KEMENTERIAN DIGITAL
JABATAN DIGITAL NEGARA

POLISI KESELAMATAN SIBER JABATAN DIGITAL NEGARA

VERSI 1.0

KEMENTERIAN DIGITAL
JABATAN DIGITAL NEGARA

POLISI KESELAMATAN SIBER
JABATAN DIGITAL NEGARA

Disediakan Oleh:	Disemak Oleh:	Diluluskan Oleh:
.....	.....	.....
Nama: Ts. Dr. Nurul Aisyah Sim binti Abdullah Jawatan: Timbalan Pengarah, Unit Pengurusan Keselamatan Maklumat, Trek Teknikal, Bahagian Perundingan Digital	Nama: Hamidah binti Mat Saat @ Abas Jawatan: ICTSO, Jabatan Digital Negara	Nama: Ts. Dr. Fazidah Binti Abu Bakar Jawatan: Ketua Pengarah, Jabatan Digital Negara
Tarikh: 21 Jun 2024	Tarikh: 24 Jun 2024	Tarikh: 25 Jun 2024

Versi: 1.0 25 Jun 2024		

PRAKATA

Assalamualaikum Warahmatullahi Wabarakatuh dan Salam Sejahtera,

Dalam era yang serba digital ini, keperluan untuk melindungi data dan infrastruktur kritikal kerajaan daripada ancaman siber menjadi semakin penting. Jabatan Digital Negara, sebagai jabatan yang menerajui pendigitalan kerajaan, memainkan peranan yang amat penting dalam memastikan keselamatan siber sentiasa terpelihara untuk mendukung misi kerajaan digital mampan yang menjadi pemangkin kepada negara digital.

Visi Jabatan Digital Negara untuk memacu pendigitalan kerajaan tidak akan dapat dicapai tanpa adanya rangka kerja keselamatan siber yang kukuh dan berkesan. Polisi Keselamatan Siber Jabatan Digital Negara ini ialah manifestasi komitmen kita untuk melindungi aset digital kerajaan dan memastikan keberlangsungan operasi digital yang selamat dan terlindung daripada sebarang ancaman keselamatan siber.

Saya berharap agar semua pihak yang terlibat dapat memberikan kerjasama yang padu dalam melaksanakan polisi ini dengan penuh dedikasi dan tanggungjawab serta mematuhi Polisi Keselamatan Siber Jabatan Digital Negara yang ditetapkan demi mencapai aspirasi kita untuk menjadikan Malaysia sebuah negara digital yang maju dan selamat.

Sekian, terima kasih.

TS. DR. FAZIDAH BINTI ABU BAKAR
Ketua Pengarah
Jabatan Digital Negara
25 JUN 2024

ISI KANDUNGAN

REKOD PINDAAN DOKUMEN

Versi	Kelulusan	Tarikh Kuat Kuasa
1.0	JPICT JDN	25 Jun 2024

1. PENGENALAN

1.1. LATAR BELAKANG

1.1.1. Polisi Keselamatan Siber (PKS) Jabatan Digital Negara (JDN) ialah dokumen yang menetapkan hala tuju yang jelas bagi Jabatan Digital Negara dalam usaha memastikan keselamatan maklumat secara menyeluruh. Polisi ini telah mendapat kelulusan rasmi serta komitmen penuh daripada pengurusan tertinggi untuk pelaksanaan yang efektif.

1.1.2. Polisi ini disediakan dengan tujuan untuk melindungi kerahsiaan, integriti, dan ketersediaan maklumat di Jabatan Digital Negara merangkumi satu set arahan, peraturan, garis panduan, dan amalan yang ditetapkan untuk melindungi maklumat serta data yang sensitif dan kritikal daripada capaian yang tidak sah, kehilangan, atau pendedahan yang tidak dibenarkan.

1.1.3. PKS JDN ini mentakrifkan kawalan keselamatan yang bersesuaian berdasarkan dasar, pekeliling, garis panduan kerajaan semasa yang berkuat kuasa serta mengikut amalan terbaik keselamatan yang relevan. Polisi ini terpakai kepada semua sistem dan persekitaran maklumat Jabatan Digital Negara, memastikan perlindungan menyeluruh terhadap ancaman siber yang semakin kompleks.

1.2. TUJUAN

PKS JDN dibangunkan untuk mewujudkan rangka kerja yang komprehensif dalam melindungi aset maklumat JDN daripada ancaman dan kerentanan yang mungkin timbul. Polisi ini bertujuan untuk memastikan kerahsiaan, integriti, dan ketersediaan maklumat, sambil mematuhi keperluan undang-undang dan peraturan yang relevan. Dengan wujudnya PKS JDN ini, diharapkan pengurusan keselamatan data dan maklumat di jabatan ini akan menjadi lebih efisien dan efektif, serta dapat meningkatkan tahap jaminan keselamatan yang lebih tinggi.

1.3. OBJEKTIF

PKS JDN ini bertujuan mencapai objektif-objektif utama berikut:

(a) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dalam aspek kerahsiaan, integriti, kebolehsediaan, dan kesahihan maklumat serta penyangkalan;

(b) Mematuhi keperluan perundangan, peraturan, standard, pekeliling dan prosedur yang sedang berkuat kuasa;

(c) Melaksanakan pengurusan risiko dan insiden keselamatan siber yang lebih berkesan;

(d) Memastikan penyampaian perkhidmatan JDN pada tahap keselamatan tertinggi yang dapat meningkatkan keyakinan pihak berkepentingan seperti jabatan kerajaan, industri, dan orang awam;

(e) Menjamin kelancaran operasi dan kesinambungan perkhidmatan Jabatan Digital Negara dengan meminimumkan impak insiden keselamatan maklumat fizikal dan logikal;

(f) Memudahkan perkongsian maklumat yang selamat dan terjamin;

(g) Mencegah sebarang penyalahgunaan atau kecurian maklumat kerajaan; dan

(h) Menyediakan asas bagi penambahbaikan yang berterusan dalam pengurusan keselamatan dan pentadbiran teknologi maklumat dan komunikasi.

1.4. SKOP

1.4.1. PKS JDN merupakan panduan utama bagi semua warga JDN serta pihak-pihak yang terlibat dalam pengurusan data atau maklumat di jabatan ini. Polisi ini memperincikan peranan, tanggungjawab, arahan, peraturan, garis panduan, dan amalan yang **WAJIB DIBACA, DIFAHAMI, dan DIPATUHI** oleh semua warga jabatan, termasuk pembekal, pakar runding, serta pihak-pihak yang terlibat dengan perkhidmatan teknologi maklumat dan komunikasi JDN.

1.4.2. Polisi ini juga terpakai untuk pelindungan terhadap kesemua aset maklumat Jabatan Digital Negara, yang meliputi data dan maklumat dalam bentuk digital (softcopy) atau bercetak (hardcopy), perkakasan, perisian, infrastruktur ICT, manusia, dan premis. Aset-aset ini adalah sangat penting dan sangat berharga, memastikan Jabatan Digital Negara dapat menjalankan urusan rasmi Kerajaan dengan lancar kepada masyarakat, sektor swasta, serta jabatan kerajaan yang berkaitan.

1.4.3. PKS JDN menetapkan keperluan asas seperti yang berikut:

(a) **Kebolehcapaian Data dan Maklumat:** Data dan maklumat mesti dapat dicapai secara berterusan dengan pantas, tepat, mudah, dan boleh dipercayai. Ini adalah penting untuk memastikan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.

(b) **Kerahsiaan dan Kesempurnaan Maklumat:** Semua data dan maklumat hendaklah dilindungi kerahsiaannya dan dikendalikan dengan baik pada setiap masa untuk memastikan ketepatan serta melindungi kepentingan kerajaan, perkhidmatan, dan masyarakat.

1.4.4. Untuk memastikan keselamatan aset maklumat sepanjang masa, PKS JDN meliputi perlindungan semua bentuk maklumat kerajaan yang diwujudkan, diproses, disimpan, dihantar, sedang digunakan, diedarkan, disimpan, diselenggara, dihapuskan dan dimusnahkan serta diarkibkan dalam persekitaran ICT JDN. Perlindungan ini dilaksanakan melalui sistem kawalan dan prosedur pengendalian yang menyeluruh bagi elemen-elemen yang berikut:

(a) **Data atau Maklumat:** Koleksi fakta dalam bentuk kertas atau mesej elektronik yang digunakan untuk mencapai misi dan objektif jabatan. Contohnya, sistem dokumentasi, prosedur **operasi**, rekod, pangkalan data, dan arkib maklumat.

(b) **Salinan Digital (Softcopy):** Fakta dalam bentuk digital yang digunakan untuk mencapai misi dan objektif jabatan, termasuk rekod digital, pangkalan data, dan maklumat arkib.

(c) **Salinan Bercetak (Hardcopy):** Fakta dalam bentuk bercetak, seperti sistem dokumentasi, prosedur operasi, rekod, dan fail-fail.

(d) **Perkakasan (Hardware):** Semua aset fizikal yang menyokong pemprosesan dan penyimpanan maklumat, termasuk komputer, pelayan, dan peralatan komunikasi.

(e) **Perisian (Software):** Program dan dokumentasi yang berkaitan dengan sistem komputer, termasuk perisian aplikasi dan sistem operasi yang digunakan untuk pemprosesan maklumat di jabatan.

(f) **Infrastruktur ICT:** Set lengkap perkakasan, perisian, rangkaian, dan kemudahan yang menyokong pemprosesan, penyimpanan, dan penghantaran maklumat dalam organisasi. Ini termasuk LAN, WAN, sistem

kad akses, perkhidmatan pengcomputeran awan, serta kemudahan sokongan seperti bekalan elektrik dan sistem pencegah kebakaran.

(g) **Manusia:** Individu yang memiliki pengetahuan dan kemahiran untuk melaksanakan tugas harian bagi mencapai misi dan objektif jabatan. Mereka ialah aset berdasarkan tugas dan peranan yang mereka laksanakan.

(h) **Premis:** Semua kemudahan dan premis yang menempatkan aset-aset di atas, yang mesti dilindungi dengan ketat untuk mencegah kebocoran rahsia atau kelemahan perlindungan, yang akan dianggap sebagai pelanggaran keselamatan.

1.4.5. Polisi ini memastikan bahawa setiap aspek di atas diberikan perlindungan yang sewajarnya, meminimumkan risiko dan mengekalkan integriti operasi Jabatan Digital Negara.

1.5. PERNYATAAN POLISI KESELAMATAN SIBER

JDN komited untuk mengekalkan persekitaran yang selamat bagi aset maklumat dengan melaksanakan kawalan keselamatan siber yang berkesan selaras dengan standard dan rangka kerja keselamatan siber yang ditetapkan oleh jabatan ini.

1.6. PRINSIP KESELAMATAN DATA DAN MAKLUMAT

Prinsip-prinsip keselamatan data dan maklumat yang menjadi asas kepada Polisi Keselamatan Siber Jabatan Digital Negara dan perlu dipatuhi ialah seperti yang berikut:

1.6.1. Capaian Atas Dasar Perlu Mengetahui

Capaian terhadap penggunaan aset maklumat hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar perlu mengetahui sahaja. Ini bermakna capaian hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk capaian ialah berdasarkan klasifikasi dan peringkat dokumen seperti mana yang dinyatakan dalam para 53 Arahan Keselamatan (Semakan dan Pindaan 2017).

1.6.2. Hak Capaian Minimum

Pengguna hendaklah diberikan hak capaian minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak capaian pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak askes atau capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu berdasarkan peranan tersebut. Hak capaian perlu dikaji mengikut sela masa yang ditetapkan atau **sekurang-kurangnya sekali dalam tempoh setahun**.

1.6.3. Akauntabiliti

Semua pengguna bertanggungjawab ke atas semua tindakannya terhadap aset maklumat JDN. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap perlindungan keselamatan yang diperlukan oleh sesuatu sumber/aset maklumat. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem ICT tersebut boleh dipertanggungjawabkan atas tindakan mereka. Akauntabiliti atau tanggungjawab pengguna termasuklah:

(a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

(b) Memeriksa dan menentukan data dan maklumat adalah tepat dan lengkap dari masa ke masa;

(c) Menentukan maklumat sedia untuk digunakan;

(d) Menjaga kerahsiaan kata laluan;

(e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

(f) Memberi perhatian kepada maklumat terperingkat terutama semasa diwujudkan, diproses, disimpan, dihantar, sedang digunakan, diedarkan, disimpan, diselenggara, dihapuskan dan dimusnahkan serta diarkibkan; dan

(g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

1.6.4. Pengasingan Tugas

Bagi mengekalkan prinsip semak-dan-imbang (check and balance), jabatan hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset maklumat daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian, keselamatan dan aplikasi mengikut kesesuaian.

1.6.5. Prinsip Kepercayaan Sifar (Zero Trust)

Prinsip ini menegaskan bahawa tiada pengguna, peranti, atau rangkaian harus dipercayai secara automatik, sama ada berada dalam atau luar perimeter rangkaian. Setiap permintaan untuk mencapai data atau maklumat mesti melalui proses pengesahan yang teliti sebelum hak capaian diberikan. Prinsip ini menyatakan bahawa:

(a) semua trafik rangkaian (dalaman dan luaran) dianggap sebagai tidak dipercayai;

(b) Capaian kepada sumber diberikan berdasarkan set kriteria yang komprehensif dan dinamik, termasuk identiti pengguna, keadaan dan kesihatan peranti, lokasi capaian, serta faktor konteks lain yang relevan. Capaian kepada sumber hanya akan diluluskan selepas pengesahan menyeluruh terhadap identiti pengguna dan status peranti, tanpa mengira lokasi fizikal, untuk memastikan keselamatan yang maksimum; dan

(c) menekankan prinsip keistimewaan yang paling sedikit, capaian kepada sumber yang perlu dicapai akan diberikan berdasarkan keperluan, apabila diperlukan dan hanya untuk tempoh masa yang ditetapkan.

1.6.6. Pengauditan

Pengauditan ialah tindakan untuk menilai, memeriksa, serta menganalisis aktiviti, rekod dan proses yang telah dilaksanakan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Tujuannya adalah untuk memastikan bahawa aktiviti tersebut mematuhi peraturan, piawaian, dan

prosedur yang ditetapkan serta untuk mengidentifikasi sebarang isu, ketidakpatuhan, atau potensi risiko. Oleh itu, aset maklumat seperti komputer, pelayan, penghala rangkaian (network router), tembok keselamatan (firewall) dan peralatan rangkaian **hendaklah dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit**.

1.6.7. Pematuhan

Polisi Keselamatan Siber Jabatan Digital Negara hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan maklumat.

1.6.8. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kesediaan 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.

1.6.9. Saling Bergantungan

Setiap prinsip keselamatan adalah saling melengkapi dan bergantung antara satu dengan lain untuk membentuk sistem keselamatan yang menyeluruh dan berkesan. Prinsip-prinsip ini tidak boleh dilaksanakan secara terpisah, tetapi mesti diintegrasikan dan diselaraskan untuk mencapai keselamatan yang maksimum.

1.7. CIRI KESELAMATAN DATA DAN MAKLUMAT

Ciri-ciri keselamatan data dan maklumat yang perlu diberi perhatian oleh semua pihak merangkumi perkara yang berikut:

1.7.1. Kerahsiaan

Kerahsiaan merujuk kepada perlindungan maklumat daripada capaian yang tidak dibenarkan. Ciri keselamatan ini bertujuan untuk memastikan bahawa hanya pihak yang sah dan berhak sahaja boleh mencapai maklumat tertentu. Perkara ini penting untuk melindungi maklumat sensitif seperti data peribadi, maklumat kewangan, dan rahsia perniagaan. Langkah-langkah yang biasa

digunakan untuk mengekalkan kerahsiaan termasuk penyulitan maklumat, kawalan capaian yang ketat, dan penggunaan kata laluan yang kukuh.

1.7.2. Integriti

Integriti merujuk kepada ketepatan, kelengkapan, dan kesempurnaan maklumat. Ciri ini diperlukan bagi memastikan bahawa data dan maklumat tidak diubah suai atau dirosakkan oleh pihak yang tidak dibenarkan. Sebarang perubahan terhadap data atau maklumat hendaklah dilakukan hanya oleh pihak yang mempunyai kebenaran yang sah dan perubahan tersebut haruslah direkodkan dengan jelas untuk tujuan audit. Integriti adalah sangat penting dalam memastikan bahawa keputusan yang dibuat berdasarkan maklumat tersebut adalah tepat dan boleh dipercayai.

1.7.3. Tidak Boleh Disangkal

Ciri ini memastikan bahawa pihak yang bertanggungjawab terhadap penciptaan, penghantaran, atau penerimaan data atau maklumat tidak boleh menafikan penglibatan mereka. Dalam transaksi digital, ciri ini dapat membuktikan penglibatan pihak tertentu dalam transaksi secara digital yang dilaksanakan. Contoh langkah keselamatan yang digunakan untuk memastikan tiada penafian termasuk penggunaan tandatangan digital dan rekod transaksi yang terperinci dalam jejak audit.

1.7.4. Kesahihan

Kesahihan merujuk kepada pengesahan bahawa data dan maklumat adalah sah dan berasal daripada sumber yang dipercayai. Ciri kesahihan memastikan bahawa maklumat yang diterima atau dihantar tidak dimanipulasi oleh pihak ketiga. Langkah-langkah seperti penggunaan sijil digital dan protokol pengesahan membantu memastikan bahawa maklumat yang diterima adalah sahih dan boleh dipercayai.

1.7.5. Ketersediaan

Ketersediaan memastikan bahawa maklumat boleh dicapai oleh pihak yang yang dibenarkan pada bila-bila masa yang diperlukan. Ketersediaan adalah penting untuk memastikan kelancaran operasi harian dan membuat keputusan yang tepat pada masanya. Untuk mengekalkan ketersediaan, semua pihak yang terlibat hendaklah melaksanakan langkah-langkah seperti menyediaan dan pengaktifan pelan pemulihan bencana, menyediakan sistem sandaran,

dan melaksanakan pengurusan risiko yang menyeluruh untuk mengurangkan gangguan terhadap capaian data dan maklumat.

1.8. IMPLIKASI KETIDAKPATUHAN POLISI KESELAMATAN SIBER

Ketidakpatuhan terhadap Polisi Keselamatan Siber Jabatan Digital Negara boleh mengakibatkan pelbagai implikasi yang serius, termasuk tetapi tidak terhad kepada:

(a) **Risiko Keselamatan:** Ketidakpatuhan boleh menyebabkan pendedahan data sensitif, pencerobohan sistem, atau gangguan operasi, yang boleh mengakibatkan kehilangan maklumat penting atau kerosakan kepada infrastruktur digital.

(b) **Gangguan Operasi:** Ketidakpatuhan boleh menyebabkan gangguan kepada operasi harian Jabatan, termasuk masa henti sistem, kehilangan data, dan kerosakan peralatan, yang boleh memberi kesan langsung kepada penyampaian perkhidmatan.

(c) **Kesan Undang-Undang**: Kegagalan mematuhi polisi ini boleh menyebabkan tindakan undang-undang diambil terhadap pihak yang terlibat, termasuk denda atau tindakan undang-undang lain yang berkaitan dengan pelanggaran peraturan dan undang-undang keselamatan siber.

