Kementerian Dalam Negeri
Jabatan Pendaftaran Negara

Polisi Keselamatan Siber

2024

KEMENTERIAN DALAM NEGERI
JABATAN PENDAFTARAN NEGARA

No. 20, Persiaran Perdana, Presint 2,
62551 W.P Putrajaya

MANUAL KESELAMATAN

Tajuk Dokumen :
POLISI KESELAMATAN SIBER

Nombor Dokumen :
JPN-BTM-L1-14

Versi: 3.0

Tarikh : 8 MEI 2024

ISI KANDUNGAN

1.0 PENGENALAN

Polisi Keselamatan Siber Jabatan Pendaftaran Negara (JPN) mengandungi peraturan-peraturan yang **mesti dipatuhi** dalam menggunakan dan melindungi aset teknologi maklumat dan komunikasi (ICT) JPN seperti yang dinyatakan dalam Bidang 1 hingga Bidang 14. Tanggungjawab ini mesti dipikul oleh penjawat awam dan sesiapa yang berkaitan menggunakan aset ICT JPN. Aset ICT dikategori kepada lima (5) elemen iaitu perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia yang mengendalikan aset ICT. Aset ICT terutama data atau maklumat perlu dilindungi kerana ianya tidak ternilai dan Kerajaan telah membuat pelaburan yang besar bagi meningkatkan mutu, kecekapan dan keberkesanan sistem penyampaian perkhidmatan Kerajaan.

2.0 TUJUAN

Polisi ini bertujuan untuk menerangkan peranan dan tanggungjawab pengguna dan semua pihak yang terlibat dalam melindungi aset Kerajaan.

3.0 OBJEKTIF

Objektif Polisi Keselamatan Siber JPN adalah sebagaimana berikut:

a. Menjamin kesinambungan perkhidmatan urusniaga JPN dengan meminimumkan kesan insiden keselamatan;
b. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan aset ICT; dan
c. Mencegah salahguna, kecuaian atau kecurian aset ICT.

4.0 PERNYATAAN POLISI KESELAMATAN SIBER JPN

Polisi Keselamatan Siber JPN mestilah dibaca, diperakui dan dipatuhi oleh setiap kakitangan JPN dan Pihak Ketiga yang mempunyai kepentingan dalam mengendalikan aset ICT JPN.

5.0 SKOP

5.1 Skop Polisi Keselamatan Siber JPN adalah untuk melindungi keselamatan ke atas aset ICT melalui pengendalian ke atas semua perkara berikut:

a. **Perkakasan** - Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan JPN. Contoh: komputer, pelayan, peralatan komunikasi dan sebagainya;

b. **Perisian** - Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada JPN;

c. **Perkhidmatan** - Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsinya:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penyaman udara, sistem pencegah kebakaran dan lain-lain.

d. **Data atau Maklumat** - Koleksi fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat untuk digunakan bagi mencapai misi dan objektif JPN. Contoh: Sistem dokumentasi, prosedur operasi, rekod JPN, profil pelanggan, pangkalan data dan fail data, maklumat arkib dan lain-lain; dan

e. **Manusia** - Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian JPN bagi mencapai visi dan misi jabatan. Individu berkenaan merupakan aset berdasarkan kepada tugas dan fungsi yang dilaksanakan.

5.2 Polisi ini juga adalah saling melengkapi dan perlu dilaksanakan secara konsisten dengan undang-undang dan peraturan yang sedang berkuatkuasa.

6.0 PRINSIP KESELAMATAN

6.1 Prinsip keselamatan adalah sebagaimana berikut:

a. Kerahsiaan
Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

b. Integriti
Data dan maklumat hendaklah tepat, lengkap dan dikemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan; dan

c. Kebolehsediaan
Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

6.2 Bagi mencapai prinsip keselamatan tersebut perkara berikut hendaklah dipatuhi:

a. Prinsip "Perlu-Tahu"

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

b. Hak Keistimewaan Minimum

Hak akses kepada pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu data atau maklumat.

c. Pengasingan Tugas

Prinsip pengasingan bermaksud skop tugas dan tanggungjawab pengguna (seperti mewujud, memadam, mengemaskini dan mengubah data) dan pengesah hendaklah diasingkan supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya. Ia bertujuan untuk mengelak akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran

maklumat terperingkat, dimanipulasi dan seterusnya mengekalkan integriti dan kebolehsediaan.

d. Kawalan Capaian Berdasarkan Peranan

Capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.

e. Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii. Menjaga kerahsiaan kata laluan;

iii. Mematuhi standard, prosedur, langkah dan garis panduan yang ditetapkan;

iv. Memberi perhatian kepada maklumat terperingkat terutama semasa pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

v. Menjaga kerahsiaan daripada diketahui umum.

7.0 PENILAIAN RISIKO

JPN hendaklah mengenal pasti risiko terhadap aset ICT. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan kebolehsediaan maklumat dalam aset ICT. Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran. Pengolahan risiko hendaklah dikenal pasti dan dilaksanakan. Proses penilaian risiko merangkumi perkara-perkara berikut:

a. Kerentanan

Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

b. Ancaman

JPN hendaklah mengenal pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kerentanan yang telah dikenal pasti.

c. Impak

JPN hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi Jabatan. Impak teknikal melibatkan perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti. Impak fungsi Jabatan melibatkan kewangan, reputasi, ketidakpatuhan dan perlanggaran privasi.

d. Tahap Risiko

JPN hendaklah menganggarkan tahap risiko yang ditentukan daripada penemuan ancaman, kebarangkalian dan impak risiko. Kaedah penentuan tahap risiko hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuatkuasa.

e. Pengolahan Risiko

Penilaian risiko keselamatan aset ICT bertujuan membolehkan JPN mengukur, menganalisis tahap risiko aset ICT dan seterusnya mengambil tindakan untuk merancang dan mengawal risiko.

8.0 TADBIR URUS PENGURUSAN RISIKO

JPN hendaklah mengenal pasti struktur tadbir urus pengurusan risiko bagi pelaksanaan perkara berikut:

a. Mengenal pasti kerentanan;
b. Mengenal pasti ancaman;
c. Menilai risiko;
d. Menentukan pengolahan risiko;
e. Memantau keberkesanan pengolahan risiko; dan
f. Memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

9.0 BIDANG POLISI KESELAMATAN SIBER JPN

Polisi Keselamatan Siber JPN terdiri daripada 14 bidang berikut:

BIDANG	TAJUK
1	Pelaksanaan Polisi Keselamatan Siber
2	Organisasi Keselamatan Maklumat
3	Keselamatan Sumber Manusia
4	Pengurusan Aset
5	Kawalan Capaian
6	Kriptografi
7	Keselamatan Fizikal Dan Persekitaran
8	Keselamatan Operasi
9	Keselamatan Komunikasi
10	Perolehan, Pembangunan Dan Penyelenggaraan Sistem
11	Hubungan Dengan Pembekal
12	Pengurusan Pengendalian Insiden Keselamatan
13	Aspek Keselamatan Maklumat Dalam Pengurusan Kesinambungan Perkhidmatan
14	Pematuhan

BIDANG 1: PELAKSANAAN POLISI KESELAMATAN SIBER

1.1 PELAKSANAAN POLISI

OBJEKTIF

Menerangkan pelaksanaan dan sokongan pengurusan terhadap Polisi Keselamatan Siber JPN (PKS) selaras dengan keperluan JPN dan perundangan yang berkaitan.

PERKARA	TANGGUNGJAWAB
Pelaksanaan polisi ini akan dijalankan oleh Ketua Pengarah Pendaftaran Negara (KPPN) selaku Pengerusi Jawatankuasa Pemandu ICT (JPICT). Polisi ini hendaklah dilaksanakan oleh pihak pengurusan JPN.	KPPN, CDO, ICTSO, ICTSM, JPICT, JKICT, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Ketua-ketua Pejabat.
PKS mestilah dibaca, diperakui dan dipatuhi oleh setiap kakitangan JPN dan Pihak Ketiga yang mempunyai kepentingan dalam mengendalikan maklumat JPN.	Kakitangan JPN, Pihak Ketiga.

1.2 PENYEBARAN POLISI

PERKARA	TANGGUNGJAWAB
PKS perlu ditakrif, dilulus, diterbit dan dihebah oleh pihak pengurusan JPN dan disebarkan kepada semua kakitangan JPN serta Pihak Ketiga yang berurusan dengan JPN agar memahami kepentingan keselamatan maklumat JPN.	CDO, ICTSO, Bahagian Dasar dan Pemodenan (BDP), ICTSM, Pengurus Projek ICT.

1.3 PENYELENGGARAAN POLISI

PERKARA	TANGGUNGJAWAB
PKS adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Polisi ini juga hendaklah dibaca bersama dokumen-dokumen mengenai Akta / Pekeliling / Arahan / Peraturan / Garis Panduan dan langkah keselamatan ICT Kerajaan / Prosedur Operasi Standard / Dasar yang dikeluarkan dari semasa ke semasa. Berikut adalah prosedur yang berhubung dengan penyelenggaraan PKS: a. Menyemak polisi ini secara berkala bagi mengenal pasti dan menentukan perubahan yang diperlukan; dan b. Polisi ini hendaklah disemak semula sekurang-kurangnya lima (5) tahun sekali atau mengikut keperluan semasa bagi memastikan dokumen sentiasa dipatuhi.	CDO, ICTSO, ICTSM.

BIDANG 2: ORGANISASI KESELAMATAN MAKLUMAT

2.1 STRUKTUR ORGANISASI KESELAMATAN

OBJEKTIF

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif PKS.

PERKARA	TANGGUNGJAWAB
Ketua Pengarah Pendaftaran Negara (KPPN) Peranan dan tanggungjawab KPPN adalah sebagaimana berikut: a. Menguatkuasakan PKS; b. Memastikan semua keperluan organisasi seperti sumber kewangan, kakitangan dan perlindungan keselamatan adalah mencukupi; c. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan sebagaimana yang ditetapkan di dalam PKS; dan d. Melantik CDO serta memaklumkan pelantikan kepada Ketua Pengarah, Jabatan Digital Negara (JDN).	KPPN.
Ketua Pegawai Digital (CDO) Peranan dan tanggungjawab CDO adalah sebagaimana berikut: a. Melaksana dan menyelaras penggunaan dasar, standard dan amalan terbaik global; b. Memastikan kawalan keselamatan maklumat dalam organisasi diseragam dan diselaraskan dengan sebaiknya; c. Bertanggungjawab ke atas perkara yang berkaitan dengan keselamatan ICT;	CDO.

PERKARA	TANGGUNGJAWAB
d. Mengetuai pasukan JPN *Cyber Security Insiden Response Team* (JPNCSIRT); e. Menentukan keperluan keselamatan ICT; f. Meneraju perubahan melalui penjajaran Pelan Strategik Pendigitalan JPN dengan keperluan Pelan Strategik Kementerian dan Pelan Strategik Sektor Awam; g. Menyelaras penggalakan pembudayaan ICT, dan Inovasi Pendigitalan dalam Sistem Penyampaian JPN dan Perkhidmatan Awam; h. Melantik ICTSO serta memaklumkan pelantikan kepada JDN dan NACSA; dan i. Memastikan kakitangan JPN dan Pihak Ketiga memahami dan mematuhi peruntukan di bawah PKS.	
Pegawai Keselamatan ICT (ICTSO) Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Memastikan kajian dan semakan semula serta pelaksanaan standard keselamatan ICT selaras dengan keperluan organisasi; b. Menguatkuasa PKS kepada semua kakitangan JPN dan Pihak Ketiga; c. Menjalankan pengurusan risiko dan audit keselamatan ICT berpandukan peraturan dan garis panduan yang berkuatkuasa; d. Menyedia dan menyebarkan panduan yang sesuai berkaitan keselamatan ICT dan memberikan khidmat nasihat serta	ICTSO.

PERKARA	TANGGUNGJAWAB
menyediakan langkah-langkah perlindungan yang bersesuaian; e. Mengurus pasukan JPN *Cyber Security Insiden Response Team* (JPNCSIRT); f. Melaporkan insiden keselamatan ICT kepada KDNCSIRT dalam membantu penyiasatan atau pemulihan; g. Melaporkan insiden keselamatan ICT kepada CDO bagi insiden yang memerlukan pengaktifan Pelan *Disaster Recovery Plan* (DRP) yang terkandung di dalam Pelan Pengurusan Kesinambungan Perkhidmatan (PKP) JPN; h. Menguruskan keseluruhan program keselamatan ICT organisasi; i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah baik pulih dengan segera; j. Melaksanakan pematuhan PKS oleh kakitangan JPN dan Pihak Ketiga; k. Menyemak laporan berkaitan dengan isu-isu keselamatan ICT; dan l. Memastikan pelaksanaan latihan dan program kesedaran keselamatan ICT dari semasa ke semasa.	
Pengurus Keselamatan ICT (ICTSM) Peranan dan tanggungjawab ICTSM yang dilantik adalah seperti berikut:	ICTSM.

PERKARA	TANGGUNGJAWAB
a. Membantu ICTSO dalam mengurus keselamatan ICT JPN dan pasukan JPNCSIRT; b. Membantu ICTSO menjalankan pengurusan risiko dan audit keselamatan ICT berpandukan peraturan serta garis panduan yang berkuatkuasa; c. Memberi penerangan dan pendedahan berkenaan PKS kepada semua pengguna; d. Menyedia dan melaksanakan latihan dan program kesedaran keselamatan ICT dari semasa ke semasa; e. Menyelaras penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden yang sama dapat dielakkan; f. Melaporkan sebarang insiden atau penemuan mengenai keselamatan ICT kepada ICTSO untuk tindakan; g. Memastikan rekod bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT didokumenkan; dan h. Mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT.	
PENGARAH BAHAGIAN / PENGARAH NEGERI Peranan dan tanggungjawab adalah sebagaimana berikut: a. Melaksana dan memastikan semua kakitangan JPN dan Pihak Ketiga mematuhi PKS / Akta / Pekeliling / Arahan / Peraturan / Garis Panduan / Prosedur Operasi Standard (SOP) / Dasar yang sedang berkuatkuasa;	Pengarah Bahagian/Negeri.

PERKARA	TANGGUNGJAWAB
b. Menentukan pengguna dan kategori atau tahap capaian pengguna sistem; c. Memastikan semua keperluan organisasi seperti sumber kewangan, sistem dan aset ICT, kakitangan JPN dan perlindungan keselamatan adalah di tahap optimum; d. Menyebarkan amaran yang sesuai terhadap kemungkinan berlaku ancaman keselamatan ICT dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; e. Melaporkan insiden keselamatan ICT kepada *Helpdesk* dan ICTSO dengan kadar segera dan seterusnya membantu dalam penyiasatan atau pemulihan; f. Menyedia dan melaksanakan program kesedaran keselamatan ICT kepada kakitangan dalam melaksanakan tugas dan tanggungjawab; g. Mengurus, menyelaras dan memantau semua perjanjian di bawah tanggungjawabnya dan memastikan Pihak Ketiga berkaitan menjalani tapisan keselamatan; h. Melaksanakan promosi, penguatkuasaan dan pemantauan penggunaan sistem secara berterusan kepada pengguna sasaran; dan i. Memberi perakuan tindakan tatatertib ke atas pengguna yang melanggar PKS / Akta / Pekeliling / Arahan / Peraturan / Garis Panduan / Prosedur Operasi Standard (SOP) / Dasar yang sedang berkuatkuasa.	

PERKARA	TANGGUNGJAWAB
PENGURUS PROJEK ICT Peranan dan tanggungjawab adalah seperti berikut: a. Membangun Pelan Pengurusan Keselamatan Maklumat selaras dengan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA); b. Memastikan projek ICT dilaksanakan selaras dengan keperluan keselamatan ICT JPN; c. Mewujud dan mengkaji semula garis panduan, prosedur dan tatacara selaras dengan PKS / Akta / Pekeliling / Arahan / Peraturan / Garis Panduan yang sedang berkuatkuasa; d. Melaksana pengurusan risiko, audit keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT; e. Memastikan pembekal dan rakan usahasama memohon tapisan keselamatan dan memperaku PKS; f. Melapor sebarang insiden atau penemuan mengenai keselamatan ICT kepada ICTSM dan ICTSO; dan g. Memastikan penyimpanan rekod bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT didokumenkan.	Pengurus Projek ICT.
PENTADBIR SISTEM Peranan dan tanggungjawab Pentadbir Sistem adalah seperti berikut: a. Membangun Pelan Pengurusan Keselamatan Maklumat (ISMP) selaras dengan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA);	Pentadbir Sistem.

PERKARA	TANGGUNGJAWAB
b. Memastikan projek ICT dilaksanakan selaras dengan keperluan keselamatan ICT JPN; c. Memastikan segala data dan maklumat di dalam sistem adalah tepat, lengkap dan boleh dipercayai; d. Memahami dan mematuhi PKS dan sebarang prosedur berkaitan dalam mewujudkan akaun pengguna ke atas setiap sistem; e. Menjaga kerahsiaan data, katalaluan dan konfigurasi aset ICT; f. Mengambil tindakan pengemaskinian atau pembatalan akaun pengguna dengan segera apabila dimaklumkan pengguna tersebut bertukar bidang tugas kerja / bertukar keluar Jabatan / bersara / ditamatkan perkhidmatan / dalam prosiding dan / atau dikenakan tindakan tatatertib / bercuti atau berkursus panjang / meninggal dunia; g. Memastikan pemantauan dilaksanakan ke atas sistem dan rangkaian agar berjalan lancar / beroperasi sepanjang masa; h. Mengenal pasti aktiviti tidak normal pada sistem dan rangkaian seperti cubaan menggodam, pencerobohan, dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; i. Menganalisis dan menyimpan rekod jejak audit (mengikut keperluan); j. Memastikan sistem mempunyai tempoh masa aktif dan tamat selepas melebihi tempoh *idle* yang ditetapkan;	

PERKARA	TANGGUNGJAWAB
k. Menghadkan capaian dokumentasi bagi mengelakkan dari penyalahgunaannya; l. Mengemaskini *patches* yang bersesuaian supaya terhindar daripada ancaman virus dan penggodam; m. Memastikan kod-kod program sistem adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaannya; n. Memastikan *backup* sistem aplikasi, data, konfigurasi dan rangkaian yang berkaitan dengannya dibuat secara berjadual; o. Mengenal pasti isu-isu keselamatan yang akan timbul dalam proses kerja dan mencadangkan pengurusan perubahan; dan p. Melaporkan kepada *Helpdesk* dan ICTSO dengan segera jika berlaku insiden keselamatan ke atas sistem di bawah pentadbirannya.	
Jawatankuasa Pemandu ICT (JPICT) Peranan dan tanggungjawab JPICT seperti di dalam Surat Pekeliling Am Bil 3 Tahun 2015 adalah merancang dan menentukan langkah-langkah keselamatan ICT.	JPICT.
Jawatankuasa Keselamatan ICT (JKICT) Peranan dan tanggungjawab JKICT adalah seperti berikut : a. Merancang dan memantau Dasar, Strategi dan Pelan Tindakan infrastruktur dan Keselamatan ICT b. Merancang, mencadang pengemaskinian dan memantau pelaksanaan Polisi Keselamatan Siber (PKS)	JKICT.

PERKARA	TANGGUNGJAWAB
c. Merancang dan memantau perolehan infrastruktur, perkakasan, aplikasi dan perisian Keselamatan ICT d. Merancang Program Keselamatan ICT e. Menyelaras dan memantau Rangkaian Komunikasi dan Sistem E-Mel f. Menyelaras dan memantau Pelaksanaan Keselamatan ICT g. Melapor perancangan, Status Pelaksanaan dan Pemantauan serta sebagai Penasihat Keselamatan ICT kepada Jawatankuasa Pemandu ICT (JPICT) Ahli-ahli : 1. ICTSO 2. KPP 3. PPK 4. PP	
JPN *CYBER SECURITY INCIDENT RESPONSE TEAM* (JPNCSIRT) Keanggotaan JPNCSIRT adalah seperti berikut: i. Pengarah CSIRT : CDO ii. Pengurus CSIRT I : ICTSO iii. Pengurus CSIRT II: ICTSM <u>Ahli</u> i. Timbalan Pengarah Kanan BTM ii. Timbalan Pengarah BTM iii. Ketua Penolong Pengarah BTM iv. Pentadbir Rangkaian dan Keselamatan Rangkaian v. Pentadbir Portal vi. Pentadbir Pangkalan Data	JPNCSIRT.

