi untuk mengenalpasti sebarang kerosakan maklumat sama ada disebabkan oleh ralat pemprosesan atau tindakan yang disengajakan; • Mengenalpasti dan melaksanakan kawalan untuk mengesah dan melindungi integriti mesej dalam sistem aplikasi; dan • Melaksanakan proses pengesahan ke atas output data bagi menjamin kesahihan dan ketepatan pemprosesan sistem aplikasi. Sistem maklumat hendaklah mengambilkira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem) • Pegawai Bahagian DS (Infra)

KENYATAAN	TANGGUNGJAWAB
yang boleh mengganggu pemprosesan dan ketepatan maklumat. Ujian keselamatan hendaklah dijalankan ke atas sistem input bagi tujuan menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna serta sistem output untuk memastikan data yang telah diproses adalah tepat. Sebaiknya-baiknya, semua sistem yang dibangunkan sama ada secara dalaman atau outsource hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	
Polisi Pembangunan Aplikasi	
Pembangunan aplikasi dan sistem perlu dilaksanakan mengikut keperluan dan ianya hendaklah dikaji dan disemak secara berkala untuk memastikan keberkesanannya. Peraturan bagi pembangunan aplikasi dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: • Keselamatan persekitaran pembangunan; • Keselamatan pangkalan data; • Keperluan keselamatan dalam fasa reka bentuk; • Keperluan check point keselamatan dalam carta perbatuan projek; • Keperluan pengetahuan ke atas keselamatan aplikasi; • Keselamatan dalam kawalan versi; dan	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem) • Pegawai Bahagian DS (Infra)

KENYATAAN	TANGGUNGJAWAB
• Bagi pembangunan secara penyumberluaran (outsource), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	
9.27 Prinsip Keselamatan Berkaitan Kejuruteraan Sistem *(Secure system architecture and engineering principles)*	
Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada prosedur atau garis panduan yang berkuatkuasa Prinsip keselamatan dalam pembangunan dan sokongan sistem yang berkaitan dengan kejuruteraan sistem perlu dikekalkan dan direkodkan.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem) • Pegawai Bahagian DS (Infra)
9.28 Keselamatan Pengekodan (*Secure coding)*	
Peraturan keselamatan pengekodan hendaklah digunakan untuk pembangunan perisian.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem)

KENYATAAN	TANGGUNGJAWAB
9.29 Ujian Keselamatan Dalam Pembangunan dan Penerimaan Sistem (*Security testing in development and acceptance)*	
Maklumat yang terlibat dalam urusniaga perkhidmatan permohonan hendaklah dilindungi untuk mencegah penghantaran yang tidak lengkap, salah penghantaran dan pendedahan, pengubahan mesej dan duplikasi mesej yang tidak dibenarkan atau berulang.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem)
9.30 Pembinaan Perisian Secara Luaran (Outsource) (*Outsourced development)*	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. *Source code* adalah menjadi hak milik SEDA. SEDA hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara outsource oleh pihak luar. Bagi sistem aplikasi yang dibangunkan oleh pembekal, klausa mengenai pemindahan Teknologi (Transfer of Technology), tempoh jaminan, kod sumber (source code) sebagai HAK MILIK SEDA hendaklah dinyatakan dengan jelas dalam dokumen kontrak perjanjian. Perkara yang perlu dipatuhi adalah seperti yang berikut: • Perkiraan perlesenan, kod sumber ialah HAK MILIK SEDA dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara outsource; • Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori bahawa kod sumber perlu diserahkan kepada SEDA;	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem)

KENYATAAN	TANGGUNGJAWAB
• Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; • Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem; • Mengguna pakai prinsip dan tatacara *escrow*; dan • Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.	
9.31 Pengasingan Segmen Pembangunan, Pengujian dan Persekitaran Operasi (*Separation of development, test and production environments)*	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: • Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; • Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan • Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem)
Keselamatan Persekitaran dalam Pembangunan Aplikasi	
Persekitaran yang sihat dan selamat perlu diwujudkan sepanjang proses pembangunan aplikasi dijalankan dari segi memastikan keselamatan ke atas proses untuk	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian

KENYATAAN	TANGGUNGJAWAB
pembangunan sistem dan integrasi yang meliputi kitaran hayat keseluruhan pembangunan sistem.	Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem)
9.32 Pengurusan Perubahan (*Change management)*	
Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) terlebih dahulu. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh Juruteknik Komputer Jabatan atau pegawai yang diberi kuasa yang mempunyai pengetahuan dan terlibat secara langsung dengan aset ICT berkenaan. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem)
Prosedur Kawalan Perubahan Sistem	
Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum ianya digunapakai bagi menghalang sebarang peluang untuk membocorkan maklumat.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)

KENYATAAN	TANGGUNGJAWAB
	• Pegawai Bahagian DS (Pentadbir Sistem)
Semakan Teknikal Bagi Aplikasi Setelah Pertukaran Platform Sistem Pengoperasian	
Apabila pengoperasian sistem ditukar, aplikasi yang kritikal mesti disemak dan diuji untuk memastikan tiada kesan sampingan terhadap keselamatan dan operasi SEDA secara khususnya dan organisasi secara amnya daripada berlaku.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem)
Sekatan ke atas Perubahan Pakej Perisian	
Mengawal perubahan dan pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja dan Akses kepada kod sumber aplikasi perlu dihadkan kepada pengguna yang diizinkan sahaja	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS) • Pegawai Bahagian DS (Pentadbir Sistem)
9.33 Ujian Keselamatan Sistem *(Test Information)*	
Semua sistem baru merangkumi sistem yang dikemaskini atau diubahsuai hendaklah memenuhi kriteria yang telah ditetapkan sebelum ianya diterima atau dipersetujui. Ujian fungsi keselamatan harus dijalankan semasa pembangunan sistem.	• Ketua Pegawai Digital (CDO) / Pengarah Bahagian Perkhidmatan Digital (DS)

KENYATAAN	TANGGUNGJAWAB
Data ujian mesti dilakukan secara teliti, dikawal dan dilindungi. Data ujian perlu dihapuskan setelah penggunaannya selesai. Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: • Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; • Sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna; • Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat; dan • Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.	• Pegawai Bahagian DS (Pentadbir Sistem)
9.34 Pengawalan Audit Sistem Maklumat (*Protection of information systems during audit testing)*	
Keperluan dan aktiviti audit yang memerlukan pengesahan sistem yang beroperasi perlulah dirancang sebaik mungkin dan ianya hendaklah dipersetujui untuk mengurangkan gangguan kepada proses-proses lain yang sedang beroperasi di dalam organisasi	Pegawai Bahagian DS (Pentadbir Sistem)