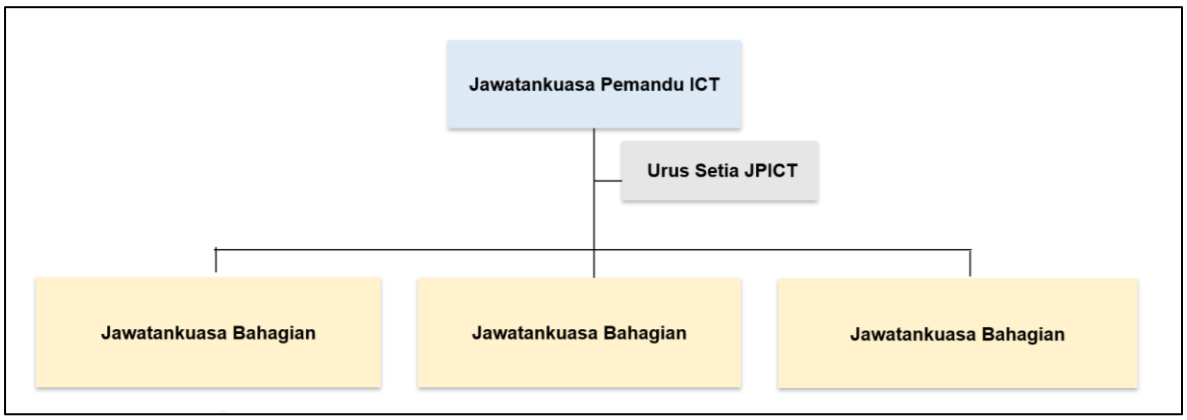
(d) **Kerugian Kewangan:** Ketidakpatuhan boleh membawa kepada kerugian kewangan yang besar, sama ada melalui denda, kos pemulihan, atau kehilangan kepercayaan pelanggan dan pihak berkepentingan yang boleh menjejaskan kedudukan kewangan Jabatan.

(e) **Kerosakan Reputasi:** Insiden keselamatan siber yang disebabkan oleh ketidakpatuhan boleh merosakkan reputasi JDN, mengurangkan kepercayaan pihak berkepentingan dan masyarakat umum terhadap keupayaan JDN dalam menguruskan keselamatan maklumat.

(f) **Tindakan Disiplin:** Warga JDN yang didapati tidak mematuhi PKS ini boleh dikenakan tindakan disiplin, termasuk amaran, penggantungan, atau penamatan perkhidmatan, bergantung kepada tahap pelanggaran yang dilakukan.

2. TADBIR URUS

2.1. Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS JDN, sebuah struktur tadbir urus yang mantap telah diwujudkan dengan penubuhan Jawatankuasa Pemandu ICT (JPICT) JDN. Jawatankuasa ini memainkan peranan penting dalam memantau, menyelaras, dan memastikan kawalan keselamatan ICT yang dilaksanakan mencapai objektif yang ditetapkan. Struktur Tadbir Urus JPICT JDN seperti **Rajah 1** di bawah:



Rajah 1: Struktur Tadbir Urus Jawatankuasa Pemandu ICT Jabatan Digital Negara

2.2. Jawatankuasa ini diperngerusikan oleh Pengarah Bahagian Perundingan Digital dan keahlian JPICT JDN terdiri daripada pihak pengurusan kanan JDN, Pegawai Keselamatan ICT (Information and Communication Security Officer, ICTSO) serta timbalan pengarah kewangan JDN. Urus setia bagi JPICT ialah bahagian yang melaksanakan fungsi pengurusan maklumat jabatan. Perincian struktur tadbir urus JPICT ialah seperti yang berikut:

(a) Pengerusi**:** Pengarah Bahagian Perundingan Digital

(b) Ahli**:**
- (i) Ketua Perunding ICT Bahagian Perundingan Digital;
- (ii) Semua Pengarah Bahagian;
- (iii) Pegawai Keselamatan ICT Jabatan Digital Negara; dan
- (iv) Timbalan Pengarah Kewangan.

2.3. Bidang rujukan JPICT JDN ialah seperti yang berikut:

(a) Menetapkan arah tuju dan strategi untuk pembangunan dan pelaksanaan ICT agensi;

(b) Merancang, mengenal pasti dan mencadangkan sumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan hala tuju/strategi ICT agensi;

(c) Merancang dan menyelaras pembangunan dan pelaksanaan program/projek ICT agensi;

(d) Menyelaras dan menyeragamkan pembangunan ICT agensi agar selari dengan pelan strategik organisasi dan pelan strategik ICT agensi;

(e) Meluluskan projek ICT agensi berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan;

(f) Mengikuti dan memantau perkembangan program ICT agensi serta memahami keperluan, masalah dan isu yang dihadapi dalam pembangunan dan pelaksanaan ICT;

(g) Merancang dan menentukan langkah-langkah keselamatan ICT;

(h) Mengemukakan perolehan ICT yang telah diluluskan di peringkat JPICT Agensi kepada JPICT Kementerian untuk kelulusan; dan

(i) Mengemukakan laporan kemajuan projek ICT yang telah diluluskan oleh Jawtankuasa Teknikal ICT Sektor Awam (JTISA) kepada JPICT Kementerian Digital mengikut tempoh yang telah ditetapkan.

3. PENGURUSAN RISIKO

3.1. Semua pihak yang terlibat dalam pengurusan data dan maklumat di JDN harus mengambil kira risiko yang wujud terhadap aset maklumat akibat kelemahan (vulnerability) dan ancaman yang semakin berkembang dalam persekitaran digital masa kini. Oleh itu, langkah-langkah proaktif dan bersesuaian perlu diambil untuk menilai tahap risiko terhadap aset maklumat, bagi memastikan pendekatan dan keputusan yang paling berkesan dapat dikenal pasti dalam menyediakan perlindungan dan kawalan yang optimum.

3.2. Penilaian risiko ini bertujuan untuk mengenal pasti dan mengambil tindakan susulan serta langkah-langkah mitigasi yang bersesuaian bagi mengurangkan atau mengawal risiko keselamatan maklumat berdasarkan penemuan daripada penilaian risiko tersebut. Penilaian risiko keselamatan maklumat hendaklah dilaksanakan

secara berkala **sekurang-kurangnya sekali setahun** atau sekiranya terdapat perubahan aset maklumat.

3.3. Laporan Penilaian Risiko dan Pelan Penguraian Risiko harus dijadikan agenda tetap dalam mesyuarat bahagian atau mesyuarat yang setara dengannya, serta perlu dibincangkan oleh bahagian masing-masing dan dimaklumkan kepada Mesyuarat Jawatankuasa Pemandu ICT JDN.

3.4. Penilaian risiko keselamatan maklumat harus dilaksanakan ke atas semua aset maklumat JDN, termasuk aset fizikal, aplikasi, perisian, pelayan, rangkaian, serta proses dan prosedur yang berkaitan. Selain itu, penilaian risiko ini juga perlu dijalankan di premis yang menempatkan aset maklumat seperti pusat data, bilik media storan, kemudahan utiliti, dan sistem-sistem sokongan lain.

3.5. Pelaksanaan pengurusan risiko hendaklah selaras dengan Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024. Dalam menghadapi potensi risiko, semua pihak yang terlibat perlu mengenal pasti tindakan yang sewajarnya, termasuk:

(a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

(b) Menerima atau bersedia menghadapi risiko yang mungkin berlaku selagi risiko tersebut tidak menjejaskan penyampaian perkhidmatan JDN;

(c) Mengelakkan atau mencegah risiko dengan mengambil langkah-langkah yang dapat mengelakkan atau mencegah terjadinya risiko; dan

(d) Memindahkan risiko kepada pihak ketiga seperti pembekal, pakar runding, atau pihak berkepentingan lain.

4. PELAN PENGURUSAN KESELAMATAN MAKLUMAT

4.1. Setiap projek di JDN hendaklah menyediakan Pelan Pengurusan Keselamatan Maklumat. Pelan ini mengandungi maklumat terperinci yang menyatakan keutamaan aplikasi, kawalan capaian dan keperluan-keperluan khusus yang lain.

4.2. Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), PKS JDN dan surat pekeliling/arahan yang sedang berkuat kuasa untuk menangani isu keselamatan operasi semasa projek dilaksanakan.

4.3. Pelan ini hendaklah dibangunkan dengan berpandukan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), PKS JDN dan surat pekeliling/arahan yang sedang berkuat kuasa untuk menangani isu keselamatan operasi semasa projek dilaksanakan.

4.4. Pelan ini hendaklah mengenal pasti perlindungan data-dalam-penggunaan, data-dalampergerakan, data-dalam-simpanan dan menghalang ketirisan data. Pelan Pengurusan Keselamatan Maklumat hendaklah mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen yang berikut:

(a) Peranti Pengkomputeran Peribadi

Peranti Pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, telefon pintar, tablet dan peranti storan.

(b) Peranti Rangkaian

(i) Peranti rangkaian merujuk kepada peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem seperti *switch*, penghala rangkaian, tembok keselamatan, peranti Virtual Private Network (VPN) dan kabel.

(ii) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi datadalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(c) Aplikasi

(i) Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi dan sistem operasi.

(ii) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi datadalam penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(d) Pelayan

(i) Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.

(ii) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi datadalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

(e) Persekitaran Fizikal

(i) Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan aset ICT.

(ii) Cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat hendaklah dirujuk Pejabat Ketua Pegawai Keselamatan Kerajaan untuk mendapatkan nasihat serta hendaklah selaras dengan perundangan dan arahan yang sedang berkuat kuasa.

(iii) Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip kawalan *defend-in-depth*.

(iv) Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi datadalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

5. KAWALAN ORGANISASI

Terdapat 37 kawalan organisasi yang terpakai dalam perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di JDN. Perincian kawalan organisasi seperti di bawah.

5.1. POLISI KESELAMATAN SIBER

ID	KETERANGAN	PERANAN
5.1.1	**Pelaksanaan Polisi** Satu set polisi untuk keselamatan siber perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan Jabatan kepada pengguna, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di JDN. Pelaksanaan polisi hendaklah dilaksanakan oleh Ketua Pengarah dengan disokong oleh JPICT yang terdiri daripada Pengarah Bahagian, Pegawai Keselamatan ICT (ICTSO) dan ahli-ahli yang dilantik oleh Ketua Jabatan.	Ketua Pengarah
5.1.2	**Pengesahan Polisi** Dasar itu perlu diperakui diperingkat pengurusan tertinggi JDN.	Ketua Pengarah JPICT
5.1.3	**Penguatkuasaan Polisi** PKS JDN mestilah dipatuhi oleh semua warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di JDN. Sebarang ketidakpatuhan kepada dasar ini boleh mengakibatkan tindakan tatatertib termasuk sebarang remedi/tindakan undang-undang lain di bawah akta/peraturan/undang-undang semasa yang berkuat kuasa.	Warga JDN Pihak yang terlibat dalam perkhidmatan ICT di JDN

ID	KETERANGAN	PERANAN
5.1.4	**Penyebaran Polisi** Program kesedaran tentang PKS JDN ini hendaklah diatur dan diselaraskan.	ICTSO Pengarah Bahagian
5.1.5	**Pengecualian Polisi** Keselamatan ICT jabatan terpakai kepada warga JDN dan pembekal serta semua pihak yang terlibat dalam pembekalan perkhidatan ICT di JDN dan tiada pengecualian diberikan.	Warga JDN Pihak yang terlibat dalam perkhidmatan ICT di JDN
5.1.6	**Penyelenggaraan Polisi** Penyelenggaraan dan kajian semula dasar hendaklah dilaksanakan mengikut diperlukan. Semua dokumen atau rekod hendaklah diwujudkan dan diselenggara untuk menyediakan bukti pematuhan kepada keperluan dan operasi berkesan pengurusan keselamatan maklumat. Semua dokumen dan rekod hendaklah dilindungi dan dikawal mengikut undang-undang/arahan/peraturan/garis panduan semasa yang berkuat kuasa.	CDO JPICT ICTSO
5.1.7	**Kajian Semula/Semakan Polisi** Polisi ini perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan, dan polisi Kerajaan bagi memastikan kesesuaian, kecukupan dan keberkesanannya berterusan. Berikut ialah prosedur yang berkaitan dengan kajian semula Polisi Keselamatan Siber:	CDO JPICT ICTSO

ID	KETERANGAN	PERANAN
	(a) Memastikan penguatkuasaan pelaksanaan PKS JDN ini; (b) Mengenal pasti dan menentukan perubahan yang diperlukan; (c) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan kepada JPICT/Ketua Jabatan bagi tujuan kelulusan; (d) Memaklumkan pindaan yang telah diluluskan oleh JPICT kepada warga JDN serta semua pihak yang terlibat dalam perkhidmatan ICT di JDN**;** dan (e) Polisi ini hendaklah dikaji semula setiap **LIMA TAHUN SEKALI** atau mengikut keperluan semasa sekiranya perubahan tersebut kurang dari tempoh kajian semula bagi memastikan dokumen sentiasa relevan.	

5.2. PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.2.1	**Peranan dan Tanggungjawab Keselamatan Maklumat** Semua peranan dan tanggungjawab keselamatan maklumat hendaklah ditakrifkan dan diperuntukkan mengikut keperluan. Peranan dan tanggungjawab Keselamatan Maklumat ialah seperti yang berikut: (a) **Ketua Pengarah** **Tanggungjawab:**	Ketua Pengarah CDO ICTSO Pengarah Bahagian/Ketua Unit di JDN Pentadbir Sistem Pemilik Sistem Pentadbir Rangkaian JPICT CSIRT Pengguna Sistem Pengguna Aset Warga JDN

ID	KETERANGAN	PERANAN
	(i) Memastikan penguatkuasaan PKS ini; (ii) Memastikan warga, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di JDN memahami dan mematuhi peruntukan-peruntukan di bawah PKS JDN ini; (iii) Memastikan semua keperluan seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi; (iv) Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan dalam PKS JDN ni; dan (v) Melantik CDO dan ICTSO. (b) **Ketua Pegawai Digital (CDO)** CDO yang dilantik mestilah mempunyai pengalaman dalam bidang teknikal serta transformasi digital yang kukuh. **Tanggungjawab:** (i) Memastikan polisi keselamatan siber selaras dengan matlamat digital jabatan dan mengurus risiko keselamatan dalam transformasi digital; (ii) Membantu membangunkan, mengemas kini, dan melaksanakan PKS JDN yang relevan dengan teknologi digital terkini;	

ID	KETERANGAN	PERANAN
	(iii) Mendidik dan meningkatkan kesedaran keselamatan siber dalam kalangan warga JDN serta memastikan penglibatan semua pihak berkepentingan; (iv) Memastikan inisiatif digital mematuhi peraturan keselamatan siber dan mengawasi tadbir urus yang berkesan; (v) Memastikan semua inisiatif digital dilaksanakan dengan selamat; (vi) Menilai dan mengintegrasikan keselamatan dalam penggunaan teknologi digital baru tanpa menjejaskan inovasi; (vii) Membantu dalam persediaan dan tindak balas terhadap insiden keselamatan siber, serta menilai keberkesanan selepas insiden berlaku; dan (viii) Memastikan perlindungan data dan privasi dalam semua inisiatif digital, mematuhi peraturan yang berkaitan. (c) **Pegawai Keselamatan ICT (ICTSO)** ICTSO yang dilantik mestilah mempunyai pengalaman dalam bidang teknikal, keselamatan rangkaian, pengurusan insiden dan perlindungan data yang kukuh. **Tanggungjawab:** (i) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan PKS JDN ini;	

ID	KETERANGAN	PERANAN
	(ii) Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat yang berkuat kuasa; (iii) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (iv) Menyelaras insiden keselamatan siber JDN dan seterusnya membantu dalam penyiasatan atau pemulihan; (v) Melaporkan Insiden Keselamatan Siber kepada Ketua Jabatan bagi insiden yang memerlukan pengaktifan Pengurusan Kesinambungan Perkhidmatan (PKP); (vi) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau Insiden Keselamatan Siber; (vii) Memperakukan langkah-langkah baik pulih dengan segera; (viii) Memastikan pematuhan PKS JDN ini oleh pengguna, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di JDN;	

ID	KETERANGAN	PERANAN
	(ix) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; (x) Menyedia dan merangka latihan dan program kesedaran keselamatan siber; (xi) Merancangkan dan melaksanakan program kesedaran kepada semua warga JDN untuk memahami keperluan standard, garis panduan dan prosedur keselamatan di bawah PKS ini; (xii) Mewujudkan program-program bagi meningkatkan pengetahuan dan pembudayaan mengenai teknologi dan mekanisme kawalan maklumat dan aset ICT, ancaman-ancaman siber dan peranan dan tanggungjawab pengguna dalam mengendalikan kemudahan ICT; dan (xiii) Mengurus keseluruhan program keselamatan ICT. (d) **Pengarah Bahagian/Ketua Unit** **Tanggungjawab:** (i) Melaksanakan keperluan polisi ini dalam operasi semasa pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu, pembelian atau peningkatan perisian dan sistem komputer serta perolehan teknologi dan perkhidmatan komunikasi baharu;	

ID	KETERANGAN	PERANAN
	(ii) Memastikan pembekal dan pihak ketiga yang berkaitan dengan perkhidmatan ICT di JDN yang dibekalkan menjalani tapisan keselamatan dan membuat perakuan pematuhan PKS JDN ini; dan (iii) Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan dan pelan pengurusan keselamatan maklumat Kerajaan yang sedang berkuat kuasa. (e) **Pentadbir Sistem** Pentadbir Sistem terdiri daripada: (i) Pentadbir rangkaian dan keselamatan; (ii) Pentadbir pangkalan data; (iii) Pentadbir portal atau sistem aplikasi; (iv) Pentadbir e-mel; (v) Pentadbir media sosial JDN; dan (vi) Pegawai Aset ICT. **Tanggungjawab:** (i) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai personel yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (ii) Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat seperti mana yang telah ditetapkan di dalam PKS JDN ini; (iii) Memantau aktiviti capaian sistem;	

ID	KETERANGAN	PERANAN
	(iv) Mengenal pasti dan melaporkan aktiviti-aktiviti tidak normal seperti pencerobohan atau pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; (v) Menganalisis dan menyimpan rekod jejak audit; (vi) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan (vii) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada personel dalam keadaan yang baik. (f) **Pemilik Sistem** Sesuatu sistem mempunyai pemilik sistem yang mempunyai kepentingan terhadap sistem yang dibangunkan. Pemilik Sistem terdiri daripada pegawai yang terlibat dengan sistem yang dibangunkan. Peranan dan tanggungjawab Pemilik Sistem ialah seperti berikut: (i) Pelaksanaan promosi sistem kepada pengguna sasaran; (ii) Penentuan pengguna dan kategori atau tahap capaian pengguna sistem; (iii) Pengurusan senarai pengguna yang terlibat dengan latihan pengguna; (iv) Penguatkuasaan penggunaan sistem dalam kalangan pengguna;	