PERKARA	TANGGUNGJAWAB
vii. Pentadbir Aplikasi viii. Pentadbir Pusat Data & Pusat Pemulihan Bencana ix. Pentadbir Server dan *Helpdesk* x. Urusetia Peranan dan tanggungjawab JPNCSIRT adalah seperti berikut: a. Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; b. Merekod dan menjalankan siasatan awal insiden yang diterima; c. Menangani tindak balas insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d. Menasihati Bahagian / Negeri mengambil tindakan pemulihan dan pengukuhan; dan e. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT.	
MEJA BANTUAN ICT (*HELPDESK*) Peranan dan tanggungjawab Meja Bantuan ICT adalah sebagaimana berikut : a. Menerima aduan daripada pengguna berkaitan masalah ICT yang dihadapi; b. Perkhidmatan bantuan peringkat pertama bagi sebarang masalah ICT; dan c. Menyalurkan aduan yang telah dilaporkan kepada pegawai bertanggungjawab untuk penyelesaian.	Meja Bantuan ICT (*Helpdesk*).

PERKARA	TANGGUNGJAWAB
PENGGUNA Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi PKS; b. Bersetuju dan memperaku PKS; c. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; d. Lulus tapisan keselamatan; e. Melaksanakan tugasan mengikut PKS / Akta / Pekeliling / Arahan / Peraturan / Garis Panduan / Prosedur Operasi Standard (SOP) / Dasar yang sedang berkuatkuasa; f. Menjaga kerahsiaan maklumat JPN; g. Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan,	Pengguna.

PERKARA	TANGGUNGJAWAB
pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; vii. Menjaga kerahsiaan bagi setiap langkah-langkah keselamatan ICT dari diketahui umum; viii. Melaporkan aktiviti yang mengancam keselamatan ICT seperti *Denial-Of-Service* (DOS), *Distributed Denial-Of-Service* (DDoS), Pencerobohan (*Intrusion*), Jangkitan Perisian Hasad (*Malicious Software/Malware*), Pengehosan Perisian Hasad (*Malware Hosting*), Percubaan Pencerobohan (*Intrusion Attempt*), Potensi Serangan (*Potential Attack*) kepada Pentadbir Sistem dengan segera; ix. Selain perkara viii di atas perlu dilaporkan kepada Meja Bantuan (*Helpdesk*) Jabatan; x. Memaklumkan kepada pihak Pentadbir Sistem yang berkaitan dengan kadar segera bagi mengemaskini akaun pengguna apabila berlaku perubahan peranan seperti bertukar, bercuti dan berhenti/bersara; xi. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan xii. Menandatangani Perakuan PKS di **Lampiran 1**.	
PIHAK KETIGA Peranan dan tanggungjawab Pihak Ketiga yang menggunakan dan / atau mengendalikan aset ICT JPN adalah seperti berikut:	Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber JPN; b. Bersetuju dan menandatangani Perakuan PKS di **Lampiran 1**; c. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; d. Membuat permohonan / telah mendapatkan kelulusan tapisan keselamatan; e. Memahami dengan jelas syarat keselamatan dalam perjanjian dengan pihak JPN. Perkara-perkara berikut termasuk di dalam perjanjian yang dimeterai: i. PKS; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. f. Mematuhi Akta / Pekeliling / Arahan / Peraturan / Garis Panduan / Prosedur Operasi Standard (SOP) / Dasar yang sedang berkuatkuasa; g. Akses kepada aset ICT JPN perlu berlandaskan kepada perjanjian kontrak; h. Memaklumkan kepada Pengurus Projek ICT dengan kadar segera apabila berlaku perubahan peranan dengan : i. Memulangkan Pas Vendor (jika ada) ii. Membatalkan ID i. Menjaga kerahsiaan maklumat JPN.	

2.2 PENGASINGAN TUGAS

OBJEKTIF

Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah, atau menyalahgunakan aset organisasi.

PERKARA	TANGGUNGJAWAB
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset ICT. Perkara yang perlu dipatuhi adalah seperti berikut: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. 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; dan c. Tugas yang kritikal hendaklah diasingkan dan tugas tersebut tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.	CDO, ICTSO, ICTSM, Pentadbir Sistem.

2.3 HUBUNGAN DENGAN PIHAK BERKUASA

OBJEKTIF

Hubungan yang baik dengan pihak berkuasa yang berkaitan hendaklah dikekalkan.

PERKARA	TANGGUNGJAWAB
Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Hendaklah mewujudkan dan mengemaskini senarai pihak berkuasa perundangan/pihak yang boleh dihubungi semasa kecemasan seperti Polis Diraja Malaysia, Suruhanjaya Komunikasi dan Multimedia, pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, pihak keselamatan, pihak kesihatan dan bomba.	CDO, ICTSO, ICTSM, Pentadbir Sistem.

2.4 HUBUNGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS

OBJEKTIF

Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan persatuan/pertubuhan profesional yang lain hendaklah dikekalkan.

PERKARA	TANGGUNGJAWAB
Hubungan yang baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau forum adalah bagi: a. Meningkatkan ilmu berkenaan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;	CDO, ICTSO, ICTSM, Pentadbir Sistem.

b.	Menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini;	
c.	Berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan	
d.	Berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	

BIDANG 3: KESELAMATAN SUMBER MANUSIA

3.1 SEBELUM PERKHIDMATAN

OBJEKTIF

Memastikan kakitangan JPN dan Pihak Ketiga memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.

3.1.1 TAPISAN KESELAMATAN

PERKARA	TANGGUNGJAWAB
Ketua Jabatan bertanggungjawab menjalankan tapisan keselamatan terhadap kakitangan JPN dan Pihak Ketiga yang mempunyai urusan dengan perkhidmatan ICT JPN yang terlibat berasaskan kepada keperluan perundangan, peraturan dan etika terpakai selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Pengarah Bahagian/Negeri, Pengarah Sumber Manusia, Pengurus Projek ICT.

3.1.2 TERMA DAN SYARAT PERKHIDMATAN

PERKARA	TANGGUNGJAWAB
Perkara yang mesti dipatuhi adalah: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab kakitangan JPN dan Pihak Ketiga dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan b. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian / prosedur yang telah ditetapkan.	Pengarah Bahagian/Negeri, Kakitangan JPN, Pihak Ketiga.

3.2 DALAM PERKHIDMATAN

OBJEKTIF

Memastikan kakitangan JPN dan Pihak Ketiga peka dan faham terhadap ancaman keselamatan maklumat, mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pihak yang terlibat hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuatkuasa.

3.2.1 TANGGUNGJAWAB PENGURUSAN

PERKARA	TANGGUNGJAWAB
a. Pengurusan hendaklah memastikan kakitangan JPN dan Pihak Ketiga mematuhi Perundangan, Arahan, Peraturan dan Prosedur Jabatan yang berkuatkuasa; dan b. Pengurusan hendaklah memastikan kakitangan JPN dan Pihak Ketiga mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh JPN.	Pengarah Bahagian/Negeri, Kakitangan JPN, Pihak Ketiga.

3.2.2 KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT

PERKARA	TANGGUNGJAWAB
a. Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber JPN, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk / fungsi / aplikasi / sistem keselamatan secara berterusan dalam melaksanakan tugas dan tanggungjawab; b. Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber JPN perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;	Pengarah Bahagian/Negeri, Kakitangan JPN, Pihak Ketiga.

c. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	

3.2.3 PROSES TATATERTIB

PERKARA	TANGGUNGJAWAB
a. Memastikan adanya proses tindakan tatatertib dan / atau undang-undang ke atas kakitangan JPN dan Pihak Ketiga sekiranya berlaku perlanggaran Akta / Pekeliling / Arahan / Peraturan / Garis Panduan yang sedang berkuatkuasa. Jika disabitkan kesalahan boleh dikenakan hukuman; dan b. Kakitangan JPN dan Pihak Ketiga yang melanggar polisi ini juga boleh digantung daripada mendapat capaian kepada kemudahan ICT JPN.	Ketua Unit Integriti, Pengarah Bahagian/Negeri, Pengarah Sumber Manusia, Kakitangan JPN, Pihak Ketiga.

3.3 PENAMATAN ATAU PERTUKARAN PERKHIDMATAN

OBJEKTIF

Memelihara kepentingan keselamatan ICT Jabatan dengan memastikan pertukaran, penamatan perkhidmatan dan perubahan bidang tugas kakitangan JPN dan Pihak Ketiga diurus dengan teratur.

3.3.1 TANGGUNGJAWAB APABILA PENAMATAN ATAU PERTUKARAN PERKHIDMATAN

PERKARA	TANGGUNGJAWAB
Perkara yang perlu dipatuhi adalah seperti berikut: a. Pekeliling berkaitan penamatan atau pertukaran perkhidmatan; b. Memastikan semua aset ICT dikembalikan	Pengarah Bahagian/Negeri, Pengarah Sumber Manusia, Kakitangan JPN, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
kepada JPN mengikut peraturan dan terma perkhidmatan yang ditetapkan; c. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan JPN dan/atau terma perkhidmatan yang ditetapkan; d. Maklumat rasmi JPN dalam peranti tidak dibenarkan dibawa keluar dari JPN. e. Memastikan Pas Keselamatan Jabatan kakitangan JPN dan Pihak Ketiga yang terlibat dikembalikan ke Bahagian Sumber Manusia; dan f. Menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada Penyelia yang berkaitan (bagi kakitangan JPN).	

BIDANG 4: PENGURUSAN ASET

4.1 TANGGUNGJAWAB TERHADAP ASET

OBJEKTIF

Setiap aset ICT perlu dikenal pasti, diklasifikasi, direkodkan, diselenggara, dan dilupuskan apabila tiba masanya berdasarkan kepada tatacara/arahan/peraturan pengurusan aset yang berkuatkuasa dari semasa ke semasa. Ini adalah untuk memberikan perlindungan keselamatan yang bersesuaian kepada semua aset ICT.

4.1.1 PENDAFTARAN ASET

PERKARA	TANGGUNGJAWAB
Tanggungjawab yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset ICT dikenal pasti, diklasifikasi, didaftar, dilabel dan didokumen. Maklumat aset direkod dan dikemas kini dengan mematuhi arahan dan peraturan yang berkuatkuasa dari semasa ke semasa; b. Pegawai aset hendaklah memastikan semua aset ICT didaftarkan, dilabel dan dilekatkan di tempat yang mudah dilihat. c. Mengenal pasti Pegawai Penerima Aset Bahagian / Negeri / Cawangan untuk menguruskan penerimaan aset ICT bagi projek ICT; dan d. Pegawai Aset Bahagian / Negeri / Cawangan yang dilantik perlu memastikan semua aset ICT mempunyai pemilik dan lokasi penempatan sebenar dan dikendalikan oleh kakitangan JPN yang dibenarkan sahaja.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Ketua Pejabat, Pegawai Aset, Pemilik Aset, Pembantu Pegawai Aset, Pihak Ketiga.

4.1.2 PENYIMPANAN DAN PENEMPATAN ASET

PERKARA	TANGGUNGJAWAB
Tanggungjawab yang perlu dipatuhi adalah sebagaimana berikut: a. Kakitangan JPN adalah bertanggungjawab ke atas aset ICT dan maklumat di bawah kawalannya dan hendaklah digunakan untuk tujuan rasmi sahaja; b. Kakitangan JPN hendaklah mengesahkan penempatan aset ICT dan memastikan dimasukkan dalam senarai aset; c. Semua aset ICT yang disewa hendaklah diuruskan dengan baik oleh kakitangan JPN; d. Kakitangan JPN hendaklah memastikan semua aset ICT yang didaftarkan dilabel dan dilekatkan di tempat yang mudah dilihat; e. Kakitangan JPN tidak dibenarkan mengubah kedudukan aset ICT dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset; f. Kakitangan JPN perlu memaklumkan perubahan maklumat penempatan dan pemilik kepada Pegawai Aset dengan kadar segera untuk pengemaskinian rekod; g. Aset ICT yang hendak dibawa keluar dari premis perlulah mendapat kelulusan Pegawai Aset dan direkodkan; h. Aset ICT hendaklah disimpan di tempat yang selamat dan sentiasa di bawah kawalan pegawai yang bertanggungjawab. Arahan Keselamatan Kerajaan hendaklah sentiasa dipatuhi bagi mengelakkan berlakunya kerosakan atau kehilangan Aset ICT; dan	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Ketua Pejabat, Pegawai Aset, Pemilik Aset, Pihak Ketiga.

i. Setiap pegawai penempatan atau pegawai yang menggunakan Aset ICT tersebut adalah bertanggungjawab terhadap apa-apa kekurangan, kerosakan atau kehilangan Aset ICT di bawah tanggungjawabnya.	

4.1.3 PENERIMAAN DAN PENGGUNAAN ASET

PERKARA	TANGGUNGJAWAB
Memastikan semua pekelililing dan prosedur pengurusan aset ICT dikenal pasti, didokumenkan dan dilaksanakan.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Ketua Pejabat, Pegawai Aset, Pembantu Pegawai Aset, Pegawai Penerima Aset, Pemilik Aset, Pihak Ketiga.

4.1.4 PEMULANGAN ASET

PERKARA	TANGGUNGJAWAB
Memastikan semua aset ICT dikembalikan kepada JPN mengikut pekeliling dan peraturan yang berkuatkuasa serta terma perkhidmatan yang ditetapkan sebelum bertukar Jabatan, bersara dan penamatan perkhidmatan atau kontrak.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Ketua Pejabat, Pegawai Aset, Pembantu Pegawai Aset, Pemilik Aset, Pihak Ketiga.

4.1.5 PELUPUSAN ASET

PERKARA	TANGGUNGJAWAB
a. Memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan. b. Memastikan tidak menyimpan Aset ICT yang tidak boleh digunakan atau tidak diperlukan	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Ketua Pejabat, Pegawai Aset, Pegawai Perakuan Pelupusan (PEP), Pembantu Pegawai Aset, Pembantu Pelupusan Aset, Pemilik Aset, Pihak Ketiga.

4.2 KLASIFIKASI MAKLUMAT

OBJEKTIF

Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

4.2.1 PENGELASAN MAKLUMAT

PERKARA	TANGGUNGJAWAB
Maklumat hendaklah dikelaskan oleh Pegawai Pengelas seperti yang ditetapkan di dalam dokumen Arahan Keselamatan berasaskan nilai, perundangan, tahap sensitiviti dan tahap kritikal kepada JPN.	Pegawai Pengelas, Kakitangan JPN.

4.2.2 PENGHAPUSAN MAKLUMAT

PERKARA	TANGGUNGJAWAB
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah bagi kategori fizikal hendaklah mengambil kira langkah-langkah keselamatan berikut: a. Maklumat terperingkat JPN yang disimpan secara fizikal tidak boleh disimpan melebihi tempoh yang ditetapkan. b. Maklumat terperingkat JPN hendaklah dilupuskan dengan kaedah yang selamat apabila tidak lagi diperlukan merujuk kepada tatacara pelupusan Kerajaan yang sedang berkuatkuasa. Ini adalah untuk mengelakkan daripada pendedahan maklumat rasmi Kerajaan dan maklumat sensitif seperti Privacy Information Identification (PII) kepada pihak yang tidak dibenarkan. c. Maklumat terperingkat JPN yang disimpan secara elektronik seperti cakera padat, *thumbdrive*, *tape* dan sebagainya hendaklah dimusnahkan dengan kaedah yang selamat apabila tidak lagi diperlukan mengikut tatacara pelupusan Kerajaan yang sedang berkuatkuasa. Ini adalah untuk mengelakkan daripada pendedahan maklumat rasmi Kerajaan dan maklumat sensitif seperti PII kepada pihak yang tidak dibenarkan. d. JPN hendaklah memastikan rekod pelupusan disimpan sebagai bukti.	Bahagian Pentadbiran, JPN Unit Aset, BTM Unit Pentadbiran Bahagian Kakitangan JPN

4.2.3 PELABELAN MAKLUMAT

PERKARA	TANGGUNGJAWAB
Prosedur pelabelan peringkat keselamatan pada maklumat hendaklah dipatuhi mengikut Arahan Keselamatan.	Pegawai Pengelas, Kakitangan JPN.

4.2.4 PENGENDALIAN ASET

PERKARA	TANGGUNGJAWAB
Aktiviti pengendalian maklumat hendaklah mengambil kira langkah-langkah keselamatan berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah-langkah dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan merujuk kepada Pekeliling dan Peraturan-Peraturan semasa yang berkuat kuasa; dan g. Menjaga kerahsiaan keselamatan maklumat ICT dari didedahkan dan diketahui umum.	Pengarah Bahagian/Negeri, Kakitangan JPN, Pihak Ketiga.

4.3 PENGENDALIAN MEDIA

OBJEKTIF

Melindungi maklumat dalam media storan dari sebarang pendedahan, pengubahsuaian, pemindahan dan pemusnahan.

4.3.1 PENGURUSAN MEDIA MUDAH ALIH

PERKARA	TANGGUNGJAWAB
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah sebagaimana berikut: a. Prosedur pengurusan media mudah alih hendaklah dilaksanakan mengikut Arahan Keselamatan; b. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; c. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; d. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; e. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan f. Menyimpan semua media di tempat yang selamat.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Kakitangan JPN.

4.3.2 PELUPUSAN MEDIA

PERKARA	TANGGUNGJAWAB
Prosedur-prosedur pelupusan media yang perlu dipatuhi adalah sebagaimana berikut: a. Media yang mengandungi maklumat terperingkat yang perlu dihapuskan atau dimusnahkan hendaklah mengikut sebagaimana prosedur yang berkuatkuasa; b. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa; dan c. Pelupusan media perlu dilaksanakan berdasarkan Garis Panduan Pengurusan Rekod Elektronik Arkib Negara.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pegawai Aset, Pembantu Pegawai Aset, Pembantu Pelupusan Aset, Pegawai IT Negeri, Kakitangan JPN.

4.3.3 PEMINDAHAN MEDIA FIZIKAL

PERKARA	TANGGUNGJAWAB
Prosedur-prosedur pemindahan media fizikal yang perlu dipatuhi adalah sebagaimana berikut: a. Setiap pergerakan media keluar dan masuk pejabat-pejabat JPN perlu direkodkan secara teratur; b. Memastikan media yang mengandungi maklumat dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan; c. Penyingkiran / pemadaman maklumat dalam media hendaklah dilaksanakan mengikut prosedur dan polisi yang ditetapkan;	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pegawai Aset, Pembantu Pegawai Aset, Pembantu Pelupusan Aset, IT Negeri, Kakitangan JPN.

PERKARA	TANGGUNGJAWAB
d. Langkah keselamatan perlu diambil kira semasa pemindahan media dilaksanakan melalui Pihak Ketiga seperti pos / kurier; dan e. Langkah yang sesuai perlu dilaksanakan untuk melindungi media yang disimpan di luar premis JPN atau tempat awam.	

4.4 PENCEGAHAN KETIRISAN DATA

OBJEKTIF
Memastikan data dan maklumat dikawal dan dilindungi daripada risiko ketirisan data dan maklumat, penyalahgunaan dan kehilangan integriti.