ID	KETERANGAN	PERANAN
	(v) Pemantauan pelaksanaan dan keberkesanan sistem secara berterusan; dan (vi) Pemakluman sebarang masalah dan keperluan peningkatan sistem kepada Pembangun Sistem. Pemilik Sistem hendaklah melantik seorang pegawai sebagai Pentadbir Sistem untuk tujuan penyenggaraan/penambahbaikan sistem yang dikendalikan tersebut. (g) **Pentadbir Rangkaian** Pentadbir Rangkaian ICT ialah Pegawai ICT yang dilantik oleh JDN bagi mentadbir rangkaian yang digunakan oleh Warga JDN bagi urusan rasmi Kerajaan. Peranan dan tanggungjawab Pentadbir Rangkaian ICT ialah seperti yang berikut: i. Mentadbir akaun pengguna; ii. Merangka, melaksana dan menguatkuasakan polisi keselamatan siber seperti perlindungan dan perkongsian data; iii. Merancang dan melaksana polisi ancaman keselamatan, memantau keadaan rangkaian dan mengawal penggunaan sumber; iv. Pemantauan aktiviti capaian harian pengguna; v. Menyediakan laporan mengenai aktiviti capaian secara berkala; vi. Menyelia dan membuat proses sandaran pelayan; dan	

ID	KETERANGAN	PERANAN
	vii. Memberi bantuan dalam menyelesaikan masalah-masalah berkaitan rangkaian yang dilaporkan oleh pengguna. (h) **Jawatankuasa Pemandu ICT (JPICT)** Peranan dan tanggungjawab JPICT seperti yang terkandung dalam **Surat Pekeliling Am Bil 3 Tahun 2015: Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Agensi Sektor Awam** bagi pengurusan keselamatan siber. (i) **Cyber Security Incident Response Team (CSIRT)** Keanggotaan CSIRT ialah seperti yang berikut: a. Pengarah: Ketua Jabatan b. Pengurus: ICTSO c. Ahli: Pegawai Teknologi Maklumat yang dilantik Peranan dan tanggungjawab CSIRT ialah seperti yang berikut: a. Mengendalikan insiden berdasarkan garis panduan/prosedur yang telah ditetapkan; b. Memantau, mengesan insiden, menerima dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber;	

ID	KETERANGAN	PERANAN
	c. Merekodkan dan menjalankan siasatan awal terhadap insiden yang diterima; d. Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan; e. Menyebarkan makluman/amaran berkaitan insiden kepada warga JDN; dan i. Memastikan fail log disimpan **sekurang-kurangnya enam bulan** di tempat yang selamat. **(i) Pengguna Sistem atau Aset Maklumat** i. Membaca, memahami dan mematuhi PKS JDN ini; ii. Mengetahui dan memahami implikasi keselamatan siber kesan daripada tindakannya; iii. Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat rasmi terperingkat; iv. Mematuhi prinsip-prinsip keselamatan yang dinyatakan dalam PKS ini dan menjaga kerahsiaan maklumat Kerajaan; v. Melaksanakan langkah-langkah perlindungan seperti yang berikut:	

ID	KETERANGAN	PERANAN
	a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan maklumat tersebut sentiasa tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan maktumat; e. Mematuhi dasar, piawaian dan garis panduan keselamatan siber yang ditetapkan; f. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan kawalan keselamatan siber dari diketahui umum. vi. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT JDN dengan segera; vii. Menghadiri program-program kesedaran mengenai keselamatan siber; dan viii. Bersetuju dengan terma dan syarat yang terkandung dalam PKS JDN ini.	

5.3. PENGASINGAN TUGAS

ID	KETERANGAN	PERANAN
5.3.1	**Pengasingan Tugas** Pengasingan tugas dan bidang tanggungjawab dilaksanakan bagi mengurangkan peluang pengubahsuaian data dan maklumat tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) 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 dimanipulasi; (b) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai produksi; (c) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; (d) Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya; dan (e) Semakan dan pemantauan hak capaian perkakasan, perisian dan sistem hendaklah dilaksanakan secara berkala.	Pengarah Bahagian/Ketua Unit

5.4. TANGGUNGJAWAB PENGURUSAN

ID	KETERANGAN	PERANAN
5.4.1	**Tanggungjawab Pengurusan** Pelaksanaan PKS JDN ini akan dijalankan oleh Ketua Pengarah dengan disokong oleh JPICT yang terdiri daripada Pengarah Bahagian, Pegawai Keselamatan ICT (ICTSO), Ketua Jabatan/Ketua Bahagian dan ahli-ahli yang dilantik oleh Ketua Pengarah. PKS JDN mestilah dipatuhi oleh semua warga JDN, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di JDN. Pengarah bahagian atau ketua unit di JDN hendaklah memastikan semua warga JDN, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan supaya mengamalkan keselamatan maklumat mematuhi PKS JDN dan prosedur yang ditetapkan.	Pengarah Bahagian Ketua Unit

5.5. HUBUNGAN DENGAN PIHAK BERKUASA

ID	KETERANGAN	PERANAN
5.5.1.	**Hubungan dengan Pihak Berkuasa** Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab;	BKP ICTSO CSIRT Pemilik Sistem

ID	KETERANGAN	PERANAN
	(b) mewujudkan dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi dan Multimedia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba, penyedia perkhidmatan telekomunikasi dan perkhidmatan bekalan air; dan (c) insiden keselamatan maklumat harus dilaporkan tepat pada masanya kepada CSIRT, Ketua Jabatan dan pihak berkaitan seperti Agensi Keselamatan Siber (NACSA) selaras dengan Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022 bagi mengurangkan impak insiden.	

5.6. HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS

ID	KETERANGAN	PERANAN
5.6.1	**Hubungan dengan Kumpulan Berkepentingan yang Khusus** Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau forum yang berkaitan bagi:	CSIRT Pemilik Perkhidmatan

ID	KETERANGAN	PERANAN
	(a) Meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; (b) Memastikan pemahaman tentang persekitaran keselamatan maklumat adalah terkini; (c) Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; (d) Mendapat capaian kepada nasihat pakar keselamatan maklumat; (e) Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan (f) Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	

5.7. PERISIKAN ANCAMAN

ID	KETERANGAN	PERANAN
5.7.1	**Perisikan Ancaman** Maklumat berkaitan ancaman keselamatan maklumat yang berpotensi atau memberi ancaman kepada fungsi JDN perlu diperoleh dan dianalisis untuk menghasilkan maklumat perisikan berkaitan ancaman. Maklumat tentang ancaman sedia ada atau baharu akan dikumpul dan dianalisis untuk memudahkan tindakan dan mengelakkan ancaman atau mengurangkan impak kepada aset maklumat yang terlibat.	CSIRT Pemilik Sistem

ID	KETERANGAN	PERANAN
	Pemilik aset maklumat hendaklah melaksanakan tindakan berikut bagi meningkatkan tahap kawalan keselamatan aset: (a) Mengenal pasti ancaman dengan melaksanakan penilaian risiko terhadap aset maklumat; (b) Mengenal pasti dan melaksanakan kawalan keselamatan yang berkaitan. Kawalan keselamatan tersebut juga dijadikan sebagai satu daripada keperluan dalam kitar hayat pembangunan sistem dan penyediaan infrastruktur ICT; dan (c) Menjadikan ancaman sebagai satu daripada ancaman yang perlu diambil kira dalam pelaksanaan ujian keselamatan sistem dan infrastruktur ICT.	

5.8. KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK

ID	KETERANGAN	PERANAN
5.8.1	**Keselamatan Maklumat dalam Pengurusan Projek** Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek tanpa mengira kerumitan, saiz, tempoh serta bidang. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek; (b) Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;	Pengarah Projek Pengurus Projek

ID	KETERANGAN	PERANAN
	(c) Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan; (d) Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber; (e) Penyediaan spesifikasi perolehan hendaklah memasukkan keperluan **pasukan projek pihak pembekal mempunyai pensijilan keselamatan maklumat**; (f) Kesesuaian pertimbangan dan aktiviti keselamatan maklumat hendaklah disusuli pada peringkat yang telah ditetapkan seperti jawatankuasa teknikal projek atau jawatankuasa pemandu projek; dan (g) Peranan dan tanggungjawab keselamatan maklumat projek hendaklah ditakrifkan dan ditentukan.	
5.8.2	**Analisis dan Spesifikasi Keperluan Keselamatan Maklumat (Information Security Requirements Analysis and Specifications)** Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada serta mematuhi perkara-perkara berikut: (a) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk pengkonsepan perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian,	Pentadbir Sistem ICT

ID	KETERANGAN	PERANAN
	penerimaan, pemasangan, penyelenggaraan dan pelupusan; (b) Semua sistem yang dibangunkan sama ada secara dalaman atau khidmat luar hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan PKS JDN; (c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan (d) Ujian keselamatan hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data. Penilaian Tahap Keselamatan (Security Posture Assessment, SPA) hendaklah dilaksanakan sebelum sistem digunakan dalam persekitaran produksi. Pelaksanaan hendaklah mematuhi Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024.	

5.9. INVENTORI MAKLUMAT DAN ASET LAIN YANG BERKAITAN

ID	KETERANGAN	PERANAN
5.9.1	**Inventori Aset** Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT jabatan. Tanggungjawab yang perlu dipatuhi merangkumi perkara yang berikut: (a) JDN hendaklah mengenal pasti Pegawai Penerima Aset setiap di setiap bahagian/unit	Pegawai Aset Pegawai Penerima Aset

ID	KETERANGAN	PERANAN
	di JDN untuk mengurus penerimaan aset-aset ICT; (b) Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumentasikan, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa; (c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pegawai yang dibenarkan sahaja; (d) Memastikan inventori maklumat dan aset lain yang berkaitan hendaklah tepat, terkini, dan konsisten; dan (e) Pegawai Aset hendaklah mengesahkan penempatan aset ICT.	
5.9.2	**Pemilikan Aset** Aset hak milik JDN hendaklah diselenggara mengikut jadual penyelenggaraan yang ditetapkan serta mematuhi Pekeliling Perbendaharaan Malaysia Am 1.1 Pengurusan Aset Kerajaan.Tanggungjawab yang perlu dipatuhi oleh pemilik aset merangkumi perkara yang berikut: (a) Memastikan aset didaftarkan dalam senarai aset mengikut klasifikasi aset dan diserahkan kepada pemilik aset; (b) Memastikan semua jenis aset dipelihara dan diselenggara dengan baik; (c) Kenal pasti dan kaji semula capaian ke atas aset penting secara berkala berdasarkan	Pegawai Aset Pemilik Aset

ID	KETERANGAN	PERANAN
	kepada polisi kawalan capaian yang telah ditetapkan; (d) Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapuskan atau dilupuskan; (e) Aset bukan hakmilik jabatan hendaklah didaftarkan dan diurus mengikut prosedur/arahan-arahan atau polisi *Bring Your Own Device* (BYOD) yang sedang berkuat kuasa.	
5.9.3	**Pengelasan Maklumat Aset** Memastikan setiap maklumat dalam aset ICT dikelaskan mengikut klasifikasi dan peringkat keselamatan dokumen selaras dengan Akta Rahsia Rasmi 1972.	Pegawai Aset Pegawai Pengkelas

5.10. PENGGUNAAN MAKLUMAT YANG BOLEH DITERIMA DAN ASET LAIN YANG BERKAITAN

ID	KETERANGAN	PERANAN
5.10.1	**Penggunaan Aset yang Dibenarkan** Memastikan penggunaan aset untuk tujuan rasmi dan mengikut fungsi sebenar yang telah ditetapkan oleh JDN.	Pemilik Aset
5.10.2	**Pengendalian Aset** Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah perlu mengambil kira langkah-langkah keselamatan berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;	Pegawai Aset Pemilik Aset

ID	KETERANGAN	PERANAN
	(b) Memeriksa dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan; (g) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum; (h) Sekatan capaian yang menyokong keperluan perlindungan untuk setiap peringkat pengelasan; dan (i) Penyelenggaraan rekod pengguna yang dibenarkan bagi maklumat dan aset lain yang berkaitan.	

5.11. PEMULANGAN ASET

ID	KETERANGAN	PERANAN
5.11.1	**Pemulangan Aset** Pengguna perlu mengembalikan aset termasuk semua aset lain yang berkaitan	Pegawai Aset Pemilik Aset

ID	KETERANGAN	PERANAN
	seperti peranti storan mudah alih, peranti pengguna fizikal yang disambungkan kepada sistem rangkaian, salinan maklumat fizikal dan perkakasan pengesahan (contohnya kunci mekanikal, token fizikal dan kad pintar) untuk sistem maklumat, tapak serta arkib fizikal mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan atau penamatan perkhidmatan atau kontrak. Pemulangan aset yang mengandungi maklumat rasmi kerajaan hendaklah disanitasi mengikut Surat Pekeliling Am Bilangan 4 Tahun 2022 Garis Panduan Sanitasi Media Elektronik Dalam Perkhidmatan Awam.	

5.12. PENGKELASAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.12.1	**Pengelasan Maklumat** Data dan maklumat perlu dikelas oleh Pegawai Pengelas mengikut keperluan keselamatan maklumat yang telah ditetapkan dalam Arahan Keselamatan berdasarkan keperluan perlindungan keselamatan makluamt tersebut. Pengkelasan maklumat terdiri daripada aktiviti penentuan klasifikasi maklumat serta penentuan peringkat keselamatan maklumat. Klasifikasi maklumat terdiri daripada maklumat rahsia rasmi dan maklumat rasmi manakala peringkat keselamatan maklumat terdiri daripada rahsia besar, rahsia, sulit terhad, data terkawal/sensitif dan terbuka.	Ketua Jabatan Pegawai Rekod Pegawai Pengelas Pegawai Pengurus Rekod Pemilik Rekod Pengguna Rekod

ID	KETERANGAN	PERANAN
	Perkara di bawah hendaklah dilaksanakan oleh semua pihak yang terlibat dalam pengkelasan maklumat: (a) Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik oleh JDN dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan dalam Arahan Keselamatan; (b) Mematuhi piawaian, prosedur, tatacara dan garis panduan keselamatan dan pengendalian maklumat atau dokumen yang sedang berkuat kuasa; (c) Memberi perhatian semasa mengendalikan maklumat rahsia terperingkat; (d) Memastikan tiada pendedahan maklumat kepada pihak yang tidak dibenarkan; (e) Pengelasan maklumat hendaklah berpandukan kepada Akta Rahsia Rasmi 1972, Arahan Keselamatan, Pekeliling Am Bilangan 2 Tahun 1987 Garis Panduan Mengenai Pengelasan Fail. (f) Pengurusan maklumat dan rekod hendaklah berpandukan kepada Akta Arkib Negara 2003, Pekeliling Am Bilangan 5 Tahun 2007 - Pengurusan Rekod Awam, Arahan Keselamatan dan standard berkaitan pengurusan rekod serta pekeliling, arahan, dasar dan garis panduan yang dikeluarkan oleh Pejabat Pegawai Keselamatan Kerajaan dan Arkib Negara Malaysia; dan (g) Memastikan kesemua fail fizikal dan digital maklumat disimpan mengikut	

ID	KETERANGAN	PERANAN
	keperluan perlindungan keselamatan yang ditetapkan oleh pihak Kerajaan.	

5.13. PELABELAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.13.1	**Pelabelan Maklumat** Peringkat keselamatan maklumat hendaklah ditandakan mengikut klasifikasi dokumen yang kekal terjilid dengan huruf cerai atau huruf besar tidak kurang daripada 7mm di sebelah luar kulit hadapan dan belakang, di muka tajuk, di muka surat pertama dan penghabisan. Peringkat keselamatan maklumat hendaklah diletakkan pada penjuru sebelah atas kiri dan sebelah bawah kanan dan setiap muka surat yang mengandungi perkara bertulis, bercetak atau bercap. Semua maklumat yang ditandakan sebagai terperingkat hendaklah mematuhi Arahan Keselamatan: Keselamatan Rahsia Rasmi dan semua maklumat yang diklasifikasikan terperingkat dalam format elektronik hendaklah mematuhi Arahan Keselamatan: Keselamatan Rahsia Rasmi Dalam Persekitaran Teknologi Maklumat dan Komunikasi (ICT).	Pegawai Rekod Pegawai Pengelas Pegawai Pengurus Rekod Pemilik Rekod Pengguna Rekod

5.14. PEMINDAHAN DATA DAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.14.1	**Polisi dan Prosedur Pemindahan Data dan Maklumat** Memastikan keselamatan perpindahan/pertukaran data, maklumat dan perisian antara dan pihak luar terjamin dengan merujuk pada Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Nasional. Pihak luar ialah pihak yang menggunakan atau pihak yang membekalkan data, maklumat atau perisian. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; (b) Terma pemindahan data, maklumat dan perisian antara jabatan dengan pihak luar hendaklah dimasukkan dalam perjanjian pertukaran data, maklumat atau perisian; (c) Media yang mengandungi data, maklumat dan perisian perlu dilindungi; dan (d) Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya.	Pemilik Sistem Pentadbir Sistem Pemilik Maklumat

ID	KETERANGAN	PERANAN
5.14.2	**Perjanjian Mengenai Pemindahan Data dan Maklumat** Semua pihak yang terlibat perlu mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara jabatan dengan pihak luar serta mematuhi Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Nasional. Perkara yang perlu dipertimbangkan ialah: (a) Pengarah Bahagian hendaklah mengawal penghantaran dan penerimaan data atau maklumat jabatan; (b) Mewujudkan prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat jabatan; (c) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan (d) Mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.	Pengarah Bahagian Pemilik Sistem Pemilik Maklumat Warga JDN
5.14.3	**Pesanan Elektronik** Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan, peraturan dan garis panduan yang sedang berkuat kuasa bagi pengurusan pesanan elektronik.	Warga JDN

5.15. KAWALAN CAPAIAN

ID	KETERANGAN	PERANAN
5.15.1	**Polisi Kawalan Capaian** Dasar khusus mengenai kawalan capaian hendaklah ditakrifkan dengan mengambil kira keperluan ini dan harus dimaklumkan kepada semua pihak yang berkepentingan yang berkaitan. Pemilik maklumat dan Pemilik Aset hendaklah menentukan tahap perlindungan keselamatan maklumat dan kawalan capaian yang diperlukan bagi mencapai maklumat tersebut. Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Kawalan capaian ditetapkan berdasar prinsip perlu tahu iatu capaian diberikan atas dasar keperluan untuk melaksanakan tugas dan keperluan untuk digunakan iaitu hanya diberikan capaian kepada infrastruktur teknologi maklumat di mana terdapat keperluan yang jelas. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Kawalan capaian perlu disemak, dikemas kini dan disahkan **sekurang-kurangnya sekali dalam tempoh setahun** atau mengikut keperluan sekiranya terdapat perubahan serta menyokong peraturan kawalan capaian pengguna sedia ada. Perkara-perkara yang perlu dipertimbangkan dalam menentukan kawalan capaian ialah seperti yang berikut:	Pentadbir Sistem Pentadbir Aset

ID	KETERANGAN	PERANAN
	(a) Menentukan entiti mana yang memerlukan jenis capaian kepada maklumat dan aset lain yang berkaitan; (b) Keperluan keselamatan aplikasi ditentukan dan diselaraskan dengan keperluan capaian entiti; (c) Hak capaian dan dasar klasifikasi maklumat sistem dan rangkaian; (d) Capaian fizikal, yang perlu disokong oleh kawalan kemasukan fizikal yang sesuai; (e) Penyebaran maklumat dan kebenaran capaian perlu mematuhi prinsip-prinsip keselamatan yang ditetapkan (dan mengikut pengkelasan maklumat; (f) Sekatan kepada capaian istimewa hendaklah dihadkan dan diurus (pengurusan hak capaian); (g) Pengasingan tugas, fungsi kawalan capaian (contohnya permintaan capaian, kebenaran capaian, pentadbiran capaian); (h) Patuh undang-undang, peraturan berkaitan yang berkuat kuasa semasa dan sebarang kewajipan kontrak berkaitan pengehadan capaian kepada data atau perkhidmatan; (i) Kebenaran rasmi untuk permintaan capaian; (j) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (k) Pengasingan peranan kawalan capaian;	

ID	KETERANGAN	PERANAN
	(l) Kebenaran rasmi permohonan capaian; (m)Keperluan semakan hak capaian berkala; (n) Pembatalan hak capaian; (o) Pengarkiban semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; (p) Hak capaian istimewa; dan (q) Pengelogan aktiviti yang dilaksanakan.	
5.15.2	**Capaian kepada Rangkaian dan Perkhidmatan Rangkaian** Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari JDN. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang aset maklumat dan perkakasan ICT yang bersesuaian antara rangkaian JDN, rangkaian jabatan lain dan rangkaian awam; (b) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Sistem Pentadbir Aset Pentadbir Rangkaian

ID	KETERANGAN	PERANAN
5.15.3	**Kawalan Capaian** Kawalan capaian adalah untuk mengurus, mengawasi, dan meningkatkan capaian maklumat dan aset maklumat dengan selamat. Ini merangkumi pelbagai aspek operasi dan pengurusan untuk memastikan mencapai matlamat, sasaran, dan hasil yang diinginkan dengan kawalan seperti yang berikut: (a) Mematuhi undang-undang, peraturan, dan polisi yang berkaitan dengan keselamatan maklumat; (b) Memastikan bahawa dasar, prosedur, dan amalan keselamatan maklumat diikuti dan dilaksanakan dengan betul; (c) Mengenal pasti, menilai, dan menguruskan risiko keselamatan maklumat yang berkaitan dengan operasi dan capaian maklumat organisasi; (d) Memastikan keselamatan maklumat dan data dalam organisasi dengan mematuhi amalan keselamatan maklumat yang sesuai; (e) Meningkatkan kesedaran dan kepahaman kakitangan tentang peningkatan capaian dan amalan keselamatan dalam organisasi; dan (f) Memantau dan menilai prestasi keselamatan capaian berterusan untuk mengenal pasti peningkatan dan kesan tindakan yang diperlukan.	