PERKARA	TANGGUNGJAWAB
JPN hendaklah mempertimbangkan perkara berikut bagi mengurangkan risiko ketirisan data dan maklumat. a. Mengenal pasti dan mengkelaskan maklumat sensitif untuk melindunginya daripada ketirisan pada sistem, storan, media, rangkaian dan *end-point devices* (perkakasan dan peralatan fizikal dan *virtual* yang bersambung kepada rangkaian bagi perkongsian data dan maklumat) seperti *serve*r, komputer, laptop , pencetak, mesin penyalin, *tablet*, telefon bimbit dan sebagainya. b. Memantau saluran-saluran ketirisan data JPN seperti e-mel, pemindahan fail, peranti mudah alih dan peranti storan mudah alih. Pemantauan dan menghadkan kebolehan pengguna daripada menyalin, menampal dan memuat naik maklumat sensitif ke atas perkhidmatan, peralatan atau storan di luar JPN boleh dilakukan dengan menggunakan perisian khusus yang sesuai. c. Melaksanakan program kesedaran kepada warga JPN sebagai langkah pencegahan bagi ketirisan data.	KPPN, CDO, ICTSO, ICTSM, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna

BIDANG 5: KAWALAN CAPAIAN

5.1 KAWALAN CAPAIAN

OBJEKTIF

Mengehadkan capaian ke atas data dan maklumat, kemudahan pemprosesan maklumat dan proses-proses utama dalam teras perkhidmatan dan perlu dikawal mengikut ketetapan yang ditentukan oleh pengurusan, pemilik data, proses, operasi atau sistem.

5.1.1 PENGURUSAN KAWALAN CAPAIAN

PERKARA	TANGGUNGJAWAB
Capaian kepada data, proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi tugas pengguna. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemaskini dan menyokong kawalan capaian sedia ada. Perkara-perkara yang perlu dipatuhi adalah sebagaimana berikut: a. Kawalan ke atas kemudahan pemprosesan maklumat; b. Pengasingan peranan kawalan capaian; c. Kebenaran rasmi capaian; d. Semakan hak capaian berkala; e. Pembatalan hak capaian; f. Arkib semua aktiviti berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat pengguna;	CDO, Timbalan Ketua Pengarah (Operasi), ICTSO, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
g. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; h. Kawalan capaian ke atas perkhidmatan internet; i. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan j. Undang-undang, Akta, Pekeliling, Peraturan dan Arahan Jabatan yang berkaitan.	

5.1.2 CAPAIAN KEPADA RANGKAIAN DAN PERKHIDMATAN RANGKAIAN

PERKARA	TANGGUNGJAWAB
Capaian ke rangkaian dan perkhidmatan rangkaian hendaklah mendapat kebenaran daripada ICTSO dan ICTSM. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menghadkan capaian di antara rangkaian JPN, rangkaian agensi lain dan rangkaian awam; b. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; dan c. Mewujud, menguatkuasa dan memantau mekanisme untuk pengesahan ID pengguna, kata laluan atau peralatan ICT yang dihubungkan ke rangkaian termasuk rangkaian tanpa wayar.	CDO, ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Sistem

5.2 PENGURUSAN CAPAIAN PENGGUNA

OBJEKTIF

Menguruskan capaian pengguna terhadap sistem, perkhidmatan dan aset ICT.

5.2.1 PENGURUSAN AKAUN PENGGUNA

PERKARA	TANGGUNGJAWAB
Akaun pengguna adalah unik dan mencerminkan identiti pengguna. Pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan akaun dibuat. Pemilikan akaun dan capaian pengguna adalah tertakluk kepada peraturan Jabatan dan tindakan pendaftaran, pengemaskinian dan / atau pembatalan hendaklah dilaksanakan sebagaimana berikut: a. Pendaftaran dan penamatan akaun pengguna hendaklah menggunakan kaedah dan garis panduan yang ditetapkan; b. Akaun pengguna yang diperuntukkan oleh Jabatan hendaklah digunakan untuk tujuan rasmi; c. Akaun pengguna luar yang diwujudkan hendaklah diberi tahap capaian dan tempoh masa mengikut peranan dan tanggungjawab pengguna dan dengan kelulusan pegawai pelulus; dan d. Tindakan pengemaskinian atau pembatalan akaun hendaklah dilaksanakan apabila: i. Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh Ketua Jabatan; ii. Pengguna yang bercuti belajar melebihi tempoh tiga (3) bulan sebagaimana	ICTSO, Pengarah Bahagian/Negeri, Pengarah Sumber Manusia, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

PERKARA	TANGGUNGJAWAB
yang diluluskan oleh Ketua Jabatan; iii. Pertukaran bidang tugas kerja; iv. Bertukar keluar Jabatan; v. Bersara; vi. Ditamatkan perkhidmatan; vii. Dalam prosiding dan/atau dikenakan tindakan tatatertib; viii. Meninggal dunia; ix. Pengguna bercuti melebihi satu tempoh yang diluluskan oleh Ketua Jabatan atau mana-mana pihak yang berautoriti (contoh Pegawai Perubatan); dan x. Tamat kontrak untuk pihak ketiga	

5.2.2 PENGURUSAN HAK CAPAIAN PENGGUNA

PERKARA	TANGGUNGJAWAB
a. Pengarah Bahagian / Negeri dan Penyelia hendaklah memastikan penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan skop tugas kakitangan di bawah seliaan; b. Pengarah Bahagian / Negeri hendaklah mewujudkan prosedur hak capaian atau pembatalan ke atas sistem JPN berdasarkan peranan dan bidang tugas; c. Penggunaan akaun milik orang lain atau akaun yang dikongsi adalah dilarang;	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

PERKARA	TANGGUNGJAWAB
d. Pengarah Bahagian / Negeri dan penyelia hendaklah memastikan hak akses kakitangan seliaan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat ke atas sistem JPN hendaklah dibatalkan/dikemaskini sekiranya terdapat perubahan bidang tugas seperti bertukar skop, bertukar Jabatan dan penamatan perkhidmatan; dan e. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan Jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan.	

5.3 TANGGUNGJAWAB PENGGUNA

OBJEKTIF

Memastikan pengguna bertanggungjawab menghalang penyalahgunaan, kecurian maklumat dan melindungi maklumat pengesahan diri.

PERKARA	TANGGUNGJAWAB
Perkara-perkara yang perlu dipatuhi sebagaimana berikut: a. Membaca, memahami dan mematuhi Polisi Keselamatan Siber JPN; b. Menjaga kerahsiaan dan melaksanakan langkah-langkah perlindungan maklumat; c. Memahami implikasi keselamatan ICT dan kesan dari tindakannya; d. Mematuhi amalan *clear desk* dan *clear screen policy;* dan e. Menandatangani borang perakuan PKS.	ICTSO, ICTSM, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Penyelia, Pengguna, Pihak Ketiga.

5.3.1 PENGURUSAN KATA LALUAN

PERKARA	TANGGUNGJAWAB
Memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan pemprosesan maklumat. Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan berdasarkan garis panduan yang telah ditetapkan: a. Kata laluan hendaklah diingat dan tidak boleh dikongsi, dicatat, disimpan atau didedahkan; b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan; c. Kata laluan hendaklah berlainan dengan pengenalan identiti pengguna dan tidak mudah diteka; d. Kombinasi sekurang-kurangnya **DUA BELAS (12) AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (*alphanumeric*) **kecuali** bagi sistem, perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; e. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; f. Sistem hendaklah mempunyai tempoh masa aktif yang akan tamat selepas melebihi tempoh *idle* yang ditetapkan tidak melebihi 10 minit atau tertakluk pada penetapan/kekangan sistem/aplikasi masing-masing;	ICTSO, ICTSM, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Penyelia, Pengguna.

PERKARA	TANGGUNGJAWAB
g. Sistem yang dibangunkan hendaklah mempunyai kemudahan menukar kata laluan oleh pengguna; h. Pertukaran kata laluan selepas *login* kali pertama atau selepas *reset* kata laluan hendaklah dikuat kuasakan; i. Kemasukan kata laluan bagi capaian sistem hendaklah mempunyai had maksimum. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga ID capaian diaktifkan semula; dan j. Cubaan (*attempt*) kemasukan kata laluan bagi capaian sistem hendaklah mempunyai had maksimum. Setelah mencapai had maksimum, capaian kepada sistem akan disekat sehingga ID capaian diaktifkan semula.	

5.3.2 CLEAR DESK POLICY / CLEAR SCREEN POLICY

PERKARA	TANGGUNGJAWAB
Dasar Meja Kosong (*Clear Desk Policy)* bermaksud tidak meninggalkan dokumen terperingkat dan bahan-bahan sensitif terdedah di ruang kerja. Dasar Skrin Kosong (*Clear Screen Policy*) bermaksud tidak memaparkan sebarang maklumat sensitif di paparan skrin apabila komputer berkenaan ditinggalkan. Perkara yang perlu dipatuhi adalah sebagaimana berikut: a. Menggunakan kemudahan *screen saver password* atau *logout* apabila meninggalkan komputer;	ICTSO, Pengarah Bahagian/Negeri, ICTSM, Pengurus Projek ICT, Pentadbir Sistem, Penyelia, Pengguna.

b. E-mel masuk dan keluar hendaklah dikawal; c. Menyimpan dokumen terperingkat dan bahan - bahan sensitif dalam laci atau kabinet berkunci; dan d. Memastikan dokumen (*softcopy* dan *hardcopy*) diambil segera dari pencetak, pengimbas, mesin faks dan mesin fotostat.	

5.4 KAWALAN CAPAIAN RANGKAIAN, APLIKASI DAN MAKLUMAT

OBJEKTIF

Menghalang capaian yang tidak dibenarkan kepada rangkaian, sistem pengoperasian, aplikasi dan maklumat.

5.4.1 KAWALAN CAPAIAN RANGKAIAN DAN PERKHIDMATAN RANGKAIAN

PERKARA	TANGGUNGJAWAB
Menghalang sebarang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian JPN, rangkaian organisasi lain dan rangkaian awam; b. Mewujudkan dan menguatkuasakan mekanisma untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; d. Memastikan *firewall* dan peralatan sempadan rangkaian mengesahkan sumber serta alamat destinasi sebelum capaian dibenarkan; dan	ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Sistem.

PERKARA	TANGGUNGJAWAB
e. Memastikan pemilik bagi sumber maklumat yang diagihkan melalui rangkaian mesti menetapkan kawalan yang bersesuaian untuk memastikan capaian sumber berkenaan hanya dihadkan kepada pengguna yang dibenarkan.	

5.4.2 KAWALAN CAPAIAN SISTEM PENGOPERASIAN, APLIKASI DAN MAKLUMAT

PERKARA	TANGGUNGJAWAB
Menghalang capaian tidak sah ke atas maklumat yang terdapat di dalam sistem pengoperasian, aplikasi dan maklumat. Kawalan capaian hendaklah mematuhi perkara-perkara berikut: a. Membenarkan pengguna mencapai aplikasi dan maklumat mengikut tahap capaian yang ditentukan; b. Setiap aktiviti capaian sistem pengoperasian dan aplikasi hendaklah direkodkan (*system log*); c. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja. d. Satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna; e. Mewujudkan sistem pengurusan kata laluan dan memastikan kata laluan adalah berkualiti; f. Mewujudkan jejak audit ke atas semua capaian dan transaksi aplikasi bagi semua peranan pengguna; g. Menyediakan kaedah sesuai untuk pengesahan capaian (*authentication*); dan	ICTSO, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

PERKARA	TANGGUNGJAWAB
h. Mengehadkan tempoh penggunaan mengikut kesesuaian sebagaimana berikut: i. Mengehadkan dan mengawal penggunaan program utiliti yang berkemampuan mengatasi sebarang kawalan sistem dan aplikasi (*time-limit*); dan ii. Menamatkan sesebuah sesi yang tidak aktif sekiranya tidak digunakan bagi satu tempoh yang ditetapkan (*log-off*).	

5.4.3 KAWALAN CAPAIAN KEPADA *SOURCE CODE*

PERKARA	TANGGUNGJAWAB
Capaian kepada *source code* hendaklah dihadkan. Perkara-perkara yang perlu dipatuhi sebagaimana berikut: a. Setiap aktiviti pindaan *source code* hendaklah direkodkan (*system log*); b. Penyelenggaraan dan penyalinan *source code* hendaklah tertakluk kepada kawalan perubahan; dan c. *Source code* bagi semua aplikasi dan perisian hendaklah menjadi hakmilik JPN.	Pengarah Bahagian/Negeri, ICTSO, Pengurus Projek ICT, Pentadbir Sistem.

5.5 PERALATAN MUDAH ALIH DAN KERJA JARAK JAUH

OBJEKTIF

Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

PERKARA	TANGGUNGJAWAB
Perkara yang perlu dipatuhi termasuk yang berikut: a. Mewujudkan peraturan dan garis panduan keselamatan yang bersesuaian bagi pengurusan peralatan mudah alih dan perlindungan risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; dan b. Mewujudkan peraturan dan garis panduan untuk memastikan persekitaran capaian kerja jarak jauh adalah selamat.	ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

BIDANG 6: KRIPTOGRAFI

6.1 KAWALAN KRIPTOGRAFI

OBJEKTIF

Memastikan penggunaan kriptografi yang betul dan berkesan untuk melindungi kerahsiaan, integriti dan kesahihan maklumat.

6.1.1 POLISI KAWALAN PENGUNAAN KRIPTOGRAFI

PERKARA	TANGGUNGJAWAB
Kriptografi adalah mekanisme penyulitan data menggunakan kaedah algoritma matematik. Transformasi penyulitan data terbahagi kepada dua (2) iaitu kaedah penyulitan (encryption) dan penyahsulitan (decryption). Teknik ini digunapakai dalam keselamatan maklumat dan data bagi menjaga kerahsiaan dan integriti sesuatu maklumat. Prosedur kawalan kriptografi untuk melindungi maklumat hendaklah diwujudkan dan dilaksanakan dengan mengambil kira perkara-perkara berikut: a. Tahap perlindungan hendaklah dikenal pasti berdasarkan penemuan penilaian risiko; b. Pemindahan maklumat secara mudah-alih dan merentasi talian komunikasi hendaklah menggunakan kaedah enkripsi (sekiranya perlu); c. Kunci kriptografi hendaklah diuruskan dengan baik; d. Kaedah kriptografi yang digunakan hendaklah mematuhi dasar dan peraturan yang berkuatkuasa; e. Jaminan pengesahan identiti / entiti melalui kaedah kriptografi;	Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

PERKARA	TANGGUNGJAWAB
f. Menyokong Dasar Kriptografi Negara (*National Cryptography Policy* (NCP)) yang disokong oleh Senarai Algoritma Kriptografi Terpercaya Negara (MySEAL); dan g. Implikasi penggunaan kriptografi terhadap proses yang bergantung kepada pemeriksaan kandungan.	

6.1.2 PENGURUSAN KUNCI AWAM

PERKARA	TANGGUNGJAWAB
Pengurusan Prasarana Kunci Awam hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

BIDANG 7: KESELAMATAN FIZIKAL DAN PERSEKITARAN

7.1 KAWASAN TERPERINGKAT

OBJEKTIF

- Mengawal dan mencegah akses ke tempat terperingkat tanpa kebenaran yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada aset fizikal dan kemudahan pemprosesan maklumat Jabatan.
- Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

7.1.1 LINGKUNGAN KESELAMATAN FIZIKAL

PERKARA	TANGGUNGJAWAB
Mengenal pasti lingkungan keselamatan dan menentukan tahap perlindungan keselamatan yang diperlukan untuk melindungi maklumat terperingkat dan kemudahan pemprosesan maklumat berdasarkan kepada Arahan Keselamatan. Kawalan kawasan terperingkat adalah bertujuan untuk menghalang capaian, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat JPN. Perkara yang perlu dipatuhi termasuk yang berikut: a. Ketua Jabatan hendaklah melantik Pegawai Keselamatan Jabatan (PKJ) yang terdiri daripada Timbalan Ketua Jabatan yang bertanggungjawab mengenai pentadbiran Jabatan bagi melaksanakan arahan-arahan keselamatan dengan mendapat nasihat Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO); b. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, jeriji besi, sistem kawalan pintu, kamera litar tertutup dan pengawal keselamatan) untuk melindungi kawasan yang mengandungi	KPPN, Timbalan Ketua Pengarah (Pengurusan), Pegawai Keselamatan Jabatan (PKJ), Pengarah Bahagian/Negeri, Ketua Pejabat, Pengawal Keselamatan, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
maklumat dan kemudahan pemprosesan maklumat; c. Garis Panduan Kawalan Keselamatan Fizikal Premis hendaklah diwujud, dikemaskini dan dilaksanakan mengikut Arahan Keselamatan serta merujuk khidmat nasihat Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO); d. Melindungi tempat terperingkat melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini dengan merekodkan akses untuk tujuan keselamatan dan pengauditan; e. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; f. Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan dan ancaman manusia; g. Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam tempat terperingkat; h. Sebarang pemasangan peralatan kawalan capaian pintu dan CCTV mengikut standard serta piawaian Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO) dan mendapat pengesahan Pegawai Keselamatan Jabatan; dan i. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada mana-mana pihak yang tidak diberi kebenaran memasukinya.	

7.1.2 KAWALAN KEMASUKAN FIZIKAL

PERKARA	TANGGUNGJAWAB
Kawasan terperingkat hendaklah dilindungi dengan kawalan kemasukan berdasarkan Arahan Keselamatan dan Arahan Jabatan Pendaftaran Negara.	Timbalan Ketua Pengarah (Pengurusan), Pegawai Keselamatan Jabatan (PKJ), Pengarah Bahagian/Negeri, Ketua Pejabat, Pihak Ketiga.

7.1.3 PEMANTAUAN KESELAMATAN FIZIKAL

PERKARA	TANGGUNGJAWAB
Akses fizikal ke premis hendaklah dikawal dan dipantau setiap masa daripada pihak yang tidak dikenali atau sebarang aktiviti yang mencurigakan. Langkah-langkah berikut boleh dipertimbangkan bagi pemantauan keselamatan fizikal : a. Memastikan premis disediakan dengan sistem pemantauan komprehensif seperti Pengawal Keselamatan, alat penggera pencerobohan, *Closed-Circuit Television* (CCTV) dan Sistem Pengurusan Maklumat Keselamatan Fizikal; b. Sistem pemantauan fizikal hendaklah dilindungi daripada sebarang ancaman yang boleh menjejaskan fungsi atau keselamatan maklumat JPN; c. Sistem pemantauan fizikal hendaklah diuji secara berkala bagi memastikan ketersediaan fungsinya semasa kecemasan; dan d. Tempoh pengekalan rekod pemantauan fizikal adalah sekurang-kurangnya 5 tahun.	Timbalan Ketua Pengarah (Pengurusan), Pegawai Keselamatan Jabatan (PKJ), Pengarah Bahagian/Pengarah Negeri, Ketua Pejabat, Pihak Ketiga.

7.1.4 KAWALAN PEJABAT, BILIK DAN TEMPAT OPERASI

PERKARA	TANGGUNGJAWAB
Kawalan keselamatan fizikal dan pemantauan bagi ruang pejabat, bilik dan kemudahan hendaklah direkabentuk dan dilaksanakan berdasarkan Arahan Keselamatan, Arahan Jabatan Pendaftaran Negara dan merujuk khidmat nasihat Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO).	Timbalan Ketua Pengarah (Pengurusan), Pegawai Keselamatan Jabatan (PKJ), Pengarah Bahagian Pentadbiran, Pengarah Bahagian/Negeri, Ketua Pejabat, Pengawal Keselamatan, Kakitangan JPN, Pihak Ketiga.

7.1.5 PERLINDUNGAN TERHADAP ANCAMAN LUARAN DAN PERSEKITARAN

PERKARA	TANGGUNGJAWAB
Perlindungan fizikal perlu direkabentuk dan dilaksanakan bagi menghadapi bencana alam, ancaman luar dan kemalangan berdasarkan Arahan Keselamatan dan Arahan Jabatan Pendaftaran Negara.	Timbalan Ketua Pengarah (Pengurusan), Pegawai Keselamatan Jabatan (PKJ), Pengarah Bahagian Pentadbiran, Pengarah Bahagian/Negeri, Ketua Pejabat, Pengawal Keselamatan, Pihak Ketiga.

7.1.6 BERTUGAS DALAM KAWASAN TERPERINGKAT

PERKARA	TANGGUNGJAWAB
Prosedur bertugas di kawasan terperingkat perlu diwujudkan, dipatuhi, dikemaskini dan dilaksanakan berdasarkan Arahan Keselamatan dan Arahan Jabatan Pendaftaran Negara.	Timbalan Ketua Pengarah (Pengurusan), Pengarah Bahagian Pentadbiran, Pegawai Keselamatan Jabatan (PKJ).

7.2 KESELAMATAN PERKAKASAN ICT DAN MAKLUMAT

OBJEKTIF

Melindungi perkakasan ICT dan maklumat daripada kehilangan, kerosakan, kecurian dan penyalahgunaan serta gangguan terhadap perkhidmatan Jabatan.

7.2.1 PENEMPATAN DAN PERLINDUNGAN PERKAKASAN ICT DAN MAKLUMAT

PERKARA	TANGGUNGJAWAB
Aset ICT hendaklah ditempatkan dan dilindungi untuk meminimakan risiko daripada ancaman dan pencerobohan. Keselamatan perkakasan adalah bertujuan untuk mengelak sebarang kehilangan, kerosakan, kecurian, bencana atau kompromi ke atas perkakasan ICT dan maklumat serta gangguan sistem penyampaian perkhidmatan JPN. Penyimpanan, penempatan dan perlindungan aset ICT hendaklah dilaksanakan. Perkara yang perlu dipatuhi termasuk yang berikut: a. **Perkakasan** i. Menempatkan dan mengawal perkakasan ICT supaya risiko ancaman dan bencana dari persekitaran serta menghalang pencerobohan oleh pihak yang tidak diberi kebenaran;	Pegawai Keselamatan Jabatan (PKJ), Pengarah Bahagian/Negeri, Ketua Pejabat, Pengurus Projek ICT, Pentadbir Sistem, Pegawai Aset, Pembantu Pegawai Aset, Pengguna, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
ii. Semua cadangan perolehan, penempatan dan penaiktarafan perkakasan ICT hendaklah dirujuk kepada Jawatankuasa Pemandu ICT JPN terlebih dahulu; iii. Pengendalian perkakasan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa; iv. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; v. Pengguna dilarang sama sekali mengubah konfigurasi, menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; vi. Pengguna hendaklah memastikan perisian antivirus di komputer peribadi sentiasa aktif dan dikemaskini; vii. Semua aset ICT hanya boleh digunakan atas urusan rasmi sahaja; viii. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya; ix. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; x. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada *Helpdesk*; dan xi. Kepala soket peralatan ICT hendaklah dicabut daripada soket sebelum meninggalkan pejabat bagi mengelakkan kerosakan perkakasan seperti banjir atau litar pintas. **b. Dokumen** Bagi memastikan integriti, kerahsiaan dan kebolehsediaan maklumat serta pengurusan dokumentasi yang baik dan selamat	

PERKARA	TANGGUNGJAWAB
sebagaimana berikut hendaklah dipatuhi: i. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; ii. Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit atau Terhad kepada dokumen; dan iii. Pengurusan dokumen terperingkat hendaklah diwujudkan bagi menerima, memproses, menyimpan dan menghantar dokumen tersebut supaya ianya diuruskan berasingan daripada dokumen tidak terperingkat berdasarkan Arahan Keselamatan. **c. Media Storan (*External Hard Disk*, *optical disk*, *flash disk*, katrij, mikrofilem dan lain-lain)**. Langkah-langkah pencegahan sebagaimana berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat. i. Menyediakan ruang dan bekas penyimpanan yang mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; ii. Mengehadkan akses kepada pengguna yang dibenarkan sahaja; iii. Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan; dan iv. Mengadakan sistem pengurusan media termasuk inventori, pergerakan, pelabelan dan *backup / restore*. **d. Bahan-bahan Habis Guna Terkawal** (Kad Pengenalan, Sijil dan semua dokumen	

PERKARA	TANGGUNGJAWAB
terkawal mentah) perlu diberi perhatian khusus kerana ia berupaya menyimpan maklumat terperingkat. Langkah-langkah pencegahan sebagaimana berikut hendaklah dilaksanakan untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat: i. Menyediakan ruang dan bekas penyimpanan yang mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; ii. Mengehadkan akses kepada pengguna yang dibenarkan sahaja; dan iii. Sebarang pelupusan hendaklah merujuk kepada tatacara pelupusan.	

7.2.2 UTILITI SOKONGAN

PERKARA	TANGGUNGJAWAB
a. Semua kemudahan utiliti seperti bekalan kuasa, pendingin udara, bekalan air dan sistem pembentungan harus dilindungi daripada sebarang gangguan; b. Semua aset ICT perlu dilindungi dari kegagalan kemudahan utiliti; c. Kemudahan utiliti mestilah diperiksa dan diuji untuk memastikan ia berfungsi dengan baik bagi mengurangkan risiko kegagalan; d. Semua cadangan berkaitan premis sama ada untuk perolehan dan pengubahsuaian hendaklah dirujuk terlebih dahulu kepada Pegawai Keselamatan Jabatan, Pejabat Ketua	Pegawai Keselamatan Jabatan, Pengarah Bahagian/Negeri, Ketua Pejabat, Kakitangan JPN, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
Pegawai Keselamatan Kerajaan (CGSO), Jabatan Kerja Raya (JKR) dan Pihak Berkuasa Tempatan (PBT) bagi menghindarkan kerosakan dan gangguan terhadap premis dan perkakasan ICT; dan e. Dilarang menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan ICT.	

7.2.3 KESELAMATAN KABEL

PERKARA	TANGGUNGJAWAB
Langkah-langkah keselamatan yang perlu diambil termasuklah perkara berikut: a. Kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi; b. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; c. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; d. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan e. Membuat pelabelan kabel yang jelas.	Pegawai Keselamatan Jabatan, Pengarah Bahagian/Negeri, Ketua Pejabat, Pengurus Projek ICT, Pentadbir Sistem, Pihak Ketiga.

7.2.4 PENYELENGGARAAN PERKAKASAN ICT

PERKARA	TANGGUNGJAWAB
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan	Pengarah Bahagian/Negeri, Ketua Pejabat,

PERKARA	TANGGUNGJAWAB
dan integriti. Langkah-langkah keselamatan yang perlu diambil termasuklah sebagaimana berikut: a. Kaedah dan tatacara penyelenggaraan perlu mematuhi prosedur yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; b. Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan dan bertauliah sahaja; c. Pengguna hendaklah menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; d. Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; e. Pihak Ketiga yang membekalkan perkakasan ICT hendaklah melabel perkataan "*Loaner*" beserta nama syarikat dengan jelas ke atas perkakasan ICT yang dipinjamkan kepada Jabatan. Pihak Ketiga tersebut hendaklah menulis maklumat peminjaman perkakasan ICT (*loaner*) di *service report* dan memaklumkan kepada Pegawai Aset / Ketua Pejabat / Pengurus Projek sebelum peralatan rosak dibawa keluar; dan f. Peminjaman perkakasan ICT (*loaner*) oleh Pihak Ketiga tidak boleh didaftarkan/direkod di dalam Sistem Pemantauan Pengurusan Aset (SPPA) atau dilabelkan sebagai aset Jabatan.	Pengurus Projek ICT, Pegawai Aset, Pemilik Aset, Pembantu Pegawai Aset, Pegawai IT Negeri, *Helpdesk*, Pengguna, Pihak Ketiga.

7.2.5 PERKAKASAN ICT DIBAWA KELUAR PREMIS

PERKARA	TANGGUNGJAWAB
a. Perkakasan ICT yang hendak dibawa keluar dari premis JPN untuk tujuan rasmi, hendaklah mendapat kelulusan dari Pegawai Aset Bahagian / Pegawai Aset Negeri dan Ketua Pejabat mengikut peraturan dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; b. Sekiranya perkakasan ICT dibawa keluar untuk tujuan penyelenggaraan, pemilik aset hendaklah memeriksa dan memastikan perkakasan ICT yang dibawa keluar tidak mengandungi maklumat rasmi Kerajaan; c. Peminjaman dan pemulangan perkakasan ICT hendaklah mendapat kelulusan dan direkodkan oleh Pegawai Aset Bahagian / Pegawai Aset Negeri / Ketua Pejabat; d. Peminjam bertanggungjawab terhadap keselamatan perkakasan ICT yang dipinjam; e. Peminjam hendaklah memastikan perkakasan yang dipulangkan berada dalam keadaan baik dan Pegawai Aset Bahagian / Pegawai Aset Negeri / Ketua Pejabat hendaklah mengesah/merekod pemulangan perkakasan ICT; f. Sebarang kehilangan semasa peminjaman perkakasan ICT tersebut hendaklah dilaporkan kepada Pegawai Aset / Pengarah Bahagian / Pengarah Negeri dengan kadar segera. Pegawai Aset Bahagian / Pegawai Aset Negeri / Ketua Pejabat hendaklah melaksanakan tindakan berdasarkan peraturan yang sedang berkuatkuasa; dan g. Penyimpanan atau penempatan perkakasan ICT yang dibawa keluar mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Ketua Pejabat, Pengawai Aset, Pembantu Pegawai Aset, Pegawai IT Negeri, Pemilik Aset, Kakitangan JPN, Pihak Ketiga.

7.2.6 PELUPUSAN DAN GUNA SEMULA PERKAKASAN ICT

PERKARA	TANGGUNGJAWAB
Semua perkakasan ICT yang mengandungi media storan hendaklah disemak dan disahkan untuk memastikan maklumat Jabatan dan perisian berlesen telah dihapuskan atau *overwritten* secara selamat mengikut peraturan-peraturan yang berkuatkuasa sebagaimana berikut: a. Langkah-langkah hendaklah diambil termasuklah menghapuskan semua maklumat Jabatan yang terkandung di dalam perkakasan sebelum dilupuskan; b. Salinan maklumat hendaklah disimpan sekiranya perlu sebelum dilupuskan; c. Perkakasan ICT yang hendak dilupuskan perlu diasingkan dan disimpan di tempat khas yang mempunyai ciri-ciri keselamatan sebelum ianya dilupuskan; dan d. Pengguna dilarang sama sekali mencabut, menanggal dan menyimpan aksesori / komponen ICT seperti *speaker*, RAM, *harddisk*, *motherboard* dan CPU sebelum dilupuskan.	Pegawai Keselamatan Jabatan, Pengarah Bahagian/Negeri, Ketua Pejabat, Pengurus Projek ICT, Pegawai Aset, Pembantu Pegawai Aset, Pegawai IT Negeri, Pemilik Aset, Kakitangan JPN, Pihak Ketiga.

7.2.7 PERKAKASAN ICT TANPA PENGAWASAN

PERKARA	TANGGUNGJAWAB
Perkakasan ICT hendaklah dijaga dan dilindungi dengan mematuhi perkara-perkara berikut: a. Menamatkan sesi setelah selesai tugas; b. Log keluar aplikasi atau perkhidmatan rangkaian apabila tidak lagi digunakan; dan c. Lindungi aset ICT daripada penggunaan yang tidak dibenarkan.	Pegawai Keselamatan Jabatan, Pengarah Bahagian/Negeri, Ketua Pejabat, Pengurus Projek ICT, Pemilik Aset, Kakitangan JPN, Pihak Ketiga.

BIDANG 8: KESELAMATAN OPERASI

8.1 PROSEDUR DAN TANGGUNGJAWAB OPERASI

OBJEKTIF

Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan ke atas kemudahan pemprosesan maklumat.

8.1.1 PENGENDALIAN PROSEDUR OPERASI

Penyediaan dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut:

PERKARA	TANGGUNGJAWAB
a. Semua prosedur pengurusan operasi hendaklah diwujud, dikenal pasti, didokumenkan, disimpan, dikemaskini, dikawalselia, dihadkan capaian dan digunapakai oleh pengguna; b. Setiap prosedur hendaklah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan notifikasi ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; c. Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan; dan d. Semua prosedur hendaklah dipatuhi bagi memastikan integriti, kerahsiaan dan kebolehsediaan maklumat yang baik dan selamat.	ICTSO, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

8.1.2 PENGURUSAN PERUBAHAN

Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut:

PERKARA	TANGGUNGJAWAB
a. Pengubahsuaian yang melibatkan peranti sistem untuk pemprosesan maklumat, perkakasan dan perisian serta prosedur mestilah mendapat kebenaran daripada pegawai penyelia terlebih dahulu; b. Aktiviti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Perubahan atau pengubahsuaian hendaklah diuji, direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada sengaja atau tidak.	ICTSO, ICTSM, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pegawai Penyelia, Pentadbir Sistem, Pegawai Aset, Pengguna.

8.1.3 PENGURUSAN KAPASITI

Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

PERKARA	TANGGUNGJAWAB
a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti bagi memastikan keperluannya mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa hadapan agar prestasi sistem di tahap optimum; dan b. Keperluan kapasiti hendaklah mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pengurus Projek ICT, Pentadbir Sistem.

8.1.4 PENGURUSAN KONFIGURASI

PERKARA	TANGGUNGJAWAB
Konfigurasi keselamatan perkakasan, perisian, perkhidmatan dan rangkaian perlu diwujudkan, didokumenkan, dilaksanakan, dipantau dan disemak. Ini bagi memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi sepertimana yang ditetapkan dan konfigurasinya adalah tepat dan tidak berubah tanpa kebenaran.	Pengurus Projek ICT, Pentadbir Sistem.

8.1.5 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN OPERASI (*PRODUCTION*)

Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

PERKARA	TANGGUNGJAWAB
Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai operasi. a. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan pembangunan; b. Data yang mengandungi maklumat terperingkat tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat; dan c. Merekodkan semua penggunaan sumber yang digunakan dalam setiap persekitaran.	ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Sistem.

8.2 PERLINDUNGAN DARIPADA PERISIAN BERBAHAYA

OBJEKTIF

Untuk memastikan kemudahan pemprosesan maklumat dan maklumat dilindungi daripada perisian berbahaya.

8.2.1 KAWALAN TERHADAP PERISIAN BERBAHAYA

Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan perisian berbahaya seperti virus, *trojan*, perisian hasad dan hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan daripada perisian berbahaya adalah seperti berikut:

PERKARA	TANGGUNGJAWAB
a. Peralatan ICT yang dilengkapi dengan sistem pengoperasian hendaklah dilengkapi dengan perisian antivirus yang aktif dan terkini; b. Memasang kawalan keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, *Intrusion Prevention System* (IPS), *Content Filtering* dan *Web Application Firewall* (WAF) dan mengikut prosedur penggunaan yang betul dan selamat; c. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; d. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; e. Menggunakan perisian antivirus yang dibenarkan oleh Jabatan sahaja; f. Mengemaskini antivirus dengan definisi terkini; g. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; h. Memasukkan klausa waranti di dalam kontrak yang telah ditawarkan kepada Pihak Ketiga. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; dan i. Mengadakan dan menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya.	Pengarah Bahagian/Negeri, ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

8.3 SANDARAN

OBJEKTIF

Memastikan sistem, aplikasi, data, imej dan maklumat mempunyai sandaran, berkeupayaan untuk *restore* semula dan melindungi daripada kehilangan maklumat agar kesinambungan perkhidmatan berjalan lancar.

8.3.1 SANDARAN MAKLUMAT *(BACKUP)*

Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut 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 tempat simpanan salinan pendua (*off-site backup tape storage)*. Perkara berikut hendaklah dilaksanakan bagi memastikan sistem dapat dipulihkan:

PERKARA	TANGGUNGJAWAB
a. Membuat sandaran penuh setelah mendapat versi terbaru; b. Membuat sandaran penuh sekurang-kurangnya sekali setahun ke atas semua sistem perisian dan aplikasi; c. Membuat sandaran ke atas semua data secara harian, mingguan, bulanan atau tahunan; d. Menguji sistem sandaran sedia ada dan prosedur *restore* sekurang-kurangnya sekali setahun bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan e. Salinan sandaran hendaklah disimpan di lokasi berlainan yang selamat dan lokasi perlu disahkan selamat oleh CGSO.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

8.4 LOG DAN PEMANTAUAN

OBJEKTIF

Merekod kronologi dan menjana fakta pembuktian mengikut dasar, arahan dan prosedur yang berkuatkuasa.

8.4.1 LOG KRONOLOGI

Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan. Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data.

Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti yang berikut:

(i) Fail log sistem pengoperasian;
(ii) Fail log servis (contoh: *web*, e-mel);
(iii) Fail log aplikasi (*audit trail*); dan
(iv) Fail log rangkaian (contoh: *switch, firewall, IPS*).

PERKARA	TANGGUNGJAWAB
Perkara-perkara yang perlu dipatuhi: a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Fail log hendaklah diaktifkan dan disimpan untuk tempoh masa yang dipersetujui; c. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; d. Waktu yang berkaitan dengan sistem perlu diselaraskan dengan sumber waktu yang ditetapkan; dan	ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Sistem, *Helpdesk*, JPNCSIRT.

PERKARA	TANGGUNGJAWAB
e. Sekiranya berlaku aktiviti-aktiviti lain yang tidak sah seperti insiden kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada JKICT/ ICTSO/ ICTSM dengan segera.	

8.4.2 PERLINDUNGAN FASILITI LOG DAN MAKLUMAT LOG

PERKARA	TANGGUNGJAWAB
Fasiliti log dan maklumat log hendaklah dilindungi daripada perkara berikut: a. Kemudahan merekod dan menyimpan maklumat log hendaklah dilindungi daripada diubahsuai; b. Melindungi maklumat log daripada capaian yang tidak dibenarkan; dan c. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera.	Pengurus Projek ICT, Pentadbir Sistem.

8.4.3 AKTIVITI PEMANTAUAN

PERKARA	TANGGUNGJAWAB
Perkara-perkara berikut hendaklah dipatuhi: a. Aktiviti aplikasi, sistem, storan, media, rangkaian dan *end-point devices* hendaklah dipantau untuk mengenalpasti tindakan anomali yang berlaku. Ia adalah bagi membolehkan tindakan sewajarnya dapat diambil untuk menilai potensi insiden keselamatan maklumat.	CDO, ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Sistem, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
b. Skop dan tahap pemantauan ditentukan mengikut keperluan organisasi, peraturan dan prosedur yang berkaitan. c. Maklumat pemantauan adalah seperti: i. Trafik keluar masuk maklumat rangkaian, sistem dan aplikasi; ii. Akses kepada sistem, server, peralatan rangkaian, sistem pemantauan, sistem-sistem kritikal dan lain-lain; iii. Fail konfigurasi sistem dan rangkaian pelbagai peringkat; iv. Log peralatan rangkaian; v. Log kejadian (*events log*) berkaitan aktiviti sistem dan rangkaian; vi. Semakan kod yang sedang digunakan hendaklah kod yang dibenarkan ke atas sistem dan tidak mengganggu operasi sistem; dan vii. Penggunaan sumber dan prestasinya.	

8.4.4 LOG PENTADBIR DAN PENGENDALI

PERKARA	TANGGUNGJAWAB
Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan disemak secara berkala seperti berikut: a. Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Log hendaklah dilindungi dan jejak audit disemak secara berkala; b. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pengurus Projek ICT / Pentadbir Sistem hendaklah melaporkan kepada JKICT	ICTSO, ICTSM, JKICT, Pengurus Projek ICT, Pentadbir Sistem. Pengendali Sistem.

PERKARA	TANGGUNGJAWAB
dengan segera; c. Kesalahan, kesilapan dan / atau penyalahgunaan pada sistem perlu direkodkan, dianalisis dan diambil tindakan sewajarnya; dan d. Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian.	

8.4.5 KESERAGAMAN WAKTU

PERKARA	TANGGUNGJAWAB
Waktu sistem pemprosesan maklumat atau *domain* keselamatan hendaklah diselaraskan dengan sumber waktu yang ditetapkan oleh Jabatan. Waktu bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JPN atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh *National Metrology Institute of Malaysia* (NMIM).	Pentadbir Sistem.

8.5 KAWALAN PERISIAN OPERASI

OBJEKTIF

Melindungi dan memastikan integriti sistem operasi.

8.5.1 PEMASANGAN PERISIAN PADA SISTEM OPERASI

PERKARA	TANGGUNGJAWAB
a. Pengemaskinian perisian operasi, aplikasi dan program hanya boleh dilakukan setelah mendapat sokongan Pengurus Projek ICT dan kelulusan ICTSM; b. Aplikasi dan sistem operasi hanya boleh dilaksanakan selepas ujian yang terperinci dan diperakui berjaya; c. Setiap konfigurasi ke atas sistem perlu dikawal dan didokumentasi dengan teratur; d. Memastikan penggunaan perisian mempunyai lesen sah; dan e. Satu strategi *rollback* harus diadakan sebelum perubahan ke atas konfigurasi, sistem dan perisian dilaksanakan.	ICTSM, Pengurus Projek ICT, Pentadbir Sistem.

8.6 PENGURUSAN KERENTANAN TEKNIKAL

OBJEKTIF

Melindungi dan mencegah daripada berlaku eksploitasi pada keterdedahan teknikal.

8.6.1 PENGURUSAN KERENTANAN TEKNIKAL

Maklumat tentang 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 ke atas sistem aplikasi dan operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut:

PERKARA	TANGGUNGJAWAB
a. Melaksanakan *Security Posture Assessment* (SPA) sekurang-kurangnya sekali setahun; b. Melaksanakan ujian penembusan (*penetration test*) untuk memperolehi maklumat kerentanan teknikal bagi sistem aplikasi dan operasi; c. Menilai tahap risiko kerentanan; dan d. Merancang dan melaksanakan aktiviti pengukuhan serta kawalan risiko.	CDO, ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Sistem.

8.6.2 KAWALAN PEMASANGAN PERISIAN

Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:

PERKARA	TANGGUNGJAWAB
a. Hanya perisian yang diperakui sahaja dibenarkan; b. Memasang dan menggunakan hanya perisian yang tulen dan berlesen; c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; dan	Pengarah Bahagian/Negeri, ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Sistem, Pengguna, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
d. Memastikan pihak Pihak Ketiga mendapat kelulusan sebelum aktiviti pemasangan dilaksanakan.	

8.7 KELULUSAN AUDIT SISTEM MAKLUMAT

OBJEKTIF

Meminimakan kesan ke atas aktiviti audit terhadap sistem operasi.

8.7.1 KAWALAN AUDIT SISTEM MAKLUMAT

PERKARA	TANGGUNGJAWAB
a. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi hendaklah dirancang dan dipersetujui oleh ICTSO bagi meminimakan gangguan dalam sistem penyampaian perkhidmatan; dan b. Laporan audit ICT perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Sistem.

8.8 PENGURUSAN ANCAMAN KESELAMATAN SIBER

OBJEKTIF

Bagi memberikan kesedaran mengenai status kedudukan organisasi terhadap situasi ancaman semasa supaya tindakan pencegahan yang bersesuai dapat diambil.

8.8.1 PERISIKAN ANCAMAN

PERKARA	TANGGUNGJAWAB
a. Maklumat berkaitan ancaman keselamatan hendaklah dikumpul dan dianalisis bagi memudahkan tindakan pencegahan diambil serta mengurangkan kesan ancaman terhadap organisasi;	CDO, ICTSO, ICTSM, Pasukan Keselamatan ICT, Jawatankuasa

b. Laporan berkaitan perisikan ancaman keselamatan hendaklah dikongsi kepada pihak yang berkenaan bagi memberikan kesedaran dan memastikan tindakan mitigasi yang sesuai boleh dilaksanakan; dan c. Program kesedaran hendaklah dilaksanakan dengan mengambil kira laporan dan analisa daripada perisikan ancaman.	Keselamatan ICT, Pentadbir Sistem.

BIDANG 9: KESELAMATAN KOMUNIKASI

9.1 PENGURUSAN KESELAMATAN RANGKAIAN

OBJEKTIF
Memastikan maklumat dan kemudahan dalam rangkaian dilindungi.

9.1.1 KAWALAN DAN KESELAMATAN RANGKAIAN

Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman.

PERKARA	TANGGUNGJAWAB
Perkara-perkara yang perlu dipatuhi: a. Memasang antaramuka yang bersesuaian di antara rangkaian organisasi, rangkaian organisasi lain dan rangkaian awam; b. Rangkaian perlu dikawal, dipantau dan diurus sebaiknya, bertujuan untuk mengawal daripada sebarang ancaman bagi menjamin keselamatan kemudahan ICT yang menggunakan rangkaian, termasuk maklumat yang dipindahkan melaluinya; c. Memastikan kerja-kerja operasi rangkaian dilindungi; d. Peranti rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat; e. Capaian rangkaian hendaklah dikawal, dihadkan dan diselia contohnya Tapisan Kandungan (*Content Filtering*) dan *Network Acces Control* (NAC); f. Memasang, mengkonfigurasi dan menyelia peralatan keselamatan rangkaian bagi mengesan cubaan pencerobohan atau aktiviti-	ICTSO, ICTSM, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna, JPNCSIRT, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
aktiviti lain yang boleh menjejaskan prestasi rangkaian, sistem dan maklumat JPN seperti *Firewall, Intrusion Prevention System* (IPS), *Web Application Firewall* (WAF) dan lain-lain perkakasan keselamatan rangkaian yang terkini; g. Log peralatan keselamatan rangkaian seperti *Firewall* dan IPS hendaklah dipantau secara berkala. Sebarang log dan trafik yang dikesan boleh memberi ancaman prestasi rangkaian atau aplikasi JPN hendaklah dimaklumkan kepada JKICT dengan segera; h. Pemasangan perkakasan dan perisian berkaitan rangkaian hendaklah mendapat kebenaran daripada ICTSM; i. Sebarang penyambungan kepada peralatan keselamatan rangkaian seperti *Firewall*, IPS dan WAF hendaklah mendapat kelulusan ICTSM; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan Jabatan adalah dilarang; k. Pemasangan rangkaian *wireless* LAN selain daripada rangkaian *wireless* Jabatan bagi capaian ke sistem JPN hendaklah mendapat kelulusan daripada ICTSM atau ICTSO; l. Semua perjanjian perkhidmatan rangkaian hendaklah mempunyai *Service Level Assurance* (SLA); m. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja;	

PERKARA	TANGGUNGJAWAB
n. Mewujud dan melaksana kawalan pengalihan laluan *(routing control*); dan o. Ciri-ciri keselamatan, jenis perkhidmatan dan keperluan pengurusan bagi perkhidmatan rangkaian perlu dikenal pasti dan dimasukkan dalam mana-mana perjanjian perkhidmatan rangkaian sama ada perkhidmatan disediakan secara dalaman atau melalui khidmat luar.	

9.1.2 PENGASINGAN RANGKAIAN

PERKARA	TANGGUNGJAWAB
a. Pengasingan rangkaian hendaklah dibuat mengikut kesesuaian dan keperluan persekitaran Jabatan; dan b. Pengasingan rangkaian hendaklah dikaji, dirancang dan dilaksanakan.	ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Sistem.

9.2 PEMINDAHAN/PERKONGSIAN DATA DAN MAKLUMAT

OBJEKTIF

Memastikan keselamatan perpindahan / pertukaran data dan maklumat di antara Jabatan / agensi dan Pihak Ketiga.

9.2.1 POLISI DAN PROSEDUR PEMINDAHAN MAKLUMAT

PERKARA	TANGGUNGJAWAB
Perkara-perkara yang perlu dipatuhi: a. Pemindahan data dan maklumat hendaklah mendapat kelulusan daripada KPPN; b. Prosedur dan kawalan pemindahan data dan maklumat hendaklah diwujudkan; dan c. Pemindahan data dan maklumat melalui media elektronik atau penghantaran secara e-mel yang mengandungi data dan maklumat rasmi hendaklah dilindungi.	KPPN, CDO, Pengarah Bahagian/Negeri, ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Sistem, Pengguna, Pihak Ketiga.

9.2.2 PERJANJIAN MENGENAI PEMINDAHAN / PERKONGSIAN DATA DAN MAKLUMAT

JPN perlu mengambil kira keselamatan data dan maklumat atau menandatangani perjanjian bertulis apabila berlaku permindahan data dan maklumat organisasi antara JPN dan pihak luar.

PERKARA	TANGGUNGJAWAB
Perkara-perkara yang perlu dipatuhi: a. Pewujudan punca kuasa kepada aktiviti perkongsian data dan maklumat; b. Penerimaan dan penghantaran data dan maklumat organisasi perlu dikawal; c. Mewujudkan prosedur bagi pengesanan data	KPPN, CDO, ICTSO, ICTSM, Pengurus Projek, Pentadbir Sistem, Pengguna, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
dan maklumat organisasi semasa pemindahan data dan maklumat; d. Mengenal pasti pihak yang bertanggungjawab ke atas risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan data dan maklumat; dan e. Mengenal pasti perlindungan data dan maklumat dalam penggunaan, pergerakan, simpanan dan menghalang ketirisan data dan maklumat.	

9.2.3 PENGURUSAN MEL ELEKTRONIK (E-MEL) DAN INTERNET

Maklumat yang terlibat dalam pengurusan mel elektronik dan internet hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian pengurusan mel elektronik dan internet dan undang-undang bertulis lain yang berkuat kuasa seperti berikut:

PERKARA	TANGGUNGJAWAB
a. Garis panduan mengenai Tatacara Pengunaan Internet dan Mel Elektronik di agensi-agensi kerajaan Bilangan 1 Tahun 2003; b. Arahan Setiausaha Majlis Keselamatan Negara Bilangan 1 2023 - pematuhan tatacara penggunaan emel dan internet; c. Surat arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 – langkah-langkah mengenai penggunaan mel elektronik agensi-agensi kerajaan; d. Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan *Government Unified Communication* (MyGovUC) dan mana-mana undang-undang bertulis yang berkuatkuasa; dan	ICTSO, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

PERKARA	TANGGUNGJAWAB
e. Garis panduan dan prosedur mengenai tatacara penggunaan internet dan e-mel jabatan.	

9.2.4 PERJANJIAN KERAHSIAAN ATAU *NON-DISCLOSURE*

PERKARA	TANGGUNGJAWAB
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak serta didokumentasi. Pihak Ketiga hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan.	ICTSO, Pengarah Bahagian/Negeri, Pengurus Projek, Pihak Ketiga.

9.3 SARINGAN WEB

PERKARA	TANGGUNGJAWAB
a. Akses kepada laman web luaran yang ditegah oleh JPN hendaklah disekat/disaring bagi mengurangkan keterdedahan kepada sebarang bentuk ancaman daripada perisian jahat (*malicious content*) serta sumber laman web yang tidak dibenarkan. b. Sebarang pengecualian akses kepada laman web yang telah disekat perlu mendapat kelulusan oleh Pengarah Bahagian atau Negeri, ICTSO atau/dan TKPP.	TKPP, CDO, ICTSO, ICTSM, Pengarah Bahagian/Pengarah Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna, Pihak Ketiga.

9.4 PENGURUSAN PERKHIDMATAN E-PAYMENT

OBJEKTIF

Memastikan keselamatan data dan maklumat yang terkandung di dalam aplikasi *E-Payment* dilindungi.

PERKARA	TANGGUNGJAWAB
Perkara yang mesti dipatuhi termasuk yang berikut: a. Data dan maklumat yang terlibat dalam *e-payment* hendaklah dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b. Data dan maklumat yang terlibat dalam *e-payment* hendaklah dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c. Integriti data dan maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem.

9.5 PENGURUSAN PERKHIDMATAN KIOSK

OBJEKTIF

Memastikan data dan keselamatan maklumat di dalam kiosk dilindungi.

PERKARA	TANGGUNGJAWAB
Perkara yang mesti dipatuhi termasuk yang berikut: a. Penempatan kiosk hendaklah ditempatkan di kawasan yang selamat dan mudah dipantau; b. Data dan maklumat yang terdapat dalam kiosk perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; c. Data dan maklumat yang terlibat dengan transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan d. Integriti data dan maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem.

BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

10.1 KEPERLUAN KESELAMATAN SISTEM MAKLUMAT

OBJEKTIF

Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

10.1.1 ANALISA KEPERLUAN DAN SPESIFIKASI KESELAMATAN MAKLUMAT

PERKARA	TANGGUNGJAWAB
Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut: a. Jabatan hendaklah mengenal pasti keperluan sebelum sebarang perolehan daripada syarikat atau pembangunan secara dalaman dilaksanakan; b. Pembangunan sistem aplikasi perlu mengambil kira sistem aplikasi sedia ada di JPN bagi mengelakkan pertindihan pembangunan aplikasi yang sama; c. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan PKS; d. Sistem yang dibangunkan perlu mendapat pengesahan melalui JPICT sebelum ianya dibangunkan dan diperluaskan;dan e. Penyediaan rekabentuk, pengaturcaraan dan pengujian dan pelaksanaan sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan.	ICTSO, ICTSM, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem.

10.1.2 MELINDUNGI TRANSAKSI PERKHIDMATAN APLIKASI

PERKARA	TANGGUNGJAWAB
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-perkara yang mesti dipatuhi adalah termasuk yang berikut: a. Memastikan kerahsiaan maklumat dan privasi pengguna terjamin; b. Memastikan keselamatan komunikasi dan protokol yang digunakan terjamin; dan c. Mematuhi garis panduan dan peraturan yang berkuatkuasa.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

10.1.3 PENYAMARAN DATA (DATA MASKING)

PERKARA	TANGGUNGJAWAB
Penyamaran data adalah kaedah menyembunyikan data bagi mengehadkan pendedahan data sensitif termasuk maklumat yang boleh dikenalpasti secara peribadi (contoh no. kad pengenalan, PII) dan untuk mematuhi keperluan undang-undang, akuan berkanun, peraturan dan kontrak. Teknik penyamaran data yang boleh digunakan adalah seperti : a. Penyulitan (memerlukan pengguna yang diberikan kebenaran untuk memiliki kunci); b. Mengosongkan atau menghapus aksara (menghalang pengguna yang tidak diberikan kebenaran daripada melihat mesej penuh);	ICTSO, ICTSM, Pengurus Projek ICT, Pentadbir Pangkalan Data Pentadbir Sistem

PERKARA	TANGGUNGJAWAB
c. Mengubah nombor dan tarikh; d. Substitusi (menukar satu nilai dengan nilai lain untuk menyembunyikan data sensitif); e. Menggantikan nilai dengan hash (#); dan f. Token.	

10.2 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN

OBJEKTIF

Memastikan keselamatan maklumat dilaksanakan di dalam kitar hayat pembangunan sistem.

10.2.1 DASAR KESELAMATAN PEMBANGUNAN SISTEM

PERKARA	TANGGUNGJAWAB
Perkara-perkara yang mesti dipatuhi adalah termasuk yang berikut: a. Memastikan kaedah keselamatan yang bersesuaian dikenal pasti, dirancang, dilaksanakan dan didokumentasi pada setiap peringkat perolehan, pembangunan dan penyelenggaraan sistem maklumat; b. Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem ICT; c. Memastikan pembangunan sistem menggunakan teknik pengekodan selamat (*secure coding*); d. Memastikan *tools* dan *libraries* yang digunakan adalah yang terkini;	CDO, ICTSO, Pengarah Bahagian/Negeri, ICTSM, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

PERKARA	TANGGUNGJAWAB
e. Pengemaskinian *patches* adalah bersesuaian dengan perisian lain; f. Melindungi kerahsiaan, integriti dan kesahihan maklumat menggunakan kaedah tertentu; g. Melaksanakan penyemakan ke atas input data sebelum disimpan ke dalam aplikasi bagi menjamin kesahihan dan ketepatan maklumat; h. Melaksanakan kawalan untuk mengesah dan melindungi integriti data dalam sistem aplikasi; i. Melaksanakan proses pengesahan ke atas ouput data (*validation*) bagi menjamin kesahihan dan ketepatan maklumat serta mengelak sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; j. Menjaga dan menjamin keselamatan sistem maklumat; dan k. Membangunkan Pelan Keselamatan Pengurusan Maklumat dengan merujuk Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) dan perlu disemak secara berkala mengikut keperluan serta perubahan.	

10.2.2 PROSEDUR KAWALAN PERUBAHAN SISTEM

PERKARA	TANGGUNGJAWAB
Perkara-perkara yang perlu dipatuhi adalah sebagaimana berikut: a. Mengawal perubahan dan / atau pindaan ke atas sistem dan memastikan sebarang perubahan adalah mengikut keperluan sahaja;	CDO, ICTSO, ICTSM, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

PERKARA	TANGGUNGJAWAB
b. Proses pengubahsuaian sistem hendaklah dikawal, diuji, disahkan dan direkod sebelum diguna pakai; c. Setiap permohonan perubahan / penambahbaikan sistem hendaklah didokumenkan bagi memantau dan mengawal perubahan / penambahbaikan yang dilaksanakan; d. Setiap perubahan mesti diuji untuk memastikan tiada impak negatif ke atas keselamatan dan perkhidmatan operasi organisasi; e. Sebarang perubahan yang melibatkan sistem pengoperasian dan perisian perlu diuji sebelum dipasang dalam *production server*; f. Perubahan sesuatu sistem hendaklah mendapat kelulusan Jawatankuasa yang dilantik berdasarkan jangkaan impak; dan g. Penilaian tahap keselamatan maklumat hendaklah dilaksanakan apabila terdapat perubahan ketara terhadap sistem.	

10.2.3 PROSES PENTAULIAHAN

PERKARA	TANGGUNGJAWAB
Proses pentauliahan melibatkan pewujudan peranan pentadbir dan pelaksanaan penilaian tahap keselamatan. a. Fungsi pentadbir adalah melaksanakan konfigurasi awal. Pentadbir merupakan satu peranan yang diberikan kepada pengguna tertentu dalam sistem. Peranan pentadbir boleh diberi dan dilucutkan oleh pentadbir lain; b. Sekurang-kurangnya dua (2) pentadbir diperlukan dalam sistem; c. Semasa pentauliahan, pengguna pertama hendaklah diberikan peranan sebagai pentadbir. Pengguna pertama boleh melantik pengguna-pengguna lain sebagai pentadbir dengan hak capaian yang sama; dan d. Penilaian tahap keselamatan hendaklah dilaksanakan sebelum pentaulihan sistem dan secara berkala semasa pelaksanaan dan apabila terdapat perubahan pada persekitaran.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

10.2.4 PROSES PELUCUTAN PENTAULIAHAN

PERKARA	TANGGUNGJAWAB
a. Proses pelucutan pentauliahan hendaklah dilaksanakan apabila sesuatu sistem tidak digunakan atau perlu ditamatkan; b. Sandaran penuh hendaklah dijalankan sebelum pelucutan pentauliahan; c. Migrasi data hendaklah berjaya dilaksanakan sebelum pelucutan pentauliahan; dan d. Pengurusan perubahan hendaklah dilaksanakan untuk memaklumkan kepada pihak berkaitan berhubung pelucutan pentauliahan sistem.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

10.2.5 PEMBANGUNAN SISTEM SECARA SUMBER LUAR

PERKARA	TANGGUNGJAWAB
Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut: a. Hak harta intelek, kod sumber dan data bagi sistem yang dibangunkan adalah menjadi hak milik JPN; b. Keperluan perjanjian hendaklah merangkumi amalan reka bentuk, pengaturcaraan dan pengujian yang selamat; c. Mengenal pasti risiko dan menentukan tahap kawalan keselamatan; d. Spesifikasi perolehan hendaklah mengandungi klausa berhubung keperluan keselamatan, ketersediaan kod sumber,	CDO, ICTSO, ICTSM, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
keperluan pelupusan data, keperluan migrasi data, keutamaan terhadap teknologi dan kepakaran tempatan, serta keperluan kompetensi pasukan pembangunan; dan e. Pihak ketiga hendaklah menjalani tapisan keselamatan sebelum memulakan kerja-kerja pembangunan sistem.	