ID	KETERANGAN	PERANAN
5.15.4	**Keperluan Pemindahan Maklumat** Menghadkan capaian pembekal, kakitangan dan pengguna pihak luar kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat. Memastikan dokumen perjanjian diwujudkan antara JDN dengan pihak ketiga bagi pemindahan maklumat melibatkan pihak ketiga.	

5.16. PENGURUSAN IDENTITI

ID	KETERANGAN	PERANAN
5.16.1	**Pendaftaran dan Pembatalan Pengguna** Setiap pengguna bertanggungjawab ke atas aset maklumat yang diamanahkan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun pengguna hanya diwujudkan setelah mendapat pengesahan daripada Pentadbir Aset Maklumat atau Pentadbir Sistem dan pengguna telah membuat perakuan pematuhan PKS JDN melalui Surat Akuan Pematuhan Polisi Keselamatan Siber seperti **LAMPIRAN A** atau melalui Sistem Akuan Pematuhan Polisi Keselamatan Siber (SPeKS). (b) Akaun yang diperuntukkan kepada pengguna sahaja boleh digunakan;	Warga JDN Pemilik Aset Pentadbir Aset Pentadbir Sistem BKP

ID	KETERANGAN	PERANAN
	(c) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (d) Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada Pemilik Sistem atau Pemilik Aset terlebih dahulu; (e) Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada penyelia/Ketua Jabatan terlebih dahulu; (f) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan penyelia/Ketua Jabatan; (g) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan semua pengguna tertakluk kepada peraturan yang ditetapkan. (h) Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (i) Penggunaan akaun milik individu lain **DILARANG**; (j) Akaun pengguna tidak boleh dikongsi; (k) Akaun pengguna boleh dibekukan atau ditamatkan apabila menerima arahan daripada Bahagian Pengurusan Sumber Manusia atas sebab-sebab yang berikut: (i) Pengguna bercuti panjang dalam tempoh waktu melebihi tiga bulan; (ii) Bertukar bidang tugas kerja;	

ID	KETERANGAN	PERANAN
	(iii) Bertukar ke jabatan lain; (iv) Bersara; (v) Bagi menjalankan siasatan; atau (vi) Ditamatkan perkhidmatan. Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Semua capaian ini perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	
5.16.2	**Pengurusan Identiti** Pengurusan akaun pengguna bagi capaian ke sistem atau aset maklumat bermula daripada penciptaan rekod pengguna baharu sehingga penamatan profil apabila pengguna telah meletakkan jawatan, bersara atau meninggal dunia dalam perkhidmatan. Pendaftaran, pengemaskinian dan penamatan akaun pengguna dilaksanakan mengikut prosedur yang ditetapkan. Proses pengurusan akaun pengguna harus memastikan bahawa: (a) Identiti yang diberikan khusus hanya dikaitkan dengan seorang sahaja untuk membolehkan orang itu bertanggungjawab atas tindakan yang dilakukan dengan identiti khusus ini; (b) Identiti yang diberikan kepada entiti selain manusia seperti mesin atau sistem tertakluk kepada kelulusan yang	Warga JDN Pemilik Aset Pentadbir Aset Pentadbir Sistem

ID	KETERANGAN	PERANAN
	diasingkan dengan sewajarnya dan pengawasan berterusan. (c) Akaun pengguna perlu dinyahaktifkan dengan segera tepat pada masanya jika tidak lagi diperlukan; (d) Dalam domain tertentu, identiti tunggal dihubungkan dengan entiti tunggal; dan (e) rekod penggunaan dan pengurusan identiti pengguna dan maklumat pengesahan hendaklah disimpan.	

5.17. MAKLUMAT PENGESAHAN IDENTITI

ID	KETERANGAN	PERANAN
5.17.1	**Pengurusan Maklumat Pengesahan Identiti Pengguna** Peruntukan maklumat pengesahan identiti pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan. Peruntukan dan proses pengurusan hendaklah memastikan bahawa: (c) Kata laluan atau nombor pengenalan diri (Personel Identification Number, PIN) yang dijana secara automatik semasa proses pendaftaran sebagai maklumat pengesahan rahsia sementara adalah tidak dapat tidak dapat diteka dan unik untuk setiap individu, dan pengguna dikehendaki menukarnya selepas penggunaan pertama; (d) Prosedur yang telah diwujudkan untuk mengesahkan identiti pengguna sebelum	Pengguna Sistem Pengguna Aset Maklumat Pentadbir Sistem Pentadbir Aset

ID	KETERANGAN	PERANAN
	memberikan maklumat pengesahan baharu, gantian atau sementara; (e) Maklumat pengesahan, termasuk maklumat pengesahan sementara, dihantar kepada pengguna secara selamat (contohnya, melalui saluran yang disahkan dan dilindungi), dan penggunaan mesej e-mel elektronik yang tidak dilindungi (clear text) untuk tujuan ini hendaklah dielakkan; (f) Pengguna mengakui penerimaan maklumat pengesahan identiti pengguna; (g) Maklumat pengesahan tetapan asal (default) seperti yang ditetapkan atau diberikan oleh sistem diubah dengan segera selepas pemasangan sistem, perkakasan atau perisian; (h) Rekod peristiwa penting mengenai peruntukan dan pengurusan maklumat pengesahan identiti pengguna disimpan dan kerahsiaannya dijamin, serta kaedah penyimpanan rekod disetujui (contohnya dengan menggunakan alat penyimpanan kata laluan yang diluluskan).	
5.17.2	**Penggunaan Maklumat Pengesahan Rahsia** Peranan dan tanggungjawab pengguna ialah seperti yang berikut: (a) Membaca, memahami dan mematuhi PKS JDN; (b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya;	Pengguna Sistem Pengguna Aset Maklumat Pentadbir Sistem Pentadbir Aset

ID	KETERANGAN	PERANAN
	(c) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat JDN; (d) Melaksanakan langkah-langkah perlindungan seperti yang 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) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (vii) Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum. (viii) Maklumat pengesahan terjejas atau telah dikompromi hendaklah ditubah serta-merta apabila pemberitahuan atau petunjuk sebarang kompromi diterima;	

ID	KETERANGAN	PERANAN
	(ix) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT JDN dengan segera; dan (x) Menghadiri program-program kesedaran mengenai keselamatan siber. Pengguna perlu mengikut amalan keselamatan yang baik dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti pengguna.	
5.17.3	**Sistem Pengurusan Kata Laluan** Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JDN seperti yang berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi bagi sistem yang menyokong pelbagai faktor pengesahan identiti. Bagi sistem yang tidak menyokong pelbagai faktor pengesahan identiti, kata laluan hendaklah ditukar sekurang-kurangnya dalam tempoh **tiga bulan sekali**; (c) Panjang kata laluan mestilah sekurang kurangnya **12 AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (alphanumeric) KECUALI bagi perkakasan dan perisian yang	Pengguna Sistem Pengguna Aset Maklumat Pentadbir Sistem Pentadbir Aset

ID	KETERANGAN	PERANAN
	mempunyai pengurusan kata laluan yang terhad; (d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun; (e) Kata laluan kunci skrin (lock screen) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; (g) Kuatkuasakan pertukaran kata laluan semasa atau selepas login kali pertama atau selepas reset kata laluan; (h) kata laluan tidak berdasarkan perkataan kamus atau gabungannya; (i) kata laluan yang sama tidak digunakan merentas perkhidmatan dan sistem yang berbeza; (j) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna (k) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum **TIGA (3) KALI** sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; dan (l) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	

5.18. HAK CAPAIAN

ID	KETERANGAN	PERANAN
5.18.1	**Peruntukan Capaian Pengguna** Hak capaian kepada maklumat dan aset maklumat yang berkaitan hendaklah diperuntukkan, disemak, diubah suai dan dikeluarkan mengikut dasar/peraturan atau garis panduan kawalan capaian yang berkuat kuasa. Pentadbir Sistem ICT perlu mewujudkan prosedur pendaftaran dan penamatan pengguna sistem masing-masing. Proses peruntukan capaian pengguna dan pembatalan hak capaian fizikal dan logik yang diberikan kepada entiti yang telah disahkan identitinya hendaklah termasuk: (a) Hak Capaian yang berkaitan dengan setiap sistem atau produk yang perlu diberikan hendaklah dikenal pasti dan dibenarkan. (b) Hak capaian maklumat dan aset maklumat mesti dihadkan berdasarkan keperluan untuk mengetahui dan prinsip-prinsip keselamatan yang ditetapkan; (c) Individu yang bukan warga JDN **TIDAK boleh diberikan** ID pengguna atau diberi keistimewaan untuk menggunakan atau mencapaian aset (komputer, maklumat atau sistem komunikasi) melainkan setelah mendapat kebenaran JDN; (d) Kebenaran rasmi mestilah telah ditandatangani oleh wakil yang diberi kuasa di pihak ketiga sebelum capaian	Pentadbir Aset Pentadbir Sistem Pengurus Projek Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT JDN

ID	KETERANGAN	PERANAN
	diberikan kepada mana-mana pihak ketiga; (e) Hak capaian hendaklah ditamatkan apabila entiti/individu tidak lagi perlu mengcapaian maklumat dan aset maklumat yang berkaitan tepat pada masanya; (f) Hak capaian sementara untuk tempoh masa terhad boleh dipertimbangkan bila diperlukan dan hendaklah dibatalkan pada tarikh tamat tempoh; (g) Tahap capaian yang diberikan hendaklah mengikut dasar kawalan capaian yang ditetapkan, peranan dan konsisten dengan keperluan keselamatan maklumat lain seperti pengasingan tugas; (h) Hak capaian pengguna hendaklah diubah suai selari dengan peranan atau pekerjaan; (i) Hak capaian diaktifkan hanya selepas kebenaran diperoleh; dan (j) Rekod hak capaian logik dan fizikal pengguna hendaklah disimpan.	
5.18.2	**Kajian Semula Hak Capaian Pengguna** Pentadbir aset hendaklah menyemak hak capaian pengguna secara berkala sekurang-kurangnya **sekali dalam tempoh setahun**. Pentadbir Sistem perlu mewujudkan rekod pendaftaran dan penamatan pengguna sistem masing-masing sebagai rujukan semakan ke atas hak capaian pengguna secara berkala.	Pentadbir Aset Pentadbir Sistem Pengurus Projek Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT JDN

ID	KETERANGAN	PERANAN
	Semakan ke atas hak capaian fizikal dan logik harus mempertimbangkan perkara berikut: (a) Hak capaian pengguna selepas sebarang perubahan dalam organisasi (contohnya pertukaran pekerjaan, kenaikan pangkat, penurunan pangkat) atau penamatan perkhidmatan/pekerjaan; dan (b) Kebenaran untuk hak capaian istimewa.	
5.18.3	**Pembatalan atau Pelarasan Hak Capaian** Hak capaian pengguna kepada maklumat dan aset yang berkaitan hendaklah disemak dan diselaraskan atau ditamatkan sebelum sebarang perubahan atau penamatan pekerjaan berdasarkan penilaian faktor risiko seperti yang berikut: (a) Sama ada penamatan atau perubahan penempatan oleh pengguna atau pengurusan dan sebab penamatan; (b) Tanggungjawab semasa pengguna; dan (c) Nilai semasa aset yang boleh dicapai oleh pengguna. Hak capaian kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan peranan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam organisasi.	Pentadbir Aset Pentadbir Sistem Pengurus Projek Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT JDN

ID	KETERANGAN	PERANAN
5.18.4	**Tanggungjawab Pengguna** Memastikan pengguna sistem atau aset maklumat bertanggungjawab melindungi maklumat pengesahan identiti mereka.	Warga JDN Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT JDN

5.19. KESELAMATAN MAKLUMAT DALAM HUBUNGAN DENGAN PEMBEKAL

ID	KETERANGAN	PERANAN
5.19.1	**Polisi Keselamatan Siber untuk Hubungan dengan Pembekal** Keperluan keselamatan maklumat hendaklah ditakrifkan, dilaksanakan, dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset maklumat. Perkara yang perlu dipertimbangkan ialah seperti yang berikut: (a) Mengenal pasti dan mendokumentasi maklumat pembekal; (b) Menyediakan prosedur pengurusan pembekal termasuk kaedah penilaian mutu perkhidmatan; (c) Memilih pembekal mengikut klasifikasi maklumat dan perkhidmatan yang disediakan oleh pembekal selaras dengan dasar dan peraturan yang berkuat kuasa; (d) Mengawal dan memantau capaian pembekal; (e) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam dokumen perjanjian; (f) Jenis-jenis obligasi kepada pembekal;	Pengurus Projek Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT di JDN ICTSO BKP

ID	KETERANGAN	PERANAN
	(g) Pelan kontigensi (contingency plan) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; (h) Melaksanakan program kesedaran terhadap PKS JDN kepada pembekal; (i) Menandatangani Surat Akuan Pembida Berjaya dan Surat Setuju Terima; dan (j) Membuat akuan pematuhan PKS JDN; (k) Pembekal perlu mematuhi arahan keselamatan yang sedang berkuat kuasa; dan (l) Mengenal pasti dan melaksanakan proses dan prosedur bagi mengurus risiko yang berkaitan dengan penggunaan produk dan perkhidmatan pembekal termasuk penamatan penggunaan produk dan perkhidmatan pembekal. Pemilik perkhidmatan atau projek hendaklah memastikan proses penamatan pembekal yang selamat, termasuk: (a) membatalkan peruntukan hak capaian; (b) pengendalian maklumat; (c) menentukan pemilikan harta intelek yang dibangunkan semasa penjanjian dilaksanakan; (d) mudah alih maklumat sekiranya berlaku pertukaran pembekal atau penyumberan; (e) pengurusan rekod; (f) pemulangan aset;	

ID	KETERANGAN	PERANAN
	(g) pelupusan selamat maklumat dan aset lain yang berkaitan; dan (h) keperluan kerahsiaan berterusan.	

5.20. MENANGANI KESELAMATAN DALAM PERJANJIAN DENGAN PEMBEKAL

ID	KETERANGAN	PERANAN
5.20.1	**Menangani Keselamatan Dalam Perjanjian Pembekal** Semua keperluan keselamatan maklumat yang berkaitan hendaklah ditakrifkan, disediakan dan dipersetujui dengan setiap pembekal yang boleh mencapai, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak jabatan selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Syarikat pembekal hendaklah mempunyai pendaftaran sah dengan Kementerian	Pengurus Projek Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT di JDN BKP

ID	KETERANGAN	PERANAN
	Kewangan Malaysia dalam kod bidang yang berkaitan; (b) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; (c) Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada jabatan berkaitan; (d) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; (e) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal; (f) Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: (i) Badan penilai pihak ketiga adalah bebas dan berintegriti; (ii) Badan penilai pihak ketiga adalah kompeten; (iii) Kriteria penilaian; (iv) Parameter pengujian; dan (v) Andaian yang dibuat berkaitan dengan skop penilaian.	

ID	KETERANGAN	PERANAN
	(g) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mencapai, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan jabatan bagi perjanjian kerahsiaan atau ketakdedahan maklumat dan Perakuan Akta Rahsia Rasmi 1972 (Akta 88); dan (h) Pembekal hendaklah mematuhi pengkelasan maklumat yang telah ditetapkan oleh JDN.	

5.21. MENGURUS KESELAMATAN MAKLUMAT DALAM RANGKAIAN BEKALAN ICT

ID	KETERANGAN	PERANAN
5.21.1	**Rantaian Bekalan Teknologi Maklumat dan Komunikasi** 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 ialah seperti yang berikut: (a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; (b) Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan atau pembekalan produk; dan	Pengurus Projek

ID	KETERANGAN	PERANAN
	(c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	

5.22. MEMANTAU, MENYEMAK DAN MENGURUS PERUBAHAN PERKHIDMATAN PEMBEKAL

ID	KETERANGAN	PERANAN
5.22.1	**Memantau dan Mengkaji Semula Perkhidmatan Pembekal** JDN hendaklah sentiasa memantau, mengkaji semula, mengaudit perkhidmatan pembekal secara berkala dan mengurus perubahan dalam amalan risiko keselamatan maklumat pembekal dan penyampaian perkhidmatan. Perkara-perkara yang perlu diambil kira ialah seperti yang berikut: (a) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; (b) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan (c) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	Pengurus Projek
5.22.2	**Menguruskan Perubahan Kepada Perkhidmatan Pembekal (Managing Changes to Supplier Services)** Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar	

ID	KETERANGAN	PERANAN
	keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diurus dengan mengambil kira kepentingan maklumat, sistem dan perkhidmatan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira ialah seperti yang berikut: (a) Perubahan dalam perjanjian dengan pembekal; (b) Perubahan yang dilakukan oleh jabatan bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan (c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor.	