10.2.6 PENGUJIAN PENERIMAAN SISTEM

PERKARA	TANGGUNGJAWAB
Perkara-perkara yang perlu dipatuhi adalah termasuk yang berikut: a. Menyediakan persekitaran pengujian yang bersesuaian; b. Memastikan penggunaan data pengujian yang bersesuaian dan lengkap; c. Menyediakan skrip pengujian yang lengkap dan bersesuaian; d. Mengenal pasti penguji sistem yang layak dan berpengalaman; dan e. Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan, bebas ralat dan memenuhi keperluan keselamatan maklumat sebelum sistem diguna pakai.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

10.3 DATA UJIAN

OBJEKTIF
Memastikan data pengujian dilindungi dan dikawal.

10.3.1 PERLINDUNGAN DATA UJIAN

PERKARA	TANGGUNGJAWAB
Perkara yang mesti dipatuhi termasuk yang berikut: a. Data dan kod pengaturcaraan yang hendak diuji perlu ditentukan, dilindungi dan dikawal; b. Hanya data yang diperlukan untuk tujuan pengujian sahaja digunakan; c. Pengujian hendaklah dibuat ke atas kod pengaturcaraan yang terkini; dan d. Setelah data pengujian tidak lagi diperlukan, data tersebut hendaklah dihapuskan.	Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pengguna.

BIDANG 11: HUBUNGAN DENGAN PEMBEKAL

11.1 KESELAMATAN MAKLUMAT DALAM HUBUNGAN DENGAN PEMBEKAL

OBJEKTIF

Memastikan aset ICT jabatan atau agensi yang boleh dicapai oleh pembekal dilindungi daripada akses yang tidak sewajarnya.

11.1.1 DASAR KESELAMATAN MAKLUMAT UNTUK PEMBEKAL

PERKARA	TANGGUNGJAWAB
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset JPN. Perkara yang mesti dipatuhi termasuk yang berikut: a. Memastikan perjanjian disediakan dan didokumentasikan dengan pembekal; b. Memastikan pembekal menandatangani Perakuan Polisi Keselamatan Siber JPN di **Lampiran 1**; c. Memastikan setiap pembekal melaksanakan tapisan keselamatan menerusi sistem *e-Vetting* yang disediakan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO); d. Menandatangani Perakuan Akta Rahsia Rasmi 1972; e. Mengenal pasti tahap capaian mengikut kategori pembekal; f. Merekod, mengawal dan memantau semua capaian pembekal; dan	Pengarah Bahagian/Negeri, ICTSO, Pengurus Projek ICT, Pentadbir Sistem, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
g. Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian;	

11.1.2 MENANGANI KESELAMATAN MAKLUMAT DALAM PERJANJIAN PEMBEKAL

PERKARA	TANGGUNGJAWAB
Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan kemudahan ICT untuk keperluan JPN. 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. JPN hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian 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 agensi berkaitan; d. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;	Pengarah Bahagian/Negeri, ICTSO, Pengurus Projek ICT, Pentadbir Sistem, Pihak Ketiga.

e. 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 Andaian yang dibuat berkaitan dengan skop penilaian. f. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan JPN; dan g. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh JPN.	

11.1.3 KAWALAN RANTAIAN PEMBEKAL TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

PERKARA	TANGGUNGJAWAB
Perjanjian dengan pembekal hendaklah mengambilkira keperluan keselamatan maklumat rantaian pembekal (*Supply Chain*) bagi menangani risiko keselamatan maklumat. Perkara-perkara yang perlu dilaksanakan adalah sebagaimana berikut: a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan	Pengarah Bahagian/Negeri, ICTSO, Pengurus Projek ICT, Pentadbir Sistem, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
perkhidmatan; b. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada sub-kontraktor atau pembekal-pembekal lain yang memberi perkhidmatan atau pembekalan produk; c. Pembekal utama hendaklah menyediakan surat rantaian yang mengandungi maklumat sub-kontraktor atau prinsipal/pengeluar kepada JPN; dan d. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	

11.2 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PEMBEKAL

OBJEKTIF

Untuk mengekalkan tahap keselamatan maklumat yang dipersetujui dengan penyampaian perkhidmatan adalah sama sebagaimana perjanjian pembekal.

11.2.1 PEMANTAUAN PERKHIDMATAN PEMBEKAL

PERKARA	TANGGUNGJAWAB
Jabatan hendaklah sentiasa memantau dan menyemak perkhidmatan pembekal. Perkara-perkara yang perlu dilaksanakan adalah sebagaimana berikut: a. Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; b. Menyemak laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan	CDO, Pengarah Bahagian/Negeri, ICTSO, ICTSM, Pengurus Projek ICT, Pihak Ketiga.

c. Memaklumkan mengenai insiden keselamatan kepada pembekal dan mengkaji insiden tersebut sebagaimana yang dikehendaki dalam perjanjian.	

11.2.2 PENGURUSAN PERUBAHAN PERKHIDMATAN PEMBEKAL

PERKARA	TANGGUNGJAWAB
Setiap perubahan perkhidmatan pembekal hendaklah dilaksanakan secara teratur dan mengikut tatacara/prosedur yang ditetapkan. Perkara yang perlu diambilkira adalah sebagaimana 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 hendaklah selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan sub-kontraktor.	CDO, ICTSO, ICTSM, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pihak Ketiga.

11.3 KESELAMATAN MAKLUMAT DAN PENGURUSAN PENYAMPAIAN PERKHIDMATAN PENGKOMPUTERAN AWAN (CLOUD)

OBJEKTIF

Untuk menyatakan dan mengurus keselamatan maklumat berkaitan pengunaan perkhidmatan pengkomputeran awan.

PERKARA	TANGGUNGJAWAB
JPN hendaklah memastikan keselamatan maklumat kerajaan adalah terjamin sebelum, semasa dan selepas penggunaan perkhidmatan pengkomputeran awan dengan mengambil kira perkara di bawah:	CDO, ICTSO, ICTSM,

PERKARA	TANGGUNGJAWAB
a. Mendapatkan kelulusan daripada pihak Pengurusan JPN dan MAMPU; b. Penggunaan perkhidmatan pengkomputeran awan perlu mematuhi Garis Panduan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam oleh CGSO dan Program Pengkomputeran Awan MAMPU; c. Melaksanakan penilaian risiko dan pengelasan maklumat sebelum dan semasa menggunakan perkhidmatan pengkomputeran awan; d. Memastikan perjanjian yang jelas antara pihak ketiga perkhidmatan pengkomputeran awan dan JPN. Perjanjian tersebut hendaklah mengandungi perkara di bawah: i. Pihak Ketiga hendaklah mempunyai pensijilan keselamatan yang berkaitan; ii. Mendokumentasikan dengan jelas tanggungjawab dan peranan pihak ketiga perkhidmatan pengkomputeran awan serta JPN; iii. Pihak ketiga hendaklah menyediakan mekanisme kawalan akses yang memenuhi keperluan JPN; iv. Pihak ketiga hendaklah menyediakan perisian bagi melindungi keselamatan maklumat daripada perisian hasad; v. Memproses dan menyimpan maklumat JPN di lokasi selamat (negara atau wilayah) yang telah diluluskan atau tertakluk kepada bidang kuasa tertentu; vi. Pihak ketiga hendaklah memberikan khidmat sokongan yang khusus sekiranya berlaku insiden keselamatan maklumat di persekitaran pengkomputeran awan;	Pengarah Bahagian/Pengarah Negeri, Pengurus Projek ICT, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
vii. Pihak ketiga hendaklah menyampaikan dan memastikan subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan turut mematuhi keperluan keselamatan maklumat JPN; viii. Pihak ketiga hendaklah menyokong JPN dalam mengumpulkan bukti digital termasuk mengambil kira undang-undang dan peraturan merentas bidang kuasa yang berbeza; ix. Pihak ketiga hendaklah menyediakan sokongan dan ketersediaan perkhidmatan untuk jangka masa yang sesuai apabila JPN ingin menamatkan perkhidmatan pengkomputeran awan; dan x. Pihak ketiga hendaklah turut mematuhi perkara 11.2.1 dan 11.2.2.	

BIDANG 12: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

12.1 PENGURUSAN DAN PENAMBAHBAIKAN INSIDEN KESELAMATAN SIBER

OBJEKTIF

a. Memastikan insiden keselamatan maklumat yang dilaporkan dapat diuruskan mengikut prosedur yang telah disediakan;
b. Meminimumkan kesan insiden yang berlaku; dan
c. Menambah baik kelemahan apabila berlaku insiden.

12.1.1 TANGGUNGJAWAB DAN PROSEDUR

PERKARA	TANGGUNGJAWAB
a. Tanggungjawab dan prosedur pengurusan hendaklah dirujuk untuk memastikan maklum balas terhadap insiden keselamatan dipatuhi mengikut prosedur yang telah disediakan; dan b. Ketua Jabatan adalah bertanggungjawab untuk memastikan Bahagian / Seksyen / Unit di bawah kawalannya mematuhi arahan mengenai pengurusan pengendalian insiden keselamatan ICT JPN dengan merujuk kepada pekeliling am, surat pekeliling am, garis panduan dan prosedur operasi *standard* yang telah dikeluarkan oleh Kerajaan.	KPPN, CDO, ICTSO, ICTSM, JPNCSIRT.

12.1.2 MEKANISME PELAPORAN INSIDEN

PERKARA	TANGGUNGJAWAB
Insiden keselamatan ICT atau ancaman mungkin berlaku ke atas aset ICT yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Berikut adalah insiden keselamatan ICT atau ancaman yang berlaku dan perlu dilaporkan kepada JPNCSIRT dan ICTSO dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Maklumat disyaki hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa; c. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; d. Kata laluan atau mekanisme kawalan akses disyaki/hilang, dicuri atau didedahkan; e. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan f. Berlaku percubaan menceroboh, penyelewengan dan insiden keselamatan siber yang tidak dijangka. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a. Surat Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam; b. *Information Security Incident Management Prosedure* (PS-JPN-SM-PS-17); dan	ICTSO, ICTSM, JPNCSIRT, *Helpdesk.*

PERKARA	TANGGUNGJAWAB
c. Lain-lain arahan / pekeliling berkaitan yang sedang berkuatkuasa.	

12.1.3 MELAPORKAN KELEMAHAN KESELAMATAN SIBER

PERKARA	TANGGUNGJAWAB
Semua warga JPN dan Pihak Ketiga yang menggunakan sistem dan perkhidmatan maklumat Jabatan dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT dengan segera kepada *Helpdesk* dan ICTSO. Semua warga JPN dan Pihak Ketiga adalah diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tetapi sebaliknya perlu terus melaporkan dengan segera bagi sebarang insiden keselamatan ICT, kerentanan yang diperhatikan atau disyaki terdapat dalam perkhidmatan dan sistem maklumat JPN. Ini adalah bagi mengelakkan kerosakan dan kehilangan bahan bukti pencerobohan atau cubaan pencerobohan.	Semua.

12.1.4 PENILAIAN DAN KEPUTUSAN MENGENAI AKTIVITI KESELAMATAN SIBER

PERKARA	TANGGUNGJAWAB
Insiden keselamatan maklumat hendaklah dinilai dan diputuskan oleh ICTSO sama ada untuk diklasifikasikan sebagai insiden. Penetapan insiden adalah berdasarkan keutamaan berikut : a. Keutamaan 1 - Insiden keselamatan siber yang memberi impak tinggi terhadap pertahanan dan keselamatan negara, kestabilan ekonomi negara, imej negara, keupayaan kerajaan untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu. b. Keutamaan 2 - Insiden keselamatan siber yang tidak memberi impak seperti mana yang dinyatakan dalam Keutamaan 1. Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk. ICTSO melaporkan kepada KDNCSIRT / NACSA apabila berlaku insiden keselamatan siber sekiranya perlu.	ICTSO, ICTSM, Pengarah Bahagian/Negeri, JPNCSIRT, JKICT.

12.1.5 TINDAK BALAS INSIDEN KESELAMATAN SIBER

PERKARA	TANGGUNGJAWAB
Insiden keselamatan maklumat hendaklah dikendalikan mengikut prosedur yang telah ditetapkan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah sebagaimana berikut: a. Menganalisa maklumat insiden keselamatan ICT bagi tujuan perancangan dan tindakan; b. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah berkualiti, lengkap dan boleh dipercayai. Ia perlu disediakan, disimpan, diselenggara dan dilindungi selepas insiden keselamatan berlaku; c. Menjalankan kajian forensik sekiranya perlu; d. Menghubungi pihak yang berkenaan dengan segera; e. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; f. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; g. Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; h. Menyediakan tindakan pemulihan segera; dan i. Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	ICTSO, JPNCSIRT.

12.1.6 PENGALAMAN DARI INSIDEN KESELAMATAN SIBER

PERKARA	TANGGUNGJAWAB
Aktiviti keselamatan maklumat hendaklah dinilai dan diputuskan sama ada untuk diklasifikasikan sebagai insiden keselamatan maklumat. Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan, dilindungi dan dianalisis bagi tujuan perancangan dan tindakan untuk melaksanakan peningkatan dan kawalan tambahan bagi mengawal kekerapan, kerosakan dan kos kejadian insiden akan datang, dan untuk tujuan mengkaji semula dasar-dasar keselamatan aset ICT sedia ada. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada JPN.	ICTSO, ICTSM, JPNCSIRT.

BIDANG 13: ASPEK KESELAMATAN MAKLUMAT DALAM PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

13.1 KESELAMATAN MAKLUMAT BAGI KESINAMBUNGAN PERKHIDMATAN

OBJEKTIF

Memastikan keselamatan maklumat dalam pengurusan kesinambungan perkhidmatan.

JPN hendaklah menentukan keperluan untuk memastikan keselamatan maklumat terpelihara dalam situasi kecemasan dengan mengambil kira faktor dalaman dan luaran yang boleh memberikan impak kepada kesinambungan sistem penyampaian perkhidmatan dan fungsi Jabatan.

PERKARA	TANGGUNGJAWAB
Perkara-perkara berikut hendaklah diambil kira: a. Merancang dan mengenal pasti keperluan keselamatan maklumat; b. Membangun, melaksana, menguji dan menyelenggara pelan kesinambungan perkhidmatan (PKP) dan pemulihan sistem selepas bencana; dan c. Mematuhi dasar, arahan dan prosedur yang berkuatkuasa.	Bahagian Pentadbiran JPN

13.1.1 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

PERKARA	TANGGUNGJAWAB
Mengurus dan memastikan keperluan pihak berkepentingan dilindungi dan imej JPN terpelihara dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan JPN di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Perkara yang	Bahagian Pentadbiran JPN (BP)

PERKARA	TANGGUNGJAWAB
perlu dipertimbangkan adalah seperti berikut: a. Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP); dan b. Melaksana Kajian Impak Perkhidmatan (*Business Impact Analysis, BIA) dan* Penilaian Risiko terhadap perkhidmatan kritikal.	

13.1.2 PELAN KESINAMBUNGAN PERKHIDMATAN (PKP)

PERKARA	TANGGUNGJAWAB
Menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan JPN. Ini bertujuan memastikan tindakan pemulihan yang cekap dan berkesan dilaksanakan apabila berlakunya musibah atau bencana. Perkara-perkara yang hendaklah dipatuhi termasuk yang berikut: **a. Perakuan Pengurusan** Pelan ini mestilah diperakukan oleh pengurusan JPN. **b. Program Latihan / Kesedaran** Program latihan / kesedaran kepada semua kakitangan JPN mengenai pelan ini dan proses serta prosedur yang terlibat perlu dilaksanakan. **c. Penyelenggaraan Pelan** Pelan Kesinambungan Perkhidmatan perlu diselenggara secara berkala dan diuji pelaksanaannya terutama apabila terdapat perubahan dalam operasi dan sistem penyampaian perkhidmatan JPN / Kerajaan.	Bahagian Pentadbiran JPN (BP)

PERKARA	TANGGUNGJAWAB
Pelan Kesinambungan Perkhidmatan (PKP) terdiri daripada tiga (3) sub-pelan berikut: a. Pelan Tindakbalas Kecemasan (*Emergency Response Plan, ERP*); b. Pelan Pemulihan Bencana (*Disaster Revovery Plan, DRP*); dan c. Pelan Komunikasi Krisis (*Crysis Communcation Plan, CCP*).	

13.1.3 KETERSEDIAAN ICT UNTUK KESINAMBUNGAN OPERASI

PERKARA	TANGGUNGJAWAB
JPN hendaklah menyediakan, mendokumenkan, melaksanakan, menyelenggara dan menguji proses, prosedur dan kawalan berkaitan ICT bagi memastikan ketersediaan maklumat serta aset ICT sekiranya berlaku bencana atau gangguan. JPN hendaklah melaksanakan perkara berikut: a. Memastikan JPN menyediakan keperluan sumber manusia yang mencukupi; b. Mewujudkan struktur tadbir urus beserta peranan dan tanggungjawab berkaitan ICT; c. Memastikan Pasukan Pemulihan Bencana (*Disaster Recovery Team* - DRT) dan Pasukan Penilaian Bencana (*Disaster Assessment Team* – DAT) terkini; d. DRT dan DAT mempunyai tahap kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksanakan ITDRP (*IT Disaster Recovery Plan*);	KPPN, CDO, ICTSO, ICTSM, Pengarah Bahagian / Pengarah Negeri, Pentadbir Sistem, Koordinator DR, Pengguna, Pihak Ketiga.

PERKARA	TANGGUNGJAWAB
e. Mewujudkan dan mengemas kini ITDRP jika berlaku perubahan seperti fungsi kritikal, pertukaran pegawai dan penambahbaikan berdasarkan keputusan pengujian; dan f. Melaksanakan pengujian Pemulihan Bencana secara berkala berdasarkan objektif JPN serta melaksanakan *post-mortem*. JPN hendaklah menyediakan, mendokumenkan, melaksanakan, menyelenggara dan menguji proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Melaksanakan ITDRP apabila terdapat gangguan ke atas perkhidmatan kritikal JPN yang telah dikenal pasti. b. Mengemaskini dokumen ITDRP berkaitan perkara berikut : i. Berlaku perubahan kepada fungsi kritikal JPN; dan ii. Perubahan struktur tadbir urus ITDRP JPN seperti pertukaran pegawai, bersara dan bertukar keluar. c. Memastikan Pasukan ITDRP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksanakan ITDRP.	

BIDANG 14: PEMATUHAN

14.1 PEMATUHAN TERHADAP KEPERLUAN PERUNDANGAN DAN PERJANJIAN KONTRAK

OBJEKTIF

Meningkat dan memantapkan tahap keselamatan ICT bagi mengelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.

14.1.1 HAK HARTA INTELEK

PERKARA	TANGGUNGJAWAB
Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan di mana mematuhi had pengguna yang telah ditetapkan atau dibenarkan dan hanya menggunakan perisian yang mempunyai lesen yang sah.	CDO, ICTSO, ICTSM, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pihak Ketiga.

14.1.2 PERLINDUNGAN REKOD

PERKARA	TANGGUNGJAWAB
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan sebagaimana yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.	Kakitangan JPN, Pihak Ketiga.

14.1.3 PRIVASI DAN PERLINDUNGAN MAKLUMAT PERIBADI

PERKARA	TANGGUNGJAWAB
Semua kakitangan JPN dan Pihak Ketiga hendaklah memberi jaminan dalam melindungi maklumat peribadi individu seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia. Perkara yang hendaklah dipatuhi adalah sebagaimana berikut: a. Tidak mendedahkan maklumat peribadi individu kepada mana-mana pihak yang tidak berkenaan; b. Memastikan kawalan penyimpanan rekod maklumat peribadi individu di tempat yang selamat; dan c. Maklumat peribadi individu hanya boleh digunakan untuk tujuan rasmi dan dengan kebenaran.	Pengarah Bahagian/Negeri, Kakitangan JPN, Pihak Ketiga.

14.1.4 MENGENAL PASTI UNDANG-UNDANG DAN PERJANJIAN KONTRAK

PERKARA	TANGGUNGJAWAB
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh kakitangan JPN dan Pihak Ketiga. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi (rujuk **Lampiran 2**).	Kakitangan JPN, Pihak Ketiga.