5.23. KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN PENGKOMPUTERAN AWAN

ID	KETERANGAN	PERANAN
5.23.1	**Keselamatan maklumat bagi penggunaan perkhidmatan pengkomputeran awan** Pengurusan perkhidmatan awan ini melibatkan pelbagai aspek teknikal dan pentadbiran untuk memastikan perkhidmatan awan digunakan secara berkesan, selamat, dan sesuai dengan keperluan organisasi. Perkara berikut perlu dipatuhi oleh semua pihak yang terlibat: (a) Memastikan kepatuhan terhadap keperluan perundangan, peraturan, garis	Pentadbir Perkhidmatan Pengkomputeran Awan Pentadbir Sistem

ID	KETERANGAN	PERANAN
	panduan dan perjanjian kontrak yang berkaitan antaranya: (i) PK 2.6: Perolehan Perkhidmatan Pengkomputeran Awan (Cloud) Sektor Awam; (ii) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam; (iii) Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan dalam Perkhidmatan Awam. (b) Pengurusan perkhidmatan yang disediakan oleh pembekal yang dilantik oleh pihak Kerajaan; (c) Menentukan/mentakrifkan dan memaklumkan cara/kaedah berkaitan pengurusan risiko bagi perkhidmatan pengkomputeran awan; (d) Memastikan keperluan keselamatan maklumat yang berkaitan dengan penggunaan perkhidmatan pengkomputeran awan dilaksanakan; dan (e) Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	

5.24. PERANCANGAN DAN PENYEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.24.1	**Tanggungjawab dan Prosedur** Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat dengan mentakrif, mewujudkan dan menyampaikan proses pengurusan insiden keselamatan maklumat, peranan dan tanggungjawab. Pengurusan insiden JDN ialah berdasarkan prosedur pengurusan pengendalian insiden keselamatan maklumat yang sedang berkuat kuasa. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Melaksanakan program kesedaran mengenai prosedur pengendalian inside keselamatan dan hebahan kepada warga JDN; dan (b) Memastikan personel yang mengurus insiden mempunyai tahap kompetensi yang diperlukan.	Pemilik Perkhidmatan Pemilik Sistem CSIRT ICTSO
5.24.2	**Perancangan dan Penyediaan Pengurusan Insiden Keselamatan Maklumat** Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kerentanan kelemahan keselamatan.	

5.25. PENILAIAN DAN KEPUTUSAN MENGENAI KEJADIAN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.25.1	**Penilaian dan Keputusan Mengenai Peristiwa Keselamatan Maklumat** Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat berdasarkan pekeliling dan prosedur pengurusan insiden keselamatan maklumat yang sedang berkuat kuasa.	Pemilik Perkhidmatan Pemilik Sistem CSIRT ICTSO

5.26. TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.26.1	**Tindak Balas Terhadap Insiden Keselamatan** Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat ialah berdasarkan Prosedur Operasi Standard Pengurusan dan Pengendalian Insiden Keselamatan Siber JDN, PKP JDN, Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022 serta prosedur operasi standard pengurusan dan pengendalian insiden mengikut perkhidmatan yang disediakan di JDN. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut: (a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku;	ICTSO CSIRT Pemilik Sistem Pemilk Perkhidmatan Pemilik Maklumat

ID	KETERANGAN	PERANAN
	(b) Menjalankan forensik digital sekiranya perlu; (c) Menghubungi pihak yang berkenaan dengan secepat mungkin; (d) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; (e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (f) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; (g) Menyediakan tindakan pemulihan segera; dan (h) Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu. (i) sebaik sahaja insiden itu berjaya ditangani, ia hendaklah ditutup secara rasmi dan direkodkani; (j) melaksanakan analisis pasca-kejadian untuk mengenal pasti punca asal dan didokumentasikan mengikut prosedur yang ditakrifkan; dan (k) mengenal pasti dan mengurus kelemahan dan kelemahan keselamatan maklumat termasuk yang berkaitan dengan kawalan yang telah menyebabkan, menyumbang kepada atau gagal untuk menghalang kejadian itu.	

5.27. PENGAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.27.1	**Pembelajaran Daripada Insiden Keselamatan Maklumat** Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya. Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah maklumat yang diperoleh daripada penilaian insiden keselamatan maklumat hendaklah digunakan untuk: (a) mempertingkat pelan pengurusan insiden termasuk senario dan prosedur insiden; (b) mengenal pasti insiden berulang atau serius dan puncanya untuk mengemas kini penilaian risiko keselamatan maklumat organisasi dan menentukan serta melaksanakan kawalan tambahan yang diperlukan untuk mengurangkan kemungkinan atau akibat kejadian serupa pada masa hadapan. Mekanisme untuk membolehkan itu termasuk mengumpul, mengukur dan memantau maklumat tentang jenis insiden, kekerapan insiden serta kos yang terlibat; dan (c) meningkatkan kesedaran dan latihan pengguna dengan memberikan contoh tentang perkara yang boleh berlaku, cara bertindak balas terhadap insiden tersebut dan cara mengelak pada masa hadapan.	CSIRT Pemilik Sistem Pemilk Perkhidmatan Pemilik Maklumat

5.28. PENGUMPULAN BAHAN BUKTI

ID	KETERANGAN	PERANAN
5.28.1	**Pengumpulan Bahan Bukti** JDN hendaklah menentukan mewujudkan dan melaksanakan prosedur untuk mengenal pasti maklumat atau rekod, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	CSIRT Pemilik Sistem Pemilk Perkhidmatan Pemilik Maklumat

5.29. KESELAMATAN MAKLUMAT SEMASA GANGGUAN

ID	KETERANGAN	PERANAN
5.29.1	**Keselamatan Maklumat Semasa Gangguan** Keselamatan maklumat semasa gangguan merujuk kepada langkah-langkah dan prosedur yang diambil untuk melindungi dan mengekalkan keselamatan maklumat, data, dan sistem ICT semasa terjadi gangguan, bencana atau insiden yang boleh mengancam integriti dan ketersediaan maklumat. Gangguan ini termasuk pelbagai situasi seperti serangan siber, bencana alam, kebakaran, banjir, kecurian, atau insiden teknikal yang tidak diingini. Aspek penting berkaitan dengan keselamatan maklumat semasa gangguan yang perlu diberi perhatian ialah seperti yang berikut: (a) Pembangunan dan pelaksanaan Pelan Perancangan Kesinambungan Perkhidmatan (Business Continuity Planning) untuk memastikan penyampaian perkhidmatan JDN berfungsi dengan minimum gangguan ketika terjadi insiden;	Ketua Jabatan CDO ICTSO CSIRT Pasukan PKP

ID	KETERANGAN	PERANAN
	(b) Pemulihan Bencana melibatkan pelan dan tindakan untuk memulihkan sistem maklumat dan data setelah bencana atau insiden; (c) Perlindungan Data melibatkan salinan data secara berkala, pengekalan data yang baik, dan pelaksanaan tindakan keselamatan yang sesuai untuk melindungi data terperingkat; (d) Pencegahan Serangan Siber (Cybersecurity Measures) melibatkan tindakan untuk mencegah serangan siber dan melindungi data dari pada ancaman siber; (e) Pemulihan Sistem Pantas (Quick System Recovery) untuk mengurangkan masa henti ketika terjadi gangguan; (f) Kawalan fizikal ke pusat data dan peralatan komputer terhad kepada individu yang sah untuk mencegah capaian yang tidak dibenarkan; (g) Pemulihan data memastikan keupayaan untuk memulihkan data yang hilang atau terjejas dalam insiden; (h) Kesedaran keselamatan (Security Awareness) untuk mengurangkan ancaman dalaman dan mencegah insiden yang disebabkan oleh kesalahan manusia; (i) Pelan Komunikasi Krisis (Crisis Communication Plan) yang jelas untuk mengurus krisis dan insiden dengan pantas.	

ID	KETERANGAN	PERANAN
	Keselamatan maklumat semasa gangguan ialah aspek penting dalam perancangan keselamatan dan keselamatan data, yang memastikan organisasi mampu menjaga integriti, kerahsiaan, dan ketersediaan maklumat penting dalam pelbagai situasi yang mengancam.	

5.30. KESEDIAAN ICT BAGI KESINAMBUNGAN PERKHIDMATAN

ID	KETERANGAN	PERANAN
5.30.1	**Kesinambungan Keselamatan Maklumat** Kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan bisnes jabatan.	BKP ICTSO
5.30.2	**Perancangan Kesinambungan Keselamatan Maklumat** JDN hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, JDN perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi Jabatan. JDN juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan ialah seperti yang berikut:	Ketua Jabatan Jawatankuasa Pemandu PKP Pasukan PKP

ID	KETERANGAN	PERANAN
	(a) Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) JDN; (b) Menetapkan polisi PKP; (c) Mengenal pasti perkhidmatan kritikal; (d) Melaksanakan Kajian Impak Perkhidmatan (Business Impact Analysis, BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal; (e) Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT. (f) Melaksanakan program kesedaran dan latihan pasukan PKP dan warga JDN; (g) Melaksanakan simulasi pelan kesinambungan perkhidmatan; dan (h) Melaksanakan penyelenggaraan ke atas pelan kesinambungan perkhidmatan.	
5.30.3	**Pelaksanaan Kesinambungan Keselamatan Maklumat** JDN hendaklah menyediakan, mendokumenkan mendokumentasikan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan ialah seperti yang berikut:	Ketua Jabatan Jawatankuasa Pemandu PKP Pasukan PKP

ID	KETERANGAN	PERANAN
	(a) Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal jabatan yang telah dikenal pasti berdasarkan kepada Pelan Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak Balas Kecemasan dan Pelan Pemulihan Bencana; (b) Melaksanakan pasca nilai (post-mortem) dan mengemas kini pelan-pelan yang terlibat; (c) Mengemas kini pelan-pelan yang terlibat jika berlaku perubahan kepada fungsi kritikal jabatan; (d) Mengemas kini struktur tadbir urus PKP JDN sekiranya berlaku pertukaran keahlian pasukan; dan (e) Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.	
5.30.4	**Menentusahkan, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat** JDN hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan **sekurang-kurangnya setahun sekali** bagi memastikannya terpakai dan berkesan semasa situasi kecemasan. Kesediaan ICT hendaklah dirancang, dilaksanakan, diselenggara dan diuji berdasarkan objektif kesinambungan	Ketua Jabatan Jawatankuasa Pemandu PKP Pasukan PKP

ID	KETERANGAN	PERANAN
	perniagaan dan keperluan kesinambungan ICT. JDN hendaklah memastikan bahawa: (a) struktur pasukan PKP yang mencukupi disediakan untuk menyediakan, mengurangkan dan bertindak balas terhadap gangguan; (b) Pelan PKP dan pelan-pelan lain yang terlibat termasuk tindak balas dan prosedur pemulihan hendaklah dinilai dan diuji melalui pelaksanaan simulasi **sekurang-kurangnya setahun sekali** serta diluluskan oleh pihak pengurusan; (c) Pelan PKP hendaklah mengandungi perkara seperti yang berikut: (i) spesifikasi prestasi dan kapasiti untuk memenuhi keperluan dan objektif kesinambungan perniagaan seperti yang dinyatakan dalam BIA; (ii) Objektif Masa Pemulihan (RTO) bagi setiap perkhidmatan ICT mengikut keutamaan pemulihan dan prosedur untuk memulihkan komponen tersebut; dan (iii) Objektif Titik Pemulihan (RPO) bagi setiap perkhidmatan ICT mengikut keutamaan pemulihan dan prosedur untuk memulihkan komponen tersebut.	

5.31. KEPERLUAN PERUNDANGAN DAN KONTRAK

ID	KETERANGAN	PERANAN
5.31.1	**Pematuhan Terhadap Keperluan Perundangan dan Kontrak** Meningkat dan memantapkan tahap keselamatan siber bagi mengelakkan pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	Warga JDN Pembekal Pihak yang terlibat dalam perkhidmatan ICT JDN
5.31.2	**Pengenalpastian Keperluan Undang-Undang dan Kontrak Yang Terpakai** Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga JDN dan pembekal serta semua pihak yang terlibat dalam pembekalan perkhidatan ICT di JDN. Keperluan perundangan yang perlu dipatuhi ialah seperti **LAMPIRAN B** dokumen ini.	Warga JDN Pembekal Pihak yang terlibat dalam perkhidmatan ICT JDN
5.31.3	**Peraturan Kawalan Kriptografi** Penggunaan kriptografi hendaklah mematuhi keperluan perundangan, dasar dan pekeliling seperti yang berikut: i. Akta Kerajaan Elektronik 2007; ii. Akta Tandatangan Digital 1997; iii. Dasar Kriptografi Negara; dan iv. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan 3 Tahun 2015 Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastructure (GPKI)]	Warga JDN Pemilik Sistem Pembekal Pihak yang terlibat dalam perkhidmatan ICT JDN

5.32. HAK HARTA INTELEK

ID	KETERANGAN	PERANAN
5.32.1	**Hak Harta Intelek** Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Semua pihak yang terlibat hendaklah melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Warga JDN Pemilik Sistem Pemilik Perkhidmatan Pengurus Projek Pembekal Pihak yang terlibat dalam perkhidmatan ICT JDN

5.33. PERLINDUNGAN REKOD

ID	KETERANGAN	PERANAN
5.33.1	**Perlindungan Rekod** Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian tanpa izin dan capaian ke atas orang yang tidak berkenaan.	Warga JDN Pemilik Sistem Pemilik Perkhidmatan Pengurus Projek Pembekal Pihak yang terlibat dalam perkhidmatan ICT JDN

5.34. PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI

ID	KETERANGAN	PERANAN
5.34.1	**Privasi dan Perlindungan Maklumat Peribadi** Maklumat peribadi merujuk kepada sebarang data yang boleh digunakan untuk mengenal pasti individu seperti nombor kad pengenalan, rekod perubatan dan lain-lain. Jika terdapat sebarang keperluan terhadap pengenalan tersebut hendaklah terlebih dahulu mendapat persetujuan daripada individu berkenaan.	Warga JDN Pemilik Sistem Pemilik Perkhidmatan Pembekal Pihak yang pihak yang mempunyai urusan dengan perkhidmatan ICT di JDN

ID	KETERANGAN	PERANAN
	Pelaksanaan perlindungan maklumat peribadi di JDN selaras dengan peruntukan yang dinyatakan dalam Akta Perlindungan Data Peribadi yang terkini.	

5.35. KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI

ID	KETERANGAN	PERANAN
5.35.1	**Kajian Semula Keselamatan Maklumat Secara Berkecuali** Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	Pemilik Sistem

5.36. PEMATUHAN DASAR, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
5.36.1	**Pematuhan Polisi dan Standard Keselamatan** Kajian semula secara berkala terhadap pematuhan dasar dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian.	CDO ICTSO Pengarah Bahagian Ketua Unit Pemilik maklumat
5.36.2	**Kajian Semula Pematuhan Teknikal** Kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung dalam polisi, piawaian dan keperluan komputer.	CDO ICTSO Pengarah Bahagian Ketua Unit Pemilik maklumat

ID	KETERANGAN	PERANAN
5.36.3	**Memastikan semua polisi, peraturan, akta dipatuhi dan dilaksana oleh semua peringkat proses perkhidmatan.** Semua warga JDN, pembekal dan pihak yang terlibat dalam perkhidmatan ICT JDN hendaklah mematuhi undang-undang, prosedur, dasar, peraturan yang sedang berkuat kuasa.	ICTSO Pengarah Bahagian Ketua Unit

5.37. DOKUMENTASI PROSEDUR OPERASI STANDARD

ID	KETERANGAN	PERANAN
5.37.1	**Dokumentasi Prosedur Operasi Standard** Semua prosedur operasi hendaklah didokumenkan dan disediakan kepada pihak yang melaksanakan operasi serta mematuhi perkara yang berikut: (a) Semua prosedur keselamatan siber yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; (b) 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; dan (c) Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	CSIRT Pemilik Sistem Pengarah Bahagian/Ketua Unit Pengarah Bahagian/Ketua Unit

6. KAWALAN SUMBER MANUSIA

Terdapat lapan kawalan sumber manusia yang terpakai dalam perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di JDN. Perincian kawalan sumber manusia seperti di bawah.

6.1. TAPISAN KESELAMATAN

ID	KETERANGAN	PERANAN
6.1.1	**Tapisan Keselamatan (Security Screening)** Tapisan keselamatan hendaklah dijalankan terhadap warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JDN yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan yang terlibat dalam menjamin keselamatan aset maklumat sebelum, semasa dan selepas perkhidmatan; dan (b) Menjalankan tapisan keselamatan untuk warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Warga JDN Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT JDN

6.2. TERMA DAN SYARAT PERKHIDMATAN

ID	KETERANGAN	PERANAN
6.2.1	**Terma dan Syarat Perkhidmatan** Persetujuan berkontrak dengan Warga JDN, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT di JDN hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi ialah seperti yang berikut: (a) menyatakan dengan lengkap dan jelas peranan serta tanggung jawab warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan yang terlibat dalam menjamin keselamatan aset ICT; dan (b) mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Warga JDN Pembekal Pihak yang mempunyai urusan ICT di JDN Pengurus Projek

6.3. KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
6.3.1	**Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat** Warga Jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai PKS JDN, sistem pengurusan keselamatan maklumat dan	Warga JDN ICTSO Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT di JDN

ID	KETERANGAN	PERANAN
	latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Memastikan kesedaran, pendidikan dan latihan diberikan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; (b) Memastikan kesedaran yang berkaitan polisi keselamatan siber jabatan perlu diberi dari masa ke semasa; dan (c) Memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ict digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.	

6.4. PROSES TATATERTIB

ID	KETERANGAN	PERANAN
6.4.1	**Proses Tatatertib** Proses tatatertib yang formal perlu ditentukan dan disampaikan kepada warga jabatan atau pihak berkepentingan terlibat yang lain bagi membolehkan tindakan diambil ke atas pelanggaran keselamatan maklumat yang dilakukan. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Memastikan adanya proses tindakan disiplin dan/atau undang-undang sekiranya berlaku pelanggaran terhadap polisi, perundangan dan peraturan yang ditetapkan oleh JDN atau Kerajaan; dan	Unit Integriti BKP

ID	KETERANGAN	PERANAN
	(b) Tindakan tatatertib atau tindakan yang sewajarnya akan dikenakan bagi sebarang pelanggaran kepada polisi ini.	

6.5. TANGGUNGJAWAB SELEPAS PENAMATAN PERANAN ATAU JAWATAN

ID	KETERANGAN	PERANAN
6.5.1.	**Pertukaran atau Penamatan Peranan atau Jawatan** Peranan dan tanggungjawab berkaitan keselamatan maklumat yang masih sah selepas penamatan atau pertukaran perjawatan hendaklah ditentukan, dikuat kuasa dan disampaikan kepada Warga JDN dan semua pihak yang terlibat. Semua Warga JDN dan pembekal serta pihak yang terlibat dengan perkhidmatan ICT JDN yang telah tamat peranan atau perkhidmatan perlu mematuhi perkara-perkara berikut: (a) Memastikan semua aset maklumat milik JDN atau kerajaan dikembalikan kepada JDN mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (c) Maklumat rasmi dalam aset maklumat tidak dibenarkan dibawa keluar dari JDN. Warga JDN yang telah bertukar keluar JDN atau tamat perkhidmatan hendaklah:	Warga JDN Pembekal Pihak yang mempunyai urusan dengan perkhidmatan ICT di JDN BKP

ID	KETERANGAN	PERANAN
	(a) Memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (c) Menyediakan dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.	

6.6. PERJANJIAN KERAHSIAAN ATAU KETAKDEDAHAN

ID	KETERANGAN	PERANAN
6.6.1	**Perjanjian Kerahsiaan atau Ketakdedahan** Syarat-syarat perjanjian kerahsiaan atau ketakdedahan (non-disclosure agreement) perlu mengambil kira keperluan organisasi dan hendaklah dikenal pasti dan didokumentasi dan ditandatangani oleh Warga JDN dan pihak berkepentingan terlibat yang lain. Pembekal atau pihak berkepentingan yang terlibat dengan perkhidmatan ICT JDN hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan. Perjanjian kerahsaan dan ketakdedahan bagi setiap pembekal atau pihak berkepentingan yang terlibat dengan perkhidmatan ICT JDN ini perlu disemak secara berkala **sekurang-**	

ID	KETERANGAN	PERANAN
	kurangnya sekali dalam tempoh setahun bagi memastikan senarai pihak pembekal atau pihak yang terlibat dengan perkhidmatan ICT JDN.	

6.7. BEKERJA SECARA JARAK JAUH

ID	KETERANGAN	PERANAN
6.7.1	**Bekerja Secara Jarak Jauh** Dasar dan langkah-langkah keselamatan hendaklah dilaksanakan bagi melindungi maklumat yang dicapai, diproses atau disimpan secara jarak jauh. Warga JDN yang bekerja jarak jauh hendaklah: (a) memastikan keselamatan maklumat jabatan dipatuhi dan tidak disebarkan kepada pihak ketiga; dan (b) memastikan arahan bekerja dari luar dipatuhi mengikut garis panduan yang ditetapkan.	

6.8. PELAPORAN INSIDEN KESELAMATAN MAKLUMAT

ID	KETERANGAN	PERANAN
6.8.1	**Pelaporan Insiden Keselamatan Maklumat** Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat berdasarkan pekeliling atau prosedur pengendalian insiden yang sedang	Pemilik Perkhidmatan CSIRT

ID	KETERANGAN	PERANAN
	berkuat kuasa. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menentukan mekanisme untuk melaporkan sebarang insiden melalui saluran dan dalam tempoh masa yang ditentukan; (b) Memberi kesedaran berkaitan prosedur pengendalian insiden dan hebahan kepada warga JDN sekiranya terdapat perubahan; dan (c) Memastikan warga JDN yang mengurus insiden mempunyai kompetensi yang diperlukan. Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT JDN berdasarkan prosedur pengendalian insiden yang sedang berkuat kuasa.	

7. KAWALAN FIZIKAL

Terdapat 14 kawalan fizikal yang terpakai dalam perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di JDN. Perincian kawalan fizikal seperti di bawah.

7.1. PERIMETER KESELAMATAN FIZIKAL

ID	KETERANGAN	PERANAN
7.1.1	**Perimeter Keselamatan Fizikal Perimeter Keselamatan Fizikal** Kawalan bertujuan untuk menghalang capaian tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan aset maklumat JDN. Perkara-perkara yang perlu dipatuhi termasuk yang berikut:	BKP

ID	KETERANGAN	PERANAN
	Perimeter keselamatan fizikal digunakan untuk melindungi aset, individu, dan persekitaran fizikal daripada ancaman, bahaya, atau kemungkinan kerosakan. Pelaksanaan kawalam ini melibatkan pelbagai strategi dan tindakan untuk memastikan keselamatan dalam ruang fizikal seperti bangunan, lokasi perindustrian, infrastruktur, atau kawasan penting lain. Berikut adalah beberapa unsur penting yang berkaitan dengan perimeter keselamatan fizikal: (a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (b) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (d) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau manusia dan sebarang bencana alam atau perbuatan manusia; (e) Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad;	

ID	KETERANGAN	PERANAN
	(f) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan (g) Memasang alat penggera atau kamera keselamatan.	

7.2. KEMASUKAN FIZIKAL

ID	KETERANGAN	PERANAN
7.2.1	**Kawalan Kemasukan Fizikal** Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis Jabatan. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Setiap warga JDN hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada jabatan apabila bertukar, tamat perkhidmatan atau bersara; (b) Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan; (c) Kehilangan pas hendaklah dilaporkan segera kepada Pihak Berkuasa; (d) Setiap pegawai dan kakitangan Jabatan yang hadir bertugas di luar waktu pejabat hendaklah melaporkan diri ke pos pengawal bagi tujuan rekod kehadiran;	Warga JDN Pelawat JDN Pihak yang mempunyai urusan dengan perkhidmatan ICT JDN

ID	KETERANGAN	PERANAN
	(e) Setiap pelawat hendaklah mendaftar kehadiran dalam buku pelawat di kaunter utama; dan (f) Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset maklumat JDN.	
7.2.2	**Kawasan Penyerahan dan Pemunggahan** Pintu masuk seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan. JDN hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.	BKP

7.3. KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN

ID	KETERANGAN	PERANAN
7.3.1	**Keselamatan Pejabat, Bilik dan Kemudahan** Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan bilik fail, bilik cetakan, bilik kawalan kamera litar tertutup (CCTV) dan pusat data perlu	BKP Pentadbir Pusat Data Warga JDN

ID	KETERANGAN	PERANAN
	dihadkan daripada dicapai tanpa kebenaran; (b) Kawasan tempat bekerja, bilik dan tempat operasi ICT perlu dihadkan daripada dicapai oleh orang luar; dan (c) Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan.	

7.4. PEMANTAUAN KESELAMATAN FIZIKAL

ID	KETERANGAN	PERANAN
7.4.1	**Pemantauan keselamatan fizikal** Premis fizikal harus dipantau oleh sistem pengawasan termasuk pengawal, penggera penceroboh, sistem pemantauan video seperti CCTV dan perisian pengurusan maklumat keselamatan fizikal sama ada diurus secara dalaman atau oleh penyedia perkhidmatan pemantauan. Sistem pemantauan harus dilindungi daripada capaian yang tidak dibenarkan untuk mengelakkan maklumat pengawasan, seperti suapan video, daripada dicapai oleh orang yang tidak dibenarkan atau sistem diceroboh secara jarak jauh. Melaksanakan pemantauan secara berterusan di premis bagi mengelakkan capaian secara fizikal yang tidak dibenarkan. Capaian kepada bangunan yang menempatkan sistem kritikal harus dipantau secara berterusan untuk mengesan capaian	BKP Pentadbir Pusat Data Warga JDN

ID	KETERANGAN	PERANAN
	yang tidak dibenarkan atau tingkah laku yang mencurigakan dengan: (a) Memasang sistem pemantauan video seperti CCTV untuk melihat dan merakam capaian ke kawasan sensitif di dalam dan di luar premis JDN; (b) Memasang, mengikut piawaian terpakai yang berkaitan, dan menguji pengesan sentuhan, bunyi atau gerakan secara berkala untuk mencetuskan penggera pencerobohan seperti: (i) Memasang pengesan sesentuh yang mencetuskan penggera apabila sesentuh dibuat atau pecah di mana-mana tempat di mana sentuhan boleh dibuat atau dipecahkan (seperti tingkap dan pintu dan di bawah objek) untuk digunakan sebagai penggera panik; (ii) Memasang pengesan yang sensitif kepada bunyi kaca pecah yang boleh digunakan untuk mencetuskan penggera bagi memberi amaran kepada kakitangan keselamatan; (c) Menggunakan penggera tersebut untuk melindungi semua pintu luar dan tingkap yang boleh dicapai. Kawasan yang tidak berpenghuni perlu sentiasa diberi perhatian; dan (d) Perlindungan juga perlu disediakan untuk kawasan lain (contoh komputer atau bilik komunikasi).	

7.5. PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN PERSEKITARAN

ID	KETERANGAN	PERANAN
7.5.1	**Perlindungan Daripada Ancaman Fizikal dan Persekitaran** Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. JDN perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	BKP Pentadbir Pusat Data

7.6. BEKERJA DI KAWASAN SELAMAT

ID	KETERANGAN	PERANAN
7.6.1	**Bekerja di Kawasan Selamat** Langkah-langkah kawalan keselamatan bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pihak yang dibenarkan sahaja. Kawalan ini dilakukan untuk melindungi aset maklumat yang terdapat dalam premis JDN termasuklah Pusat Data. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Langkah-langkah kawalan keselamatan ke atas kawasan tersebut ialah seperti yang berikut: (a) Sumber data atau pelayan, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik pelayan atau bilik khas yang mempunyai ciri-ciri keselamatan	BKP Pentadbir Pusat Data

ID	KETERANGAN	PERANAN
	yang tinggi termasuk sistem pencegahan kebakaran; (b) Capaian adalah terhad kepada pihak yang telah diberi kuasa sahaja dan dipantau pada setiap masa; (c) Pemantauan dibuat menggunakan CCTV atau lain-lain peralatan yang sesuai; (d) Peralatan keselamatan (CCTV, log capaian) perlu diperiksa secara berjadual; (e) Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; (f) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; (g) Lokasi premis yang menempatkan aset maklumat serta infrastruktur, peralatan atau perkakasan yang berkaitan hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; (h) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; (i) Memperkukuh dinding dan siling; dan (j) Mengehadkan jalan keluar masuk.	

7.7. POLISI MEJA KOSONG DAN SKRIN KOSONG

ID	KETERANGAN	PERANAN
7.7.1	**Polisi Meja Kosong dan Skrin Kosong** Polisi Meja Koson dan Skrin Kosong bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna, pada paparan skrin komputer, mesin pencetak, mesin faksimile atau mesin pengimbas apabila pengguna tidak berada di tempatnya. Polisi Meja Kosong dan Skrin Kosong ialah satu set garis panduan yang digunakan dalam pengurusan keselamatan maklumat dan keberkesanan dalam organisasi untuk melindungi maklumat sensitif dan menjaga privasi pekerja. Objektif utama polisi ini adalah untuk memastikan data dan maklumat terjamin keselamatannya dan tidak didedahkan kepada pihak yang tidak mempunyai hak capaian ke atas data atau maklumat tersebut. Polisi ini merangkumi aspek-aspek berikut: (a) Penggunaan fungsi kata laluan penyelamat skrin (screen saver password) atau log keluar apabila meninggalkan komputer; (b) Pengaktifan fungsi mod senyap; (c) Penyimpanan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; (d) Semua dokumen hendaklah diambil segera daripada pencetak, pengimbas, mesin faksimile dan mesin fotostat; (e) Pengawalan e-mel masuk dan keluar;	Warga JDN

ID	KETERANGAN	PERANAN
	(f) Kawalan penggunaan mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital; (g) Penetapanan dan hebahan peraturan serta panduan berkaitan konfigurasi mesej timbul (pop-up message) di skrin (contohnya mematikan *pop-up* e-mel dan mesej baharu semasa pembentangan, perkongsian skrin atau di kawasan awam); dan (h) Memadamkan maklumat sensitif atau kritikal pada papan putih dan jenis paparan lain apabila tidak diperlukan lagi.	
7.7.2	**Peralatan Pengguna Tanpa Kawalan** Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara yang berikut: (a) Tamatkan sesi aktif apabila selesai tugas; (b) Log keluar komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan (c) Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan.	Warga JDN

7.8. PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT

ID	KETERANGAN	PERANAN
7.8.1	**Penempatan dan Perlindungan Peralatan ICT** Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan. Langkah-langkah keselamatan yang perlu diambil ialah seperti yang berikut: (a) Penggunaan kata laluan untuk dicapai ke sistem komputer diwajibkan; (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; (d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem; (e) 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; (f) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna;	Warga JDN Pentadbir Aset Pegawai Aset

ID	KETERANGAN	PERANAN
	(g) Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; (h) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan Generator Set (Gen-Set); (i) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; (j) Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dan berkunci; (k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai; (l) Peralatan ICT yang hendak dibawa ke luar premis jabatan, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan; (m) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden; (n) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; (o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal	

ID	KETERANGAN	PERANAN
	komputer tersebut ditempatkan tanpa kebenaran Pegawai Aset; (p) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pegawai Aset untuk dibaik pulih; (q) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (r) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal tanpa kebenaran Pentadbir Aset; (s) Pengguna dilarang sama sekali mengubah kata laluan penatdbir yang telah ditetapkan oleh Pentadbir Aset; dan (t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi kerajaan dan JDN sahaja.	

7.9. KESELAMATAN ASET DI LUAR PREMIS

ID	KETERANGAN	PERANAN
7.9.1	**Keselamatan Aset di Luar Premis** Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis jabatan. Peralatan yang dibawa keluar dari premis jabatan adalah terdedah kepada	Warga JDN Pembekal Pihak yang mempunyai urusan berkaitan perkhidmatan ICT JDN

ID	KETERANGAN	PERANAN
	pelbagai risiko. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (c) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan.	

7.10. MEDIA STORAN

ID	KETERANGAN	PERANAN
7.10.1	**Pengurusan Media Boleh Alih** Untuk mengelakkan kerosakan pada aset maklumat dan gangguan kepada aktiviti perkhidmatan, media boleh alih harus dikawal dan dilindungi secara fizikal. Media boleh alih mesti dikendalikan mengikut klasifikasi maklumat. Prosedur-prosedur pengendalian media yang perlu dipatuhi ialah seperti yang berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;	Pegawai Aset Pentadbir Aset

ID	KETERANGAN	PERANAN
	(d) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan (e) Menyimpan semua jenis media di tempat yang selamat.	
7.10.2	**Pelupusan Media** Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan; dan Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	Pegawai Aset Pentadbir Aset
7.10.4	**Pengalihan Aset** Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran JDN terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: (a) Peralatan ICT yang hendak dibawa keluar dari premis jabatan untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Jabatan atau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan (b) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan.	Pegawai Aset Pentadbir Aset

ID	KETERANGAN	PERANAN
7.10.5	**Pengendalian Media** Melindungi aset maklumat daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	Warga JDN Pegawai Aset Pentadbir Aset

7.11. UTILITI SOKONGAN

ID	KETERANGAN	PERANAN
7.11.1	**Utiliti Sokongan** Aset maklumat hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan bagi aset maklumat perlu diselenggara dari semasa ke semasa **sekurang-kurangnya sekali dalam tempoh setahun**.	Pegawai Aset Pentadbir Aset

7.12. KESELAMATAN KABEL

ID	KETERANGAN	PERANAN
7.12.1	**Keselamatan Kabel** Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah-langkah keselamatan yang perlu diambil ialah seperti yang berikut:	Pentadbir Sistem Pegawai Aset Pentadbir Aset

ID	KETERANGAN	PERANAN
	(a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan pemintasan maklumat pada kabel; dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui sesalur kabel bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	

7.13. PENYELENGGARAAN PERALATAN

ID	KETERANGAN	PERANAN
7.13.1	**Penyelenggaraan Peralatan** Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut: (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;	Pentadbir Sistem Pegawai Aset Pentadbir Aset

ID	KETERANGAN	PERANAN
	(c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan pemintasan maklumat pada kabel; dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui sesalur kabel bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	

7.14. PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN

ID	KETERANGAN	PERANAN
7.14.1	**Pelupusan yang Selamat atau Penggunaan Semula Peralatan** Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (overwrite) sebelum dilupuskan atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh JDN dan ditempatkan di JDN. Peralatan aset maklumat yang hendak dilupuskan perlu mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan jabatan. Langkah-langkah seperti yang berikut hendaklah diambil: (a) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah milik, data-data dalam	Pentadbir Sistem Pegawai Aset Pentadbir Aset

ID	KETERANGAN	PERANAN
	storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat; (b) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (c) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (d) Pelupusan aset maklumat hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; (e) Warga JDN **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti yang berikut tanpa kebenaran JDN: (i) Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi; (ii) Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; (iii) Menyimpan dan memindahkan perkakasan luaran komputer seperti pembesar suara dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di agensi; (iv) Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan;	

ID	KETERANGAN	PERANAN
	(v) Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab jabatan; (f) Warga JDN bertanggungjawab memastikan segala maklumat rasmi kerajaan disalin pada media storan pendua sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan bagi tujuan sandaran maklumat; (g) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal. Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan; (h) Merujuk pekeliling yang sedang berkuat kuasa seperti: (i) Pelupusan aset: Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa. (ii) Pelupusan dokumen: Arahan Keselamatan dan tatacara Jabatan Arkib Negara. (i) Pegawai Aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem pengurusan aset.	

8. KAWALAN TEKNOLOGI

Terdapat 34 kawalan teknologi yang utama dan perlu dipatuhi oleh semua pihak yang terlibat dalam pengurusan data dan maklumat di JDN. Perincian kawalan teknologi seperti di bawah.

8.1. PERIMETER KESELAMATAN FIZIKAL (PHYSICAL SECURITY PARAMETER)

ID	KETERANGAN	PERANAN
8.1.1	**Polisi Peranti Mudah Alih** Polisi dan langkah-langkah keselamatan sokongan hendaklah digunakan bagi mengurus risiko yang timbul melalui penggunaan peranti mudah alih. **JDN perlu m**embangun serta menyebarkan dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang dikenal pasti melalui penggunaan peranti titik akhir merangkumi perkara yang berikut: (a) jenis dan tahap klasifikasi maklumat yang digunakan oleh pengguna peranti titik akhir untuk mengendali, memproses, menyimpan atau menyokong kemudahan maklumat; (b) peraturan untuk capaian kepada perkhidmatan maklumat, rangkaian awam atau mana-mana rangkaian lain di luar premis; (c) penyulitan peranti storan; (d) perlindungan terhadap virus dan perisian hasad (malware);	ICTSO Warga JDN

ID	KETERANGAN	PERANAN
	(e) Menyekat penggunaan keupayaan jarak jauh (remote disabling), pemadaman dan penguncian (lockout); (f) sandaran (back up); (g) penggunaan perkhidmatan web dan aplikasi web; (h) analisis tingkah laku pengguna akhir; (i) penggunaan perkhidmatan mudah alih (portable service), termasuk peranti memori mudah alih, dan kemungkinan untuk menghilangkan keupayaan port fizikal (contoh: port USB, USB Type-C); dan (j) penggunaan keupayaan pembahagian (partitioning capabilities) jika disokong oleh peranti titik akhir pengguna.	