14.2 KAJIAN KESELAMATAN MAKLUMAT

OBJEKTIF

Untuk memastikan keselamatan maklumat dilaksanakan mengikut polisi dan prosedur yang sedang berkuatkuasa.

14.2.1 KAJIAN BEBAS / PIHAK KETIGA TERHADAP KESELAMATAN MAKLUMAT

PERKARA	TANGGUNGJAWAB
Penilaian keselamatan maklumat oleh Pihak Ketiga hendaklah dilaksanakan sebagaimana yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	CDO, ICTSO, Pengurus Projek ICT, Pentadbir Sistem, Pihak Ketiga.

14.2.2 PEMATUHAN DASAR DAN STANDARD/PIAWAIAN

PERKARA	TANGGUNGJAWAB
Jabatan hendaklah membuat kajian semula secara berkala terhadap pematuhan dasar dan standard / piawaian keselamatan pemprosesan maklumat dan prosedur yang dipertanggungjawabkan agar selari dengan standard / piawaian yang terkini.	Pengurusan Tertinggi JPN, Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pengguna.

14.2.3 KAJIAN SEMULA PEMATUHAN TEKNIKAL

PERKARA	TANGGUNGJAWAB
Melaksanakan kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur sebagaimana di dalam polisi, piawaian dan keperluan teknikal.	Pengarah Bahagian/Negeri, CDO, ICTSO, ICTSM.

Lampiran 1

PERAKUAN
POLISI KESELAMATAN SIBER
JABATAN PENDAFTARAN NEGARA MALAYSIA

Nama (Huruf Besar) : ……..…..

Nombor Kad Pengenalan : ……..…….....

Jawatan/Gred : ……..……..

Bahagian / Cawangan / Syarikat: ....…….....

Adalah dengan sesungguhnya dan sebenarnya saya mengaku bahawa:-

1. Telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber JPN;

2. Berjanji akan menghayati Polisi Keselamatan Siber JPN sepenuhnya pada setiap masa demi menjaga nama baik Jabatan dan Negara;

3. Akur akan sebarang pindaan Polisi Keselamatan Siber JPN; dan

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

Tandatangan : ……

Tarikh : ……

Tandatangan tidak diperlukan jika perakuan dibuat secara atas talian.

Lampiran 2

UNDANG-UNDANG DAN PERJANJIAN KONTRAK

1. Akta Aktiviti Kerajaan Elektronik 2007 (Akta 680);
2. Akta Arkib Negara 2003;
3. Akta Hak Cipta (Pindaan) Tahun 1997;
4. Akta Jenayah Komputer 1997;
5. Akta Kawasan Larangan dan Tempat;
6. Akta Keselamatan Dalam Negeri 1960;
7. Akta Komunikasi dan Multimedia 1998;
8. Akta Pendaftaran Negara;
9. Akta Perlindungan Data Peribadi 2010;
10. Akta Rahsia Rasmi 1972;
11. Akta Tandatangan Digital 1997;
12. Arahan Keselamatan;
13. Arahan Perbendaharaan;
14. Arahan Teknologi Maklumat 2007;
15. Artikel “Penerapan Etika Penggunaan Media Sosial dalam Sektor Awam” terbitan MAMPU;
16. Dasar Kriptografi Negara 12 Julai 2013;
17. Etika Penggunaan E-mel dan Internet MAMPU;
18. Garis Panduan Dan Polisi Perkakasan;
19. Garis Panduan Dan Polisi Rangkaian;
20. Garis Panduan Pembangunan Laman *Web*;

21. Garis Panduan Penggunaan Internet Dan Mel Elektronik JPN;

22. Kawalan Keselamatan Rahsia Rasmi dan Dokumen Rasmi Kerajaan Yang Dikelilingkan Melalui Surat KPKK(R)200/55 KLT.7(21) bertarikh 21 Ogos 1999;

23. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS);

24. Manual Prosedur Kerja (MPK);

25. Panduan Keperluan Dan Persediaan Pelaksanaan Pensijilan MS ISO / IEC 27001 : 2013 Dalam Sektor Awam;

26. Pekeliling Am Bilangan 3 Tahun 2000 : Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi;

27. Pekeliling Am Bilangan 1 Tahun 2001 : Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

28. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 : Garis Penduan Mengenai Tatacara Penggunaan Internet Mel Elektronik di Agensi – agensi Kerajaan;

29. Pekeliling Perkhidmatan Bil. 17 Tahun 2001: Penguatkuasaan Surat Aku Janji Untuk Pegawai;

30. Pekeliling Perkhidmatan Bil. 3 Tahun 2004 : Panduan Pertukaran Pegawai;

31. Pekeliling Perkhidmatan Bil. 5 2007 : Panduan Pengurusan Pejabat bertarikh 30 April 2007;

32. Pekeliling Transformasi Pentadbiran Awam Bil. 3 Tahun 2017 : Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan (Government Unified Communication (1GovUC));

33. Pekeliling 1PP: Tatacara Pengurusan Aset Alih;

34. Pelan Kesinambungan Perkhidmatan (PKP);

35. Peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993;
36. Perintah-Perintah Am;

37. *Personal Data Protection Act* (PDPA) 2010;

38. PKPA Bil.4 Tahun 2018, MyPortfolio : Panduan Kerja Sektor Awam;

39. Prosedur Pengurusan Pelaporan Dan Pengendalian Insiden Keselamatan ICT MAMPU;

40. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA);

41. *Standard Operating Procedure* (SOP) ICT;

42. Surat Arahan MAMPU BDPICT (S)700 – 6/1/3(21) bertarikh 19 November 2009 : Penggunaan Media Jaringan Sosial di Sektor Awam;

43. Surat Arahan Ketua Pengarah MAMPU bertarikh 8 April 2011: Amalan Terbaik Penggunaan Media Jaringan Sosial Di Sektor Awam;

44. Surat Arahan Ketua Pengarah Perkhidmatan Awam Jabatan Perkhidmatan Awam Malaysia (JPA) bertarikh 7 Jun 2013 :Tanggungjawab Pegawai Awam dalam Memelihara Integriti Perkhidmatan Awam Semasa Menggunakan Kemudahan Media Sosial di Internet;

45. Surat Bil. KPKK/308/A(2) bertarikh 7/9/79.(mencetak Pas–Pas Keselamatan dan Kad-Kad Pengenalan Kementerian/Jabatan);

46. Surat Pekeliling Am Bil. 2 Tahun 1987 – Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukkan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1976;

47. Surat Pekeliling Am Bil. 6 Tahun 2005 : Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

48. Surat Pekeliling Am Bil. 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

49. Surat Pekeliling Am Rahsia Bil.1 Tahun 1975. (Keselamatan Jabatan-jabatan Kerajaan);

50. Surat Pekeliling Perbendaharaan Bil.2 / 1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

51. Surat Pekeliling Perbendaharaan Bil. 3 / 1995 - Peraturan Perolehan Perkhidmatan Perundingan;

52. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh NACSA bertarikh 28 Januari 2019

53. 1 Pekeliling Perbendaharaan (1PP) – Pengurusan Aset; dan

54. Akta, Pekeliling, Surat Pekeliling, Surat Arahan, Garis Panduan dan peraturan-peraturan lain yang berkuatkuasa.

55. Surat Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam

GLOSARI

a. **Ancaman**
Apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah.

b. **Aset ICT**
Aset ICT dikategori kepada lima (5) elemen iaitu perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia yang mengendalikan aset ICT.

c. **CDO**
Pengarah Bahagian Pengurusan Teknologi Maklumat dan Komunikasi (BTM).

d. ***Clear Desk***
Tidak meninggalkan sebarang dokumen yang sensitif di atas meja.

e. ***Clear Screen***
Tidak memaparkan sebarang maklumat sensitif apabila komputer berkenaan ditinggalkan.

f. **Enkripsi (*Encryption*)**
Satu proses penyulitan data supaya tidak difahami oleh orang lain kecuali penerima yang sah.

g. **ICTSO**
Pegawai Keselamatan ICT.

h. **ICTSM**
Pengurus Keselamatan ICT.

i. **Insiden Keselamatan**
Musibah (*adverse event*) yang berlaku ke atas sistem maklumat.

j. **JPNCSIRT**
Pasukan yang dilantik oleh CDO dan bertanggungjawab dalam mengurus pengendalian insiden keselamatan ICT di JPN. JPNCSIRT turut menganggotai KDNCSIRT.

k. **Kawasan Terperingkat**
Kawasan terperingkat ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi kakitangan JPN yang tertentu sahaja.

l. **Kerentanan *(Vulnerability*)**
Sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman.

m. **Kriptografi**
Satu sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.

n. **Maklumat Peribadi Individu**
Maklumat peribadi individu antaranya adalah nama, alamat, nombor kad pengenalan dan nombor passport.

o. **Pentadbir Sistem**
Individu yang dipertanggungjawabkan ke atas sistem / rangkaian yang ditadbir olehnya. Pentadbir sistem terdiri daripada Pentadbir Aplikasi, Pentadbir E-mel / Internet, Pentadbir Laman *Web*, Pentadbir Teknikal, Rangkaian dan Keselamatan Rangkaian, Pentadbir Pangkalan Data, Pembangun Sistem dan lain-lain pentadbir sistem yang berkaitan.

p. **Pegawai Aset**
Pegawai yang bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik. Ia terdiri daripada Ketua Pejabat atau Pegawai Aset Bahagian / Pegawai Aset Negeri / Pegawai Aset Cawangan yang dilantik oleh Urusetia Aset JPN.

q. **Pengarah Sumber Manusia**
Pegawai yang bertanggungjawab dalam aspek pengurusan dan pembangunan sumber manusia.

r. **Pengurus Projek ICT**
Disandang oleh Pegawai Teknologi Maklumat yang mengetuai dalam pelaksanaan ICT.

s. **Penilaian Risiko**
Penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.

t. **Pihak Ketiga**
Terdiri daripada pembekal, pakar perunding, agensi luar, pelawat dan pihak – pihak luar seperti panel audit dan tenaga pengajar.

u. ***Public Key Infrastructure (PKI)***
Satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui internet.

v. **Risiko**
Kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian.

w. **Sandaran (*Backup*)**
Proses penduaan sesuatu dokumen atau maklumat.

APENDIKS A: REKOD PINDAAN

Versi	Tarikh	Keterangan	Penulis
1.0	30 Julai 2018	Pengemaskinian Dasar Keselamatan ICT (DKICT) Versi 1.5 kepada Polisi Keselamatan Siber Jabatan Pendaftaran Negara (JPN) dengan merujuk kepada Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) MAMPU Versi 1.0, April 2016.	Rosnita binti Abdul Kahar
2.0	6 September 2021	1) Pengemaskinian Polisi Keselamatan Siber Jabatan Pendaftaran Negara (JPN) versi 1.0 kepada versi 2.0 dengan berdasarkan Polisi Keselamatan Siber MAMPU, 24 September 2020 dan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) MAMPU Versi 1.0, April 2016. 2) Mengeluarkan tajuk English. 3) Pindaan tempoh kepada sekurang- kurangnya lima (5) tahun sekali atau mengikut keperluan semasa bagi memastikan dokumen sentiasa dipatuhi. 4) Pengemaskinian peranan dan tanggungjawab Pengurus Projek ICT bagi Pengurus Projek. 5) Pindaan peranan dan tanggungjawab Pentadbir Sistem bagi Pentadbir Sistem, Pentadbir Sistem Aplikasi, Pembangun Sistem, Pemilik Sistem, Pentadbir Laman Web (*Webmaster*), Pentadbir Emel, Pentadbir Teknikal, Rangkaian & Keselamatan Rangkaian, Pegawai Aset, Pengurus Pusat Data & *Disaster Recovery* (DRC) di Bidang 2. 6) Penambahan maklumat keanggotaan JPNCERT di Bidang 2. 7) Pindaan pembekal, perunding, pengguna luar dan pihak-pihak lain yang berkepentingan kepada Pihak Ketiga. 8) 3.2.3 Proses Tatatertib Penambahan pernyataan: ● Kakitangan JPN dan Pihak Ketiga yang melanggar	Laila binti Abdul Majid

Versi	Tarikh	Keterangan	Penulis
		polisi ini juga boleh digantung daripada mendapat capaian kepada kemudahan ICT JPN. 9) 5.2.1 Pengurusan Akaun Pengguna. Penambahan pernyataan: ● Pendaftaran dan penamatan akaun pengguna hendaklah menggunakan kaedah dan garis panduan yang ditetapkan; ● Akaun pengguna luar yang diwujudkan hendaklah diberi tahap capaian dan tempoh masa mengikut peranan dan tanggungjawab pengguna dan dengan kelulusan Pengurusan Tertinggi JPN; dan ● Bercuti belajar melebihi tempoh 6 bulan. 10) 5.2.2 Pengurusan Hak Capaian Pengguna. Penambahan pernyataan: ● Pengarah Bahagian / Negeri dan penyelia hendaklah memastikan hak akses kakitangan seliaan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat ke atas sistem utama JPN hendaklah dibatalkan / dikemaskini sekiranya terdapat perubahan bidang tugas seperti bertukar skop, bertukar Jabatan dan penamatan perkhidmatan. 11) 5.3.1 Pengurusan Kata Laluan Mengeluarkan pernyataan: ● Menukar kata laluan sekurang-kurangnya setiap tiga (3) bulan. Penambahan pernyataan: ● Kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan; ● Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan; ● Sistem hendaklah mempunyai tempoh masa aktif akan tamat selepas tempoh *idle* yang ditetapkan; ● Sistem yang dibangunkan hendaklah mempunyai kemudahan menukar kata laluan oleh pengguna; ● Pertukaran kata laluan selepas *login* kali pertama atau selepas *reset* kata laluan hendaklah dikuat kuasakan; dan ● Kemasukan kata laluan bagi capaian sistem hendaklah mempunyai had maksimum. Setelah mencapai tahap maksimum, capaian kepada sistem	

Versi	Tarikh	Keterangan	Penulis
		akan disekat sehingga ID capaian diaktifkan semula. 12) 6.1.2 Pengurusan Kunci Awam. Penambahan pernyataan: ● Perlaksanaan pengurusan kekunci kriptografi adalah berpandukan Perkhidmatan Prasarana Kunci Awam Kerajaan (GPKI) dan peraturan yang sedang berkuatkuasa. 13) Penukaran perkataan Kawasan Larangan kepada Kawasan Terperingkat. 14) Mengeluar tajuk Kawasan Penghantaran dan Pemunggahan di Bidang 7. 15) 7.2.5 Perkakasan ICT Dibawa Keluar Premis. Penambahan pernyataan: ● Sekiranya perkakasan ICT dibawa keluar untuk tujuan penyelenggaraan, pemilik aset hendaklah memeriksa dan memastikan perkakasan ICT yang dibawa keluar tidak mengandungi maklumat rasmi Kerajaan. 16) 8.5.1 Pemasangan Perisian Pada Sistem Operasi. Penambahan pernyataan: ● Memastikan penggunaan perisian mempunyai lesen sah. 17) 8.7.1 Kawalan Audit Sistem Maklumat. Penambahan pernyataan: ● Laporan audit ICT perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan. 18) 9.2.1 Polisi dan Prosedur Pemindahan Maklumat. Penambahan pernyataan: ● Pemindahan maklumat hendaklah mendapat kelulusan daripada KPPN. 19) 9.4 Pengurusan Perkhidmatan Kiosk. Penambahan pernyataan: ● Penempatan kiosk hendaklah ditempatkan di kawasan yang selamat dan mudah dipantau. 20) 10.1.1 Analisa Keperluan dan Spesifikasi Keselamatan Maklumat. Penambahan pernyataan:	

Versi	Tarikh	Keterangan	Penulis
		● Pembangunan sistem aplikasi perlu mengambilkira sistem sedia ada di JPN bagi mengelakkan pertindihan pembangunan sistem yang sama. 21) 10.2.1 Dasar Keselamatan Pembangunan Sistem. Penambahan pernyataan: ● Memastikan pembangunan sistem menggunakan teknik pengekodan selamat (*secure coding*). 22) 11.2.1 Dasar Keselamatan Maklumat Untuk Pembekal. Penambahan pernyataan: ● Mengenal pasti tahap capaian mengikut kategori pembekal. 23) 14.1.3 Privasi dan Perlindungan Maklumat Peribadi. Penambahan pernyataan: ● Tidak mendedahkan maklumat peribadi individu kepada mana-mana pihak yang tidak berkenaan; ● Memastikan kawalan penyimpanan rekod maklumat peribadi individu di tempat selamat; dan ● Maklumat peribadi individu hanya boleh digunakan untuk tujuan rasmi dan dengan kebenaran. 24) Pengemaskinian 14.1.4 Mengenal pasti Undang-Undang dan Perjanjian Kontrak kepada Lampiran 2. 25) Pengemaskinian takrifan di Glosari.	
2.1	3 April 2024	1. Menukar ayat Polisi Keselamatan Siber kepada akronim PKS 2. Menukar akronim CIO kepada CDO 3. Perubahan logo JPN kepada logo Jata Negara. 4. Perubahan nombor dokumen. 5. Perubahan kaki dokumen – hapsu perkataan Terhad. 6. Perubahan ISO/IEC 27001:2013 kepada ISO/IEC 27001. 7. Menukar nama ***COMPUTER EMERGENCY RESPONSE TEAM*** **(JPNCERT)** kepada **JPN *Cyber Security Insiden Response Team*** **(JPNCSIRT)**	Zaiton Binti Ahmad

Versi	Tarikh	Keterangan	Penulis
		8. Bidang 1 Para 1.1 Pelaksanaan Polisi Perubahan penyataan : ● Polisi hendaklah dilaksanakan oleh pihak pengurusan ● Tambahan tanggungjawab : JPIC dan JKICT 9. Bidang 1 Para 1.3 Penyelenggaraan Polisi Penambahan penyataan : ● Prosedur Operasi Standard/Dasar Tambah tanggungjawab : ● ICTSM 10. Bidang 2 Para 2.1 Struktur Organisasi Keselamatan Penambahan penyataan : Ketua Pegawai Digital (CDO) ● a. Melaksana dan menyelaras penggunaan dasar, standard dan amalan terbaik ● f. Meneraju perubahan melalui penjajaran Pelan Strategik Pendigitalan JPN dengan keperluan Pelan Strategik Kementerian dan Pelan Strategik Sektor ● g. Menyelaras penggalakan pembudayaan ICT, dan Inovasi Pendigitalan dalam Sistem Penyampaian JPN dan Perkhidmatan ● h. Melantik ICTSO serta memaklumkan pelantikan kepada MAMPU dan NACSA Pegawai Keselamatan ICT (ICTSO) ● a. Memastikan kajian dan semakan semula serta pelaksanaan standard keselamatan ICT selaras dengan keperluan ● b. Menguatkuasa PKS kepada semua pengguna dan Pihak Ketiga ● d. Menyedia dan menyebarkan panduan yang sesuai berkaitan keselamatan ICT dan	

Versi	Tarikh	Keterangan	Penulis
		memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang ● e. Mengurus pasukan JPN Cyber Security Insiden Response Team (JPNCSIRT) ● f. Melaporkan insiden keselamatan ICT kepada KDNCSIRT dalam membantu penyiasatan atau pemulihan ● g. Melaporkan insiden keselamatan ICT kepada CDO bagi insiden yang memerlukan pengaktifan Pelan Disaster Recovery Plan (DRP) yang terkandung di dalam Pelan Pengurusan Kesinambungan Perkhidmatan (PKP) ● l. Memastikan pelaksanaan latihan dan program kesedaran keselamatan ICT dari semasa ke semasa ● j. Memastikan pelaksanaan latihan dan program kesedaran keselamatan ICT dari semasa ke semasa. Pengurus Keselamatan ICT (ICTSM) ● d. Menyedia dan melaksanakan latihan dan program kesedaran keselamatan ICT dari semasa ke semasa ● g. Memastikan rekod bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT didokumenkan; dan ● h. Mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan ICT Pengarah Bahagian/Pengarah Negeri ● a. Melaksana dan memastikan semua kakitangan JPN dan Pihak Ketiga mematuhi PKS / Akta / Pekeliling / Arahan / Peraturan / Garis Panduan / Prosedur Operasi Standard (SOP) / Dasar yang sedang berkuatkuasa ● i. Memberi perakuan tindakan tatatertib ke atas pengguna yang melanggar PKS / Akta / Pekeliling / Arahan / Peraturan / Garis Panduan / Prosedur Operasi Standard (SOP) / Dasar yang sedang berkuatkuasa	

Versi	Tarikh	Keterangan	Penulis
		Pengurus projek ICT ● e. Memastikan pembekal dan rakan usahasama memohon tapisan keselamatan dan memperaku PKS; Pentadbir Sistem ● d. Memahami dan mematuhi PKS dan sebarang prosedur berkaitan dalam mewujudkan akaun pengguna ke atas setiap sistem; Jawatankuasa Keselamatan ICT (JKICT) ● Peranan dan tanggungjawab JKICT adalah sebagaimana berikut : a. Merancang dan memantau Dasar, Strategi dan Pelan Tindakan infrastruktur dan Keselamatan ICT b. Merancang, mencadang pengemaskinian dan memantau pelaksanaan Polisi Keselamatan Siber (PKS) c. Merancang dan memantau perolehan infrastruktur, perkakasan, aplikasi dan perisian Keselamatan ICT d. Merancang Program Keselamatan ICT e. Menyelaras dan memantau Rangkaian Komunikasi dan Sistem E-Mel f. Menyelaras dan memantau Pelaksanaan Keselamatan ICT g. Melapor perancangan, Status Pelaksanaan dan Pemantauan serta sebagai Penasihat Keselamatan ICT kepada Jawatankuasa Pemandu ICT (JPICT) Ahli-ahli : 1. ICTSO 2. KPP 3. PPK 4. PP JPN *CYBER SECURITY INCIDENT RESPONSE TEAM* (JPNCSIRT) Keanggotaan JPNCSIRT adalah sebagaimana berikut: a. Pengarah CSIRT : CDO b. Pengurus CSIRT I : ICTSO c. Pengurus CSIRT II: ICTSM	

Versi	Tarikh	Keterangan	Penulis
		Ahli a. Timbalan Pengarah Kanan BTM b. Timbalan Pengarah BTM c. Ketua Penolong Pengarah BTM d. Pentadbir Rangkaian dan Keselamatan Rangkaian e. Pentadbir Portal f. Pentadbir Pangkalan Data g. Pentadbir Aplikasi h. Pentadbir Pusat Data & Pusat Pemulihan Bencana i. Pentadbir Server dan Helpdesk j. Urusetia Meja Bantuan ICT (Helpdesk) ● a. Menerima aduan daripada pengguna berkaitan masalah ICT yang dihadapi; ● c. Menyalurkan aduan yang telah dilaporkan kepada pegawai bertanggungjawab untuk penyelesaian Pengguna ● e. Melaksanakan tugasan mengikut PKS / Akta / Pekeliling / Arahan / Peraturan / Garis Panduan / Prosedur Operasi Standard (SOP) / Dasar yang sedang berkuatkuasa ● g. Melaksanakan langkah-langkah perlindungan sebagaimana berikut: viii. Melaporkan aktiviti yang mengancam keselamatan ICT seperti Denial-Of-Service (DOS), Distributed Denial-Of-Service (DDoS), Pencerobohan (*Intrusion*), Jangkitan Perisian Hasad (*Malicious Software/Malware*), Pengehosan Perisian Hasad (*Malware Hosting*), Percubaan Pencerobohan (*Intrusion Attempt*), Potensi Serangan (*Potential Attack*) kepada Pentadbir Sistem dengan segera ix. Selain perkara viii di atas perlu dilaporkan kepada Meja Bantuan (Helpdesk) Jabatan Pihak Ketiga ● b. Bersetuju dan menandatangani Perakuan PKS di **Lampiran 1**;	

Versi	Tarikh	Keterangan	Penulis
		● d. Membuat permohonan / telah mendapatkan kelulusan tapisan keselamatan; ● f. Mematuhi Akta / Pekeliling / Arahan / Peraturan / Garis Panduan / Prosedur Operasi Standard (SOP) / Dasar yang sedang berkuatkuasa 11. Bidang 2 Tambahan para 2.2 Pengasingan Tugas 12. Bidang 2 Tambahan para 2.3 Hubungan Dengan Pihak Berkuasa 13. Bidang 2 Tambahan para 2.4 Hubungan Kumpulan Berkepentingan Yang Khusus 14. Bidang 3 Para 3.1.1 Tapisan Keselamatan Penambahan penyataan : Ketua Jabatan bertanggungjawab menjalankan tapisan keselamatan terhadap kakitangan JPN dan Pihak Ketiga yang mempunyai urusan dengan perkhidmatan ICT JPN yang terlibat berasaskan kepada keperluan perundangan, peraturan dan etika terpakai selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan. 15. Bidang 3 Para 3.2.2 Latihan Pendidikan dan Kesedaran Keselamatan Maklumat Perubahan tajuk : 3.2.2 KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT Penambahan penyataan : ● a. Memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber JPN, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk / fungsi / aplikasi / sistem	

Versi	Tarikh	Keterangan	Penulis
		keselamatan secara berterusan dalam melaksanakan tugas - tugas dan tanggungjawab ● b. Memastikan kesedaran yang berkaitan Polisi Keselamatan Siber JPN perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa 16. Bidang 3 Para 3.2.3 Proses Tatatertib Perubahan penyataan : ● Ketua Unit Integriti 17. Bidang 3 Para 3.3.1 Tanggungjawab Apabila Penamatan Atau Pertukaran Perkhidmatan Penambahan penyataan : ● c. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan JPN dan/atau terma perkhidmatan yang ditetapkan ● d. Maklumat rasmi JPN dalam peranti tidak dibenarkan dibawa keluar dari JPN ● f. Menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada Penyelia yang berkaitan (bagi kakitangan JPN) 18. Bidang 4 Para 4.1 Tanggungjawab Terhadap Aset Penambahan penyataan : **OBJEKTIF** Setiap aset ICT perlu dikenal pasti, diklasifikasi, direkodkan, diselenggara, dan dilupuskan apabila tiba masanya berdasarkan kepada tatacara/arahan/peraturan pengurusan aset yang berkuatkuasa dari semasa ke semasa. Ini adalah untuk memberikan perlindungan keselamatan yang bersesuaian kepada semua aset ICT. 19. Bidang 4 Para 4.1.1 Pendaftaran Aset	

Versi	Tarikh	Keterangan	Penulis
		Penambahan penyataan : ● b. Pegawai aset hendaklah memastikan semua aset ICT didaftarkan, dilabel dan dilekatkan di tempat yang mudah dilihat ● Tanggungjawab : tambah Pembantu Pegawai Aset 20. Bidang 4 Para 4.1.2 Penematan Aset Perubahan tajuk : Penyimpanan dan Penempatan Aset Penambahan penyataan : ● g. Aset ICT yang hendak dibawa keluar dari premis perlulah mendapat kelulusan Pegawai Aset dan direkodkan; ● h. Aset ICT hendaklah disimpan di tempat yang selamat dan sentiasa di bawah kawalan pegawai yang bertanggungjawab. Arahan Keselamatan Kerajaan hendaklah sentiasa dipatuhi bagi mengelak berlakunya kerosakan atau kehilangan Aset ICT ● i. Setiap pegawai penempatan atau pegawai yang menggunakan Aset ICT tersebut adalah bertanggungjawab terhadap apa-apa kekurangan, kerosakan atau kehilangan Aset ICT di bawah tanggungjawabnya 21. Bidang 4 Para 4.1.3 Penerimaan Penggunaan Aset Perubahan tajuk : Penerimaan dan Penggunaan Aset Tanggungjawab : Pembantu Pegawai Aset, Pegawai Penerima Aset, 22. Bidang 4 Para 4.1.4 Pemulangan Aset Tambah Tanggungjawab : Pembantu Pegawai Aset	

Versi	Tarikh	Keterangan	Penulis
		23. Bidang 4 Tambahan para 4.1.5 Pelupusan Aset 24. Bidang 4 Tambahan para 4.2.2 Penghapusan Maklumat 25. Bidang 4 Para 4.3.2 Pelupusan Media Penambahan penyataan : ● Prosedur-prosedur pelupusan media yang perlu dipatuhi adalah sebagaimana berikut: a. Media yang mengandungi maklumat terperingkat yang perlu dihapuskan atau dimusnahkan hendaklah mengikut sebagaimana prosedur yang berkuatkuasa; b. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa; dan c. Pelupusan media perlu dilaksanakan berdasarkan Garis Panduan Pengurusan Rekod Elektronik Arkib Negara. ● Tanggungjawab : Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pegawai Aset, Pembantu Pegawai Aset, Pembantu Pelupusan Aset, Pegawai IT Negeri, Kakitangan JPN. 26. Bidang 4 Para 4.3.3 Pemindahan Media Fizikal Penambahan penyataan : ● Tanggungjawab : Pengarah Bahagian/Negeri, Pengurus Projek ICT, Pentadbir Sistem, Pegawai Aset, Pembantu Pegawai Aset, Pembantu Pelupusan Aset, IT Negeri, Kakitangan JPN.	

Versi	Tarikh	Keterangan	Penulis
		27. Bidang 4 Tambahan para 4.4 Pencegahan Ketirisan Data 28. Bidang 5 Para 5.1 Kawalan Capaian Penambahan penyataan : **OBJEKTIF** Mengehadkan capaian ke atas data dan maklumat, kemudahan pemprosesan maklumat dan proses-proses utama dalam teras perkhidmatan dan perlu dikawal mengikut ketetapan yang ditentukan oleh pengurusan, pemilik data, proses, operasi atau sistem. 29. Bidang 5 Para 5.1.1 Pengurusan kawalan Capaian Penambahan penyataan : ● b. Pengasingan peranan kawalan capaian; ● f. Arkib semua aktiviti berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat pengguna 30. Bidang 5 Para 5.2.1 Pengurusan Akaun Pengguna Penambahan penyataan : c. Akaun pengguna luar yang diwujudkan hendaklah diberi tahap capaian dan tempoh masa mengikut peranan dan tanggungjawab pengguna dan dengan kelulusan pegawai pelulus; dan d. Tindakan pengemaskinian atau pembatalan akaun hendaklah diambil atas sebab-sebab berikut: ii. Pengguna yang bercuti belajar melebihi tempoh tiga (3) bulan sebagaimana yang diluluskan oleh Ketua Jabatan; ix. Pengguna bercuti melebihi satu tempoh yang diluluskan oleh Ketua Jabatan atau mana-mana pihak yang berautoriti (contoh Pegawai Perubatan); dan x. Tamat kontrak untuk pihak ketiga	

Versi	Tarikh	Keterangan	Penulis
		31. Bidang 5 Para 5.3 Tanggungjawab Pengguna Penambahan penyataan: ● e. Menandatangani borang perakuan PKS. ● Tanggungjawab : Pihak Ketiga 32. Bidang 5 Para 5.3.1 Pengurusan Katalaluan Penambahan penyataan : ● d. Kombinasi sekurang-kurangnya **DUA BELAS (12) AKSARA** dengan gabungan antara huruf, aksara khas dan nombor (alphanumeric) kecuali bagi sistem, perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad ● f. Sistem hendaklah mempunyai tempoh masa aktif yang akan tamat selepas melebihi tempoh *idle* yang ditetapkan tidak melebihi 10 minit atau tertakluk pada penetapan/kekangan sistem/aplikasi masing-masing 33. Bidang 5 Tambahan para 5.4.1 Kawalan capaian rangkaian dan perkhidmatan rangkaian 34. Bidang 6 Para 6.1. Polisi Kawalan Penggunaan Kriptografi Penambahan penyataan : ● Kriptografi adalah mekanisme penyulitan data menggunakan kaedah algoritma matematik. Transformasi penyulitan data terbahagi kepada dua iaitu kaedah penyulitan (encryption) dan penyahsulitan (decryption). Teknik ini digunapakai dalam keselamatan maklumat dan data bagi menjaga kerahsiaan dan integriti sesuatu maklumat ● Prosedur kawalan kriptografi untuk melindungi maklumat hendaklah diwujudkan dan dilaksanakan dengan mengambil kira perkara-perkara berikut: e. Jaminan pengesahan identiti / entiti melalui kaedah kriptografi	

Versi	Tarikh	Keterangan	Penulis
		f. Menyokong Dasar Kriptografi Negara (National Cryptography Policy (NCP)) yang disokong oleh Senarai Algoritma Kriptografi Terpercaya Negara (MySEAL); dan 35. Bidang 6 Para 6.1.2 Pengurusan Kunci Awam Perubahan penyataan : ● Pengurusan Prasarana Kunci Awam hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut. 36. Bidang 7 Para 7.1.1 Lingkungan Keselamatan Fizikal ● Perkara yang perlu dipatuhi termasuk yang berikut: b. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, jeriji besi, sistem kawalan pintu, kamera litar tertutup dan pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat ● Tanggungjawab : Penambahan : Pengawal Keselamatan 37. Bidang 7 Tambahan para 7.1.3 Pemantauan Keselamatan Fizikal 38. Bidang 7 Para 7.1.4 Kawalan Pejabat, Bilik dan Tempat Operasi ● Tanggungjawab : Penambahan : Pengawal Keselamatan 39. Bidang 7 Para 7.1.5 Perlindungan Terhadap Ancaman Luaran dan Persekitaran ● Tanggungjawab :	

Versi	Tarikh	Keterangan	Penulis
		Penambahan : Pengawal Keselamatan 40. Bidang 7 Para 7.2.1 Penempatan dan Perlindungan Perkakasan ICT dan Maklumat ● Tanggungjawab : Penambahan : Pegawai Aset, Pembantu Pegawai Aset 41. Bidang 7 Para 7.2.4 Penyelenggaraan Perkakasan ICT ● Tanggungjawab : Penambahan : Pembantu Pegawai Aset Pegawai IT Negeri 42. Bidang 7 Para 7.2.5 Perkakasan ICT Dibawa Keluar Premis ● Tanggungjawab : Penambahan : Pembantu Pegawai Aset, Pegawai IT Negeri, Kakitangan JPN 43. Bidang 7 Para 7.2.6 Pelupusan dan guna semula perkakasan ICT ● Tanggunagjawab : Penambahan : Pembantu Pegawai Aset, Pegawai IT Negeri, Kakitangan JPN 44. Bidang 7 Para 7.2.7 Perkakasan ICT Tanpa Pengawasan ● Tanggungjawab : Kakitangan JPN 45. Bidang 8 Para 8.1.1 Pengendalian Prosedur Operasi Penambahan penyataan :	

Versi	Tarikh	Keterangan	Penulis
		● Penyediaan dokumen perlu memastikan prosedur operasi yang didokumenkan mematuhi perkara-perkara berikut: b. Setiap prosedur hendaklah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan notifikasi ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti 46. Bidang 8 Para 8.1.2 Pengurusan Perubahan ● Perubahan dalam organisasi, proses bisnes, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal. Penyedia dokumen perlu memastikan pengurusan perubahan yang didokumenkan mematuhi perkara-perkara berikut: d. Perubahan atau pengubahsuaian hendaklah diuji, direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada sengaja atau tidak. ● Tanggungjawab : Penambahan : ICTSM, Pegawai Penyelia 47. Bidang 8 Para 8.1.3 Pengurusan Kapasiti Penambahan penyataan : ● Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: ● b. Keperluan kapasiti hendaklah mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan	

Versi	Tarikh	Keterangan	Penulis
		kerugian akibat pengubahsuaian yang tidak dirancang. 48. Bidang 8 Tambahan para 8.1.4 Pengurusan Konfigurasi 49. Bidang 8 Para 8.1.5 Pengasingan Persekitaran Pembangunan, Pengujian dan Production Perubahan tajuk : 8.1.5 Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi (production) Penambahan penyataan : ● Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko capaian yang tidak dibenarkan atau perubahan kepada persekitaran operasi. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: ● a. Perkakasan dan perisian yang digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai operasi ● b. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan pembangunan ● c. Data yang mengandungi maklumat terperingkat tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat; dan ● d. Merekodkan semua penggunaan sumber yang digunakan dalam setiap persekitaran 50. Bidang 8 Para 8.2.1 Kawalan Terhadap Perisian Berbahaya Penambahan penyataan : ● Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan perisian berbahaya seperti virus, trojan,	

Versi	Tarikh	Keterangan	Penulis
		perisian hasad dan hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan daripada perisian berbahaya adalah seperti berikut: ● a. Peralatan ICT yang dilengkapi dengan sistem pengoperasian hendaklah dilengkapi dengan perisian antivirus yang aktif dan terkini; ● g. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat ● h. Memasukkan klausa waranti di dalam kontrak yang telah ditawarkan kepada Pihak Ketiga. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; dan ● i. Mengadakan dan menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya 51. Bidang 8 Para 8.3.1 Sandaran Maklumat Perubahan tajuk : 8.3.1 Sandaran Maklumat (Backup) Penambahan penyataan : ● Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut 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 berikut hendaklah dilaksanakan bagi memastikan sistem dapat dipulihkan: ● d. Menguji sistem sandaran sedia ada dan prosedur *restore* sekurang-kurangnya sekali setahun bagi memastikan ianya dapat berfungsi	

Versi	Tarikh	Keterangan	Penulis
		dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan ● e. Salinan sandaran hendaklah disimpan di lokasi berlainan yang selamat dan lokasi perlu disahkan selamat oleh CGSO 52. Bidang 8 Para 8.4.1 Log Kronologi Penambahan penyataan : ● Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti- aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan. Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti yang berikut: (i) Fail log sistem pengoperasian; (ii) Fail log servis (contoh: web, e-mel); (iii) Fail log aplikasi (audit trail); dan (iv) Fail log rangkaian (contoh: switch, firewall, IPS). 53. Bidang 8 Para 8.4.2 Perlindungan Maklumat Log Perubahan tajuk : 8.4.2 Perlindungan Fasliti Log dan Maklumat Log Penambahan penyataan : ● Fasiliti log dan maklumat log hendaklah dilindungi daripada perkara berikut:	

Versi	Tarikh	Keterangan	Penulis
		54. Bidang 8 Tambahan para 8.4.3 Aktiviti Pemantauan 55. Bidang 8 Para 8.4.4 Log Pentadbir dan Operator Perubahan tajuk : 8.4.4 Log Pentadbir dan Pengendali Penambahan penyataan : ● Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan disemak secara berkala seperti berikut: ● b. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pengurus Projek ICT / Pentadbir Sistem hendaklah melaporkan kepada JKICT dengan segera; ● Tanggungawab : Penambahan : JKICT, Pengendali Sistem. 56. Bidang 8 Para 8.4.5 Keseragaman Waktu Penambahan penyataan : ● Waktu bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah diseragamkan mengikut sumber rujukan masa tunggal. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JPN atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh National Metrology Institute of Malaysia (NMIM)	

Versi	Tarikh	Keterangan	Penulis
		57. Bidang 8 Para 8.5.1 Pemasangan Perisian Pada Sistem Operasi ● e. Satu strategi *rollback* harus diadakan sebelum perubahan ke atas konfigurasi, sistem dan perisian dilaksanakan. 58. Bidang 8 Para 8.6.1 Pengurusan Kerentanan Teknikal Penambahan penyataan : ● Maklumat tentang 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 ke atas sistem aplikasi dan operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: 59. Bidang 8 Para 8.6.2 Kawalan Pemasangan Perisian Penambahan penyataan : ● Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: 60. Bidang 8 Tambahan para 8.8 Pengurusan Ancaman Keselamatan Siber 8.8.1 Perisikan Ancaman 61. Bidang 9 Para 9.1.1 Kawalan dan Keselamatan Rangkaian Penambahan penyataan : ● Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman	

Versi	Tarikh	Keterangan	Penulis
		● d. Peranti rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat; ● g. Log peralatan keselamatan rangkaian seperti *Firewall* dan IPS hendaklah dipantau secara berkala