8.2. HAK CAPAIAN ISTIMEWA

ID	KETERANGAN	PERANAN
8.2.1	**Pengurusan Hak Capaian Istimewa** Peruntukan dan penggunaan hak capaian istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak capaian perlu diberikan kawalan dan penyeliaan yang ketat mengikut keperluan skop tugas yang telah dikenal pasti berdasarkan prosedur yang berkuat kuasa.	Pentadbir Sistem ICT

8.3. SEKATAN CAPAIAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.3.1	**Sekatan Capaian Maklumat** Capaian kepada fungsi maklumat dan sistem ICT hendaklah dihadkan mengikut dasar kawalan capaian merangkumi perkara yang berikut: (a) tidak membenarkan pengguna yang tidak berdaftar mencapai maklumat terperingkat; (b) menyediakan mekanisme konfigurasi untuk mengawal capaian kepada maklumat dalam sistem, aplikasi dan perkhidmatan; (c) mengawal data yang boleh dicapai oleh pengguna tertentu; (d) mengawal identiti atau kumpulan identiti yang mempunyai hak capaian, seperti membaca, menulis, memadam dan melaksanakan (execute); (e) menyediakan kawalan capaian fizikal atau logikal untuk mengasingkan aplikasi sensitif, data aplikasi, atau sistem; dan (f) Pentadbir Sistem hendaklah melaksanakan semakan dan pemantauan secara berkala **sekurang-kurangnya setahun sekali** bagi memastikan pengguna yang mencapai sistem adalah sah. Penggunaan proses dan teknik pengurusan capaian yang dinamik (dynamic acess management) bagi melindungi maklumat sensitif perlu dilaksanakan sekiranya	Pentadbir Sistem Pemilik Maklumat

ID	KETERANGAN	PERANAN
	diperlukan dengan mengambil kira keperluan berikut: (a) perlindungan sepanjang kitar hayat maklumat dengan menetapkan peraturan berdasarkan kes penggunaan; (b) mewujudkan operasi, proses memantau dan melapor serta infrastruktur sokongan teknikal; dan (c) melindungi data dengan menetapkan keperluan pengesahan, menghadkan capaian, melaksanakan penyulitan, menetapkan kebenaran mencetak, merekod capaian pengguna dan penggunaan maklumat serta memberikan amaran sekiranya terdapat percubaan untuk menyalahgunakan maklumat.	

8.4. KAWALAN CAPAIAN KEPADA KOD SUMBER

ID	KETERANGAN	PERANAN
8.4.1	**Kawalan Capaian Kepada Kod Sumber Program** Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan ialah seperti yang berikut: (a) Log audit perlu dikekalkan kepada semua capaian kepada kod sumber; (b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; (c) Kod sumber bagi semua sistem aplikasi atau kod sumber sistem aplikasi yang	Pentadbir Sistem ICT Pengurus Projek Pembekal Pihak yang terlibat dalam perkhidmatan IC JDN

ID	KETERANGAN	PERANAN
	disesuaikan hendaklah menjadi hak milik JDN; (d) Mengurus capaian kepada kod sumber program dan perpustakaan sumber program (program source libraries) mengikut prosedur yang ditetapkan; dan (e) Memberi capaian baca dan tulis kepada kod sumber berdasarkan keperluan dan berupaya mengawal risiko mengubah atau menyalah guna kod sumber berdasarkan prosedur yang ditetapkan.	

8.5. PENGESAHAN IDENTITI YANG SELAMAT

ID	KETERANGAN	PERANAN
8.5.1	**Prosedur Log Masuk yang Selamat** Kawalan terhadap capaian aplikasi sistem perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan ialah seperti yang berikut: (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Jabatan; (b) Menjana amaran (alert) sekiranya berlaku perlanggaran semasa proses log maşuk terhadap aplikasi sistem; (c) Mengawal capaian ke atas aplikasi sistem mengikut prosedur yang ditetapkan; (d) Mewujudkan teknik pengesahan pelbagai faktor (multi factro authentication, MFA) berdasarkan pengkelasan maklumat yang	Pemilik Sistem Pentadbir Sistem

ID	KETERANGAN	PERANAN
	bersesuaian bagi mengesahkan pengenalan diri pengguna; (e) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan yang kukuh dan berkualiti; dan (f) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	
8.5.2	**Sistem Pengurusan Kata Laluan** Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JDN seperti yang berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi atau setelah mencapai tempoh masa pertukaran kata laluan yang ditetapkan oleh Pentadbir Sistem; (c) Panjang kata laluan mestilah sekurang-kurangnya **DUA BELAS (12) AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (alphanumeric) **KECUALI** bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; (d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekali pun; (e) Fungsi kunci skrin (lock screen) hendaklah diaktifkan terutamanya pada	Pemilik Sistem Pentadbir Sistem

ID	KETERANGAN	PERANAN
	komputer yang terletak di ruang guna sama; (f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan dalam atur cara; (g) Kuat kuasa pertukaran kata laluan semasa yang ditetapkan oleh sistem secara automatik (default password) selepas login kali pertama atau selepas tetapan semula kata laluan; (h) kata laluan tidak berdasarkan perkataan kamus atau gabungannya; (i) kata laluan yang sama tidak digunakan merentas perkhidmatan dan sistem yang berbeza; (j) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (k) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum **TIGA (3) KALI** sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; dan (l) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	

8.6. PENGURUSAN KAPASITI

ID	KETERANGAN	PERANAN
8.5.1	**Pengurusan Kapasiti** Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) 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; (b) Kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang; dan (c) Mempertimbangkan penggunaan pengkomputeran awan bagi pengurusan kapasiti yang berkesan, anjal (elasticity) dan boleh skala (scalability).	Pemilik Sistem Pentadbir Sistem

8.7. PERLINDUNGAN DARIPADA PERISIAN HASAD

ID	KETERANGAN	PERANAN
8.7.1	**Perlindungan daripada Perisian Hasad** Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada serangan perisian hasad hendaklah	Pemilik Sistem Pentadbir Sistem

ID	KETERANGAN	PERANAN
	dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara yang perlu dilaksanakan bagi memastikan perlindungan aset maklumat daripada perisian hasad ialah seperti yang berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program perisian hasad seperti antivirus, *Intrusion Detection* System (IDS), *Intrusion Prevention System* (IPS) dan *Web Application Firewall* (WAF) serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang yang sedang berkuat kuasa; (c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; (d) Mengemas kini antivirus dengan *signature*/*pattern* antivirus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri program kesedaran mengenai ancaman perisian hasad dan cara mengendalikannya; (g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah	

ID	KETERANGAN	PERANAN
	ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (h) Menyediakan pelan kesinambungan perkhidmatan yang sesuai untuk pulih daripada serangan perisian hasad; (i) Menentukan prosedur dan tanggungjawab untuk menangani perlindungan terhadap perisian hasad pada sistem; dan (j) Mengesahkan ketepatan sumber maklumat yang berkaitan dengan perisian hasad.	

8.8. PENGURUSAN KERENTANAN TEKNIKAL

ID	KETERANGAN	PERANAN
8.8.1	**Pengurusan Kerentanan Teknikal** Maklumat berkaitan kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan. Kawalan terhadap keterdedahan teknikal perlu dilaksanakan untuk melindungi sistem maklumat, perisian, dan infrastruktur teknikal organisasi daripada ancaman dan serangan yang berkaitan dengan kerentanan. Perkara yang perlu dipatuhi ialah seperti yang berikut:	Pemilik Sistem Pentadbir Sistem

ID	KETERANGAN	PERANAN
	(a) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi; (b) Mengenal pasti, menilai dan menganalisis tahap risiko kerentanan yang wujud dalam sistem, perisian, dan rangkaian JDN; (c) Melaksanakan tindakan penambahbaikan untuk mengatasi kerentanan yang telah dikenal pasti, termasuk melaksanakan penambahbaikan keselamatan dan konfigurasi semula; (d) Memantau sistem dan perisian secara berterusan untuk mengenalpasti kerentanan yang mungkin muncul dalam masa sebenar; dan (e) Melaksana dan memastikan amalan terbaik dalam keselamatan teknikal dan pengurusan kerentanan.	

8.9. PENGURUSAN KONFIGURASI

ID	KETERANGAN	PERANAN
8.9.1	**Pengurusan konfigurasi** Pengurusan konfigurasi perlu dilaksanakan untuk memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul berserta dengan keperluan keselamatan. Konfigurasi tidak diubah tanpa kebenaran berdasarkan prosedur yang ditetapkan. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Melindungi capaian terhadap fail konfigurasi mengikut kawalan yang ditetapkan;	Pentadbir Sistem Pentadbir Pelayan Pentadbir Rangkaian

ID	KETERANGAN	PERANAN
	(b) Merekod dan menyimpan sebarang perubahan konfigurasi dengan selamat; dan (c) Memantau konfigurasi untuk mengesahkan tetapan konfigurasi dan menilai kawalan keselamatan.	

8.10. PENGHAPUSAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.10.1	**Penghapusan Maklumat** Maklumat terperingkat yang disimpan dalam aset maklumat hendaklah dilupuskan mengikut prosedur yang ditetapkan. Perkara yang perlu dipatuhi ialah seperti berikut: (a) Menentukan kaedah penghapusan maklumat yang sesuai selaras dengan keperluan JDN; (b) Merekod keputusan sebagai bukti penghapusan maklumat; dan (c) Mendapatkan bukti penghapusan maklumat jika menggunakan perkhidmatan pembekal.	Pemilik Maklumat Pemilik Aset Pegawai Aset

8.11. PENYEMBUNYIAN DATA

ID	KETERANGAN	PERANAN
8.11.1	**Penyembunyian data** Penyembunyian data dilaksanakan bagi melindungi data sensitif seperti data *Personal Identifiable Information* (PII), dan data terperingkat dengan mengambil kira keperluan perkhidmatan dan polisi kawalan capaian serta polisi lain yang berkaitan	Pemilik Maklumat Pentadbir Sistem

ID	KETERANGAN	PERANAN
	tertakluk kepada keperluan perundangan dan peraturan yang berkuat kuasa. Pelaksanaan penyamaran data ialah berdasarkan prosedur yang ditetapkan. Penyembunyian data diperlukan bagi melindungi data PII dan data sensitif daripada terdedah atau bocor kepada pihak yang tidak bertanggung jawab yang akan menyebabkan imej JDN terjejas. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Mengenal pasti klasifikasi data yang perlu dikongsi dengan pihak ketiga; (b) Mengenal pasti teknik yang sesuai selaras dengan sensitiviti data; dan (c) Memastikan pengguna hanya dapat mencapai data yang minimum yang dibenarkan sahaja.	

8.12. PENCEGAHAN KETIRISAN DATA

ID	KETERANGAN	PERANAN
8.12.1	**Pencegahan ketirisan Data** Data dalam sistem, rangkaian dan peralatan lain perlu dilindungi daripada pendedahan dan pengekstrakan data yang tidak sah oleh individu atau sistem. Perkara yang perlu dipatuhi ialah seperti berikut: (a) Mengenal pasti dan mengkelaskan maklumat untuk dilindungi daripada ketirisan; (b) Memantau saluran transaksi dan perkongsian data (contohnya e-mel,	Pemilik Maklumat Pentadbir Sistem

ID	KETERANGAN	PERANAN
	pemindahan fail, perkhidmatan peranti atau media mudah alih; dan (c) Melaksanakan tindakan pengukuhan untuk mengelakkan ketirisan maklumat.	

8.13. SANDARAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.13.1	**Sandaran Maklumat** Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara berkala mengikut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di off site. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi; (c) Menguji sistem sandaran sedia ada secara berkala **sekurang-kurangnya setahun sekali** bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan	Pentadbir Sistem

ID	KETERANGAN	PERANAN
	(d) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya **TIGA GENERASI**.	

8.14. LEWAHAN BAGI KEMUDAHAN PEMPROSESAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.14.1	**Lewahan bagi Kemudahan Pemprosesan Maklumat** JDN perlu mengenal pasti keperluan, mereka bentuk dan melaksanakan lewahan untuk memastikan kesinambungan perkhidmatan dan ketersediaan kemudahan pemprosesan maklumat. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Mengenal pasti keperluan dan tahap kritikal bagi ketersediaan perkhidmatan dan sistem maklumat; (b) Menyediakan lewahan bagi kemudahan pemprosesan maklumat yang dikenal pasti; (c) Menguji keberkesanan (failover testing) untuk memastikan keberkesanan kemudahan lewahan secara berkala; dan (d) Menyediakan mekanisme yang bersesuaian untuk memberi amaran gangguan atau kegagalan kemudahan pemprosesan maklumat kepada pemilik sistem untuk memastikan lewahan	Pentadbir Pusat Data, Pemilik Perkhidmatan Pentadbir Sistem

ID	KETERANGAN	PERANAN
	tersebut boleh mengambil alih fungsi kemudahan utama dibaiki atau diganti.	

8.15. PENGELOGAN MAKLUMAT

ID	KETERANGAN	PERANAN
8.15.1	**Menyediakan Log** Sistem yang dibangunkan perlu merekod aktiviti dan menjana bahan bukti untuk memastikan maklumat log adalah berintegriti dan boleh digunakan sebagai bahan bukti jika berlaku insiden keselamatan maklumat. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menyedia, menyimpan, melindungi dan menganalisis log yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa berkaitan keselamatan maklumat. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem; (b) Log hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan; (c) Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling yang sedang berkuat kuasa. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi pelayan dan aplikasi yang perlu diaktifkan ialah seperti yang berikut: (i) Fail log sistem pengoperasian;	Pentadbir Sistem

ID	KETERANGAN	PERANAN
	(ii) Fail log perkhidmatan (service) (contoh: web, e-mel); (iii) Fail log aplikasi (audit trail); dan (iv) Fail log rangkaian (contoh: switch, firewall, IPS).	
8.15.2	**Perlindungan Maklumat Log** Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada perubahan dan capaian tanpa izin merangkumi perkara berikut: (a) Pengguna, termasuk mereka yang mempunyai hak capaian istimewa, tidak diberi kebenaran untuk memadam atau menyahaktifkan log aktiviti mereka sendiri; dan (b) Kemudahan pengelogan beroperasi dengan baik.	Pentadbir Sistem
8.15.3	**Analisis Log** Analisis log perlu merangkumi analisis dan interpretasi aktiviti keselamatan maklumat untuk mengenal pasti aktiviti yang luar biasa atau tingkah laku yang janggal yang menunjukkan indikator sistem terjejas. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Memantau penggunaan kemudahan memproses maklumat secara berkala;	Pentadbir Sistem

ID	KETERANGAN	PERANAN
	(b) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak secara berkala dan laporan perlu disediakan jika perlu; (c) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; (d) Log Audit yang merekodkan semua aktiviti perlu diwujudkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan (e) Aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan aktiviti tersebut kepada CSIRT JDN.	

8.16. AKTIVITI PEMANTAUAN

ID	KETERANGAN	PERANAN
8.16.1	**Aktiviti Pemantauan** Rangkaian, sistem dan aplikasi harus dipantau dan tindakan sewajarnya diambil untuk menilai kemungkinan insiden keselamatan maklumat. Pentadbir Sistem perlu memantau untuk mengesan tingkah laku tidak normal (anomali) dan kemungkinan berlaku insiden keselamatan maklumat. Aktiviti pemantauan perlu merangkumi perkara seperti yang berikut:	Pentadbir Sistem Pentadbir Rangkaian Pentadbir Pelayan CSIRT

ID	KETERANGAN	PERANAN
	(a) Trafik keluar (outbound) dan masuk (inbound) bagi rangkaian, sistem dan aplikasi; (b) Capaian kepada sistem, pelayan, peralatan rangkaian, sistem pemantauan, aplikasi kritikal; (c) Log daripada peralatan keselamatan (contohnya antivirus, IDS, sistem pencegahan pencerobohan (IPS), penapis web, firewall, pencegahan kebocoran data); (d) Log peristiwa yang berkaitan dengan sistem dan aktiviti rangkaian; (e) Memastikan supaya kod sumber yang dilaksanakan telah diberi kebenaran untuk dilaksanakan dan tidak diubah tanpa kebenaran; dan (f) Penggunaan dan prestasi sumber.	

8.17. PENYEGERAKAN JAM

ID	KETERANGAN	PERANAN
8.17.1	**Penyegerakan Jam** Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut waktu piawai Malaysia. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam jabatan atau domain keselamatan perlu diseragamkan dengan waktu piawai Malaysia yang	Pentadbir Sistem

ID	KETERANGAN	PERANAN
	ditetapkan oleh National Metrology Institute of Malaysia (NMIM).	

8.18. PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA

ID	KETERANGAN	PERANAN
8.18.1	**Penggunaan Program Utiliti yang Mempunyai Hak Istimewa** Penggunaan program utiliti yang boleh mengatasi (overriding) kawalan sistem dan aplikasi hendaklah dikawal dan dihadkan kepada pegawai yang dibenarkan sahaja Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Had penggunaan program utiliti kepada bilangan praktikal minimum pengguna yang dipercayai dan dibenarkan; (b) Penggunaan prosedur pengenalan, pengesahan dan kebenaran untuk program utiliti, termasuk pengenalan unik pengguna program utiliti; (c) Mentakrif dan mendokumentasikan tahap kebenaran untuk program utiliti; (d) Kebenaran untuk menggunakan program utiliti secara ad hoc; (e) Melaksanakan pengasingan tugas dengan menghadkan capaian pengguna yang mempunyai capaian kepada program utiliti; (f) Mengalih keluar atau melumpuhkan semua program utiliti yang tidak diperlukan;	

ID	KETERANGAN	PERANAN
	(g) Menghadkan ketersediaan program utiliti; dan (h) Pengelogan semua penggunaan program utiliti.	

8.19. PEMASANGAN PERISIAN PADA SISTEM OPERASI

ID	KETERANGAN	PERANAN
8.19.1	**Pemasangan Perisian pada Sistem yang Beroperasi** Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus ialah seperti yang berikut: (a) Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; (b) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; (c) Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur; (d) Pengemaskinian perisian operasi hanya boleh dilaksanakan oleh pentadbir terlatih atas kebenaran pengurusan; (e) Memastikan bahawa hanya kod boleh laksana (executable code) yang telah diluluskan dan tiada kod pembangunan	Pentadbir Sistem

ID	KETERANGAN	PERANAN
	atau pengkompil (compilers) dipasang pada sistem operasi; (f) Mengemas kini semua perpustakaan sumber (source libraries) program yang sepadan; (g) Menggunakan sistem kawalan konfigurasi untuk mengekalkan kawalan semua perisian operasi serta dokumentasi sistem; (h) Mengarkibkan versi lama perisian, bersama-sama dengan semua maklumat dan parameter, prosedur, butiran konfigurasi dan perisian sokongan yang diperlukan sebagai langkah luar jangka (contigency), dan selagi perisian itu diperlukan untuk membaca atau memproses data yang diarkibkan.	
8.19.2	**Sekatan ke atas Pemasangan Perisian** Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga JDN, pembekal serta pihak yang mempunyai urusan dengan perkhidmatan ICT JDN; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan (c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.	Warga JDN Pentadbir Sistem Pegawai Aset

8.20. KESELAMATAN RANGKAIAN

ID	KETERANGAN	PERANAN
8.20.1	**Kawalan Rangkaian** Infrastruktur rangkaian hendaklah dikawal dan diuruskan sebaik mungkin dalam infrastruktur rangkaian daripada sebarang ancaman demi melindungi ancaman kepada sistem dan aplikasi dalam rangkaian. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas daripada risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; (e) Tembok keselamatan hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian; (f) Semua trafik keluar dan masuk rangkaian hendaklah melalui tembok keselamatan di bawah kawalan jabatan;	Pentadbir Rangkaian

ID	KETERANGAN	PERANAN
	(g) Semua perisian untuk menganalisis atau menawan paket rangkaian dilarang dipasang pada komputer pengguna KECUALI mendapat kebenaran JDN; (h) Memasang perisian IPS bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat Kerajaan; (i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; (j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan Jabatan tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di jabatan sahaja dan penggunaan modem adalah dilarang sama sekali; (l) Kemudahan bagi rangkaian tanpa wayar JDN hendaklah dipantau dan dikawal penggunaannya; (m) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan; (n) Menempatkan atau memasang antara muka (interfaces) yang bersesuaian antara rangkaian jabatan, rangkaian jabatan lain dan rangkaian awam; (o) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;	

ID	KETERANGAN	PERANAN
	(p) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; (q) Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; (r) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan jabatan; dan (s) Mewujud dan melaksana kawalan pengalihan laluan (routing control) bagi memastikan pematuhan terhadap peraturan jabatan. Semua peralatan yang hendak disambung kepada rangkaian perlu bebas daripada virus dan mempunyai antivirus yang sah; (t) Capaian kepada rangkaian perlu dilaksanakan mengikut kategori yang telah ditetapkan iaitu Intranet, Internet dan *Demilitrarized Zone* (DMZ); (u) Sistem yang terdapat dalam rangkaian Intranet tidak dibenarkan dicapai dari Internet; (v) Pihak ketiga tidak dibenarkan untuk mencapai rangkaian Intranet kecuali untuk kerja-kerja pembangunan atau penyelenggaraan sistem dengan kebenaran JDN; dan (w) Capaian kepada rangkaian tanpa wayar hendaklah dikawal mengikut kategori pengguna.	

8.21. KESELAMATAN PERKHIDMATAN RANGKAIAN

ID	KETERANGAN	PERANAN
8.21.1	**Keselamatan Perkhidmatan Rangkaian** Pengurusan bagi semua perkhidmatan rangkaian dalaman dan sumber luar yang merangkumi mekanisme keselamatan dan tahap serta keperluan perkhidmatan rangkaian hendaklah dikenal pasti dan dimasukkan dalam perjanjian perkhidmatan.	Pentadbir Rangkaian

8.22. PENGASINGAN RANGKAIAN

ID	KETERANGAN	PERANAN
8.22.1	**Pengasingan dalam Rangkaian** Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian di JDN.	Pentadbir Rangkaian

8.23. PENAPISAN WEB

ID	KETERANGAN	PERANAN
8.23.1	**Penapisan Web** Kawalan penapisan web dalam bentuk perisian atau sebagainya perlu dilaksanakan bagi mengesan dan menyekat ke laman web yang dianggap tidak selamat dan tidak sesuai. Ini bagi melindungi sistem maklumat daripada sebarang ancaman keselamatan laman web luaran. JDN hendaklah mengurangkan risiko mencapai laman web yang mengandungi maklumat yang dilarang atau diketahui mengandungi virus atau data pancingan (phishing) data oleh pengguna.	Pentadbir Rangkaian

ID	KETERANGAN	PERANAN
	JDN hendaklah mengenal pasti jenis laman web yang patut atau tidak boleh dicapai oleh warga JDN. JDN hendaklah mempertimbangkan untuk menyekat capaian kepada jenis laman web yang berikut: (a) Laman web yang mempunyai fungsi muat naik maklumat melainkan dibenarkan atas sebab perkhidmatan yang sah; (b) Tapak web yang diketahui atau disyaki berniat jahat; (c) Pelayan arahan dan kawalan (command and control); (d) Laman web berniat jahat yang diperoleh daripada risikan ancaman; dan (e) Laman web yang berkongsi kandungan haram.	

8.24. PENGGUNAAN KRIPTOGRAFI

ID	KETERANGAN	PERANAN
8.24.1	**Polisi Penggunaan Kawalan Kriptografi** Kriptografi merangkumi kaedah-kaedah seperti yang berikut: (a) **Penyulitan Data**: Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat penyulitan semasa dalam simpanan atau semasa sedang dipindahkan. (b) **Tandatangan Digital**: Tandatangan digital digunakan bagi memastikan	Pemilik Maklumat Pentadbir Sistem

ID	KETERANGAN	PERANAN
	maklumat digital tulen dan mempunyai integriti serta tidak boleh disangkal.	
8.24.2	**Pengurusan Infrastruktur Kunci Awam** Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah sijil digital tersebut.	Pentadbir Sistem Pemilik Sijil Digital PKI

8.25. KITAR HAYAT PEMBANGUNAN SISTEM YANG SELAMAT

ID	KETERANGAN	PERANAN
8.25.1	**Dasar Pembangunan Sistem yang Selamat** Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam sistem. Perkara yang perlu dipertimbangkan ialah seperti yang berikut: (a) Keselamatan persekitaran pembangunan; (b) Keselamatan pangkalan data; (c) Keperluan keselamatan dalam fasa reka bentuk; (d) Keperluan titik semak keselamatan dalam carta perbatuan projek; (e) Keperluan pengetahuan ke atas keselamatan aplikasi; (f) Keselamatan dalam kawalan versi; dan	Pembangun Sistem Pentadbir Sistem

ID	KETERANGAN	PERANAN
	(g) Bagi pembangunan menggunakan sumber, pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	
8.25.2	**Kitar Hayat Pembangunan Sistem yang Selamat** Pembangun Sistem hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. Pembangun Sistem perlu melaksanakan penilaian risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: (a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; (b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; (c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; (d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; (e) Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan (f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	Pembangun Sistem Pentadbir Sistem

8.26. KEPERLUAN KESELAMATAN APLIKASI

ID	KETERANGAN	PERANAN
8.26.1	**Melindungi Perkhidmatan Aplikasi dalam Rangkaian Awam** Perkara yang perlu dipertimbangkan ialah seperti yang berikut: (a) Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi jabatan. Contoh perkhidmatan sumber luaran ialah: (i) Perisian Sebagai Satu Perkhidmatan; (ii) Platform Sebagai Satu Perkhidmatan; (iii) Infrastruktur Sebagai Satu Perkhidmatan; (iv) Storan Pengkomputeran Awan; dan (v) Pemantauan Keselamatan. (b) Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala; (c) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan identiti; (d) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi;	Pentadbir Sistem

ID	KETERANGAN	PERANAN
	(e) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan (f) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	
8.26.2	**Melindungi Transaksi Perkhidmatan Aplikasi** Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: (a) Penggunaan tandatangan digital oleh setiap pihak yang terlibat dalam transaksi; (b) Memastikan semua aspek transaksi dipatuhi: (i) Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan; (ii) Mengekalkan kerahsiaan maklumat; (iii) Mengekalkan privasi pihak yang terlibat; dan (iv) Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi;	Pentadbir Sistem Pemilik Maklumat

ID	KETERANGAN	PERANAN
	(v) Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.	
8.26.3	**Keperluan Keselamatan Aplikasi** Spesifikasi reka bentuk perlu mengandungi keperluan keselamatan sistem maklumat. Sekiranya sesuatu produk perisian aplikasi tersedia (*off-the*-shelf) diperoleh, pembekal perlu dimaklumkan berkenaan keperluan keselamatan.	Pentadbir Sistem Pemilik Sistem

8.27. PRINSIP REKA BENTUK DAN KEJURUTERAAN SISTEM YANG SELAMAT

ID	KETERANGAN	PERANAN
8.27.1	**Prinsip Kejuruteraan Sistem yang Selamat** 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 Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam yang terkini.	Pentadbir Sistem Pembangun Sistem
8.27.2	**Prinsip Kejuruteraan Sistem Yang Selamat** Kawalan perubahan kepada perisian perlu dilaksanakan bagi mengurangkan risiko kerosakan pada perisian. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut:	Pentadbir Sistem Pembangun Sistem

ID	KETERANGAN	PERANAN
	(a) Proses pengemaskinian perisian atau sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang diberi tanggungjawab dan mengikut prosedur yang telah ditetapkan; (b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh digunakan selepas diuji dan diluluskan; (c) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; (d) Mengawal capaian ke atas kod atau cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (e) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan (f) Semua sistem konfigurasi perlu didaftar dan didokumenkan.	

8.28. PENGATURCARAAN PROGRAM SELAMAT

ID	KETERANGAN	PERANAN
8.28.1	Kawalan capaian kepada kod sumber Kawalan capaian kepada kod sumber atau atur cara program perlu dilaksanakan bagi mengelakkan kecurian, pengubahsuaian dan penghapusan tanpa kebenaran. Kod sumber bagi semua aplikasi dan perisian ialah hak milik Kerajaan.	Pentadbir Sistem Pembangun Sistem Pengurus Projek

8.29. PENGUJIAN DAN PENERIMAAN KESELAMATAN SISTEM

ID	KETERANGAN	PERANAN
8.29.1	**Pengujian Keselamatan Sistem** Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; (b) Membuat semakan pengesahan dalam aplikasi untuk mengenal pasti kesilapan maklumat; (c) Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan; (d) Melakukan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem; (e) Menjalankan ujian penembusan untuk mengenal pasti kod dan reka bentuk yang tidak selamat; dan (f) Melaksanakan pengujian keselamatan sistem berdasarkan ISO/IEC/IEEE 29119 Software Testing Standard serta garis panduan pengujian keselamatan dan sistem yang sedang berkuat kuasa.	Pentadbir Sistem Penguji Sistem
8.29.2	**Pengujian Penerimaan Sistem** Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk	Pentadbir Sistem Penguji Sistem

ID	KETERANGAN	PERANAN
	sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut: (a) Pengujian penerimaan sistem hendaklah merangkumi keperluan keselamatan sistem maklumat dan kepatuhan kepada polisi pembangunan selamat; (b) Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem diguna pakai; dan (c) Pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian kerentanan (vulnerability assessment).	

8.30. PEMBANGUNAN SISTEM OLEH SUMBER LUAR

ID	KETERANGAN	PERANAN
8.30.1	**Pembangunan oleh Sumber Luar** JDN hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan menggunakan sumber luar seperti pembekal. Kod sumber yang dibangunkan ialah **HAK MILIK KERAJAAN**. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Perjanjian lesen, kod sumber ialah **HAK MILIK KERAJAAN** dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi menggunakan sumber luar;	

ID	KETERANGAN	PERANAN
	(b) Bagi semua perkhidmatan yang disediakan oleh sumber luar, *Software as a Servic*e (SaaS) yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori **Pembekal hendaklah membenar Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko**; (c) Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; (d) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem; (e) Mengguna pakai prinsip dan tatacara eskrow; (f) Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian; (g) Penyediaan model ancaman (threat modelling) untuk dipertimbangkan oleh pembangun sistem serta memastikan tahap keselamatan minimum yang boleh diterima; (h) Peruntukan bukti bahawa ujian yang mencukupi telah digunakan untuk mengawal kehadiran kandungan berniat jahat semasa penghantaran; (i) Peruntukan bukti bahawa ujian yang mencukupi telah digunakan untuk	

ID	KETERANGAN	PERANAN
	melindungi daripada kelemahan yang diketahui; (j) Keperluan keselamatan untuk persekitaran pembangunan; dan (k) Mempertimbangkan perundangan yang berlaku.	

8.31. PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PRODUKSI

ID	KETERANGAN	PERANAN
8.31.1	**Pengasingan Persekitaran Pembangunan, Pengujian dan Produksi** Persekitaran pembangunan, pengujian dan produksi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Perkakasan dan perisian yang digunakan bagi tugas mentakrifkan, mendokumentasikan, membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan daripada perkakasan yang digunakan sebagai produksi. (b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; (c) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat;	Pentadbir Sistem

ID	KETERANGAN	PERANAN
	(d) Menguji perubahan yang dilaksanakan dalam persekitaran ujian atau persekitaran sementara; (e) Tidak menguji dalam persekitaran produksi kecuali dalam keadaan yang telah ditentukan dan diluluskan; (f) Pengkompil, editor dan alat pembangunan atau program utiliti lain yang tidak boleh dicapai daripada sistem pengeluaran apabila tidak diperlukan; dan (g) Memaparkan label yang bersesuaian dengan persekitaran pada menu untuk mengurangkan risiko ralat.	
8.31.2	**Persekitaran Pembangunan Selamat** Pemilik Sistem dan Pembangun Sistem hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. JDN perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: (a) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; (b) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; (c) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;	Pemilik Sistem Pembangun Sistem

ID	KETERANGAN	PERANAN
	(d) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; (e) Pegawai yang bekerja dalam persekitaran pembangunan sistem berintegriti; dan (f) Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	

8.32. PENGURUSAN PERUBAHAN

ID	KETERANGAN	PERANAN
8.32.1	**Pengurusan Perubahan** Perubahan dalam JDN, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara seperti yang berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;	Pentadbir Sistem Pemilik Sistem Pemilik Aset Pemilik Maklumat

ID	KETERANGAN	PERANAN
	(c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja.	
8.32.2	**Prosedur Kawalan Perubahan Sistem** Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan jabatan. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; dan	Pentadbir Sistem

ID	KETERANGAN	PERANAN
	(d) Capaian kepada kod sumber aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja.	
8.32.3	**Kajian Semula Keperluan Teknikal bagi Aplikasi Selepas Perubahan Platform Pengoperasian** Apabila platform pengoperasian berubah, sistem penting hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan JDN. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Pengujian ke atas sistem hendaklah dilaksanakan untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform. (b) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan (c) Memastikan maklumat perubahan tersebut dikemas kini dalam dokumen PKP dan Pelan Pengurusan Maklumat sistem yang berkaitan.	Pemilik Sistem Pentadbir Sistem
8.32.4	**Sekatan Ke atas Perubahan Dalam Pakej Perisian** Pengubahsuaian ke atas pakej perisian tidak digalakkan dan terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	Pentadbir Sistem Pengguna Sistem

8.33. DATA PENGUJIAN

ID	KETERANGAN	PERANAN
8.33.1	**Perlindungan Data Ujian** Untuk memastikan perlindungan ke atas maklumat yang digunakan untuk pengujian, data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi ialah seperti yang berikut: (a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; (b) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; (c) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; (d) Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar; (e) Melindungi maklumat sensitif melalui penyingkiran atau pengaburan data jika digunakan untuk ujian; (f) Memadam maklumat operasi daripada persekitaran ujian serta-merta dengan betul selepas ujian selesai untuk mengelakkan penggunaan maklumat ujian tanpa kebenaran.	Pemilik Maklumat Pemilik Sistem

8.34. PERLINDUNGAN SISTEM MAKLUMAT SEMASA PELAKSANAAN AUDIT

ID	KETERANGAN	PERANAN
8.34.1	**Kawalan Audit Sistem Maklumat** Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas fungsi penyampaian perkhidmatan JDN. Perkara berikut harus dipatuhi: (a) Bersetuju dengan permintaan audit untuk mencapai kepada sistem dan data dengan pengurusan yang sesuai; (b) Bersetuju dan mengawal skop ujian audit teknikal; (c) Mengehadkan ujian audit kepada capaian baca sahaja kepada perisian dan data. Jika capaian baca sahaja tidak tersedia untuk mendapatkan maklumat yang diperlukan, melaksanakan ujian oleh pentadbir berpengalaman yang mempunyai hak capaian yang diperlukan bagi pihak juruaudit; (d) Jika capaian diberikan, mewujudkan dan mengesahkan keperluan keselamatan peranti yang digunakan untuk mengcapaian sistem sebelum membenarkan capaian; (e) Hanya membenarkan capaian selain daripada baca sahaja untuk salinan terpencil fail sistem, memadamkannya apabila audit selesai, atau memberi mereka perlindungan yang sewajarnya jika terdapat kewajiban untuk menyimpan fail tersebut dibawah keperluan dokumentasi audit;	Pemilik Maklumat Pemilik Sistem

ID	KETERANGAN	PERANAN
	(f) Mengenal pasti dan bersetuju dengan permintaan untuk pemprosesan khas atau tambahan, seperti menjalankan alat audit; (g) Menjalankan ujian audit yang boleh menjejaskan ketersediaan sistem di luar waktu perniagaan; (h) Memantau dan mengelog semua capaian untuk tujuan audit dan ujian.	

LAMPIRAN A

KEMENTERIAN DIGITAL
JABATAN DIGITAL NEGARA

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER JABATAN DIGITAL NEGARA

NAMA (HURUF BESAR) :
NO. KAD PENGENALAN :
JAWATAN :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung dalam Polisi Keselamatan Siber Jabatan Digital Negara; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

TANDATANGAN :

TARIKH :

Pengesahan Pegawai Keselamatan ICT

.....
( )
b.p. Ketua Pengarah Jabatan Digital Negara
Tarikh:

NOTA: Tandatangan tidak diperlukan sekiranya perakuan ini dilaksanakan melalui Sistem Akuan Pematuhan Polisi Keselamatan Siber (SPeKS)

LAMPIRAN B

UNDANG-UNDANG, PEKELILING DAN DASAR YANG TERPAKAI

1. Akta Hak Cipta (Pindaan) Tahun 1997;
2. Akta Jenayah Komputer 1997;
3. Akta Komunikasi dan Multimedia 1998;
4. Akta Rahsia Rasmi 1972;
5. Akta Tandatangan Digital 1997;
6. Akta Keselamatan Siber 2024.
7. Arahan Teknologi Maklumat 2007;
8. Arahan Keselamatan;
9. Arahan Perbendaharaan;
10. Pekeliling Am Bilangan 3 Tahun 2000 Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
11. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi- Agensi Kerajaan;
12. Pekeliling Perbendaharaan 5 Tahun 2007 Tatacara Pengurusan Aset Alih Kerajaan (TPA);
13. Pekeliling Perkhidmatan Bil 5 2007 bertajuk Panduan Pengurusan Pejabat bertarikh 30 April 2007;
14. Pekeliling Kemajuan Pentadbiran Awam (PKPA) Bilangan 3 Tahun 2015 Dasar Perkhidmatan Prasarana Kunci Awam Kerajaan [Government Public Key Infrastruktur (GPKI)];
15. Pekeliling Transformasi Pentadbiran Awam Bil.3 Tahun 2017 Pengurusan Komunikasi Bersepadu Kerajaan (Government Unified Communication (1GovUC));
16. Pekeliling Kemajuan Pentadbiran Awam Bil.1 Tahun 2021 Dasar Perkhidmatan Pengkomputeran Awan Sektor Awam;
17. Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam;
18. Pekeliling Am Bilangan 4 Tahun 2022 Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022;
19. Surat Pekeliling Am Bilangan 3 Tahun 2024 Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024;
20. Surat Pekeliling Am Bilangan 4 Tahun 2024 Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024;
21. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan;

22. Surat Arahan Ketua Pengarah MAMPU bertarikh 23 November 2007 Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agensi Kerajaan;
23. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS);
24. Perintah-Perintah Am;
25. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) April 2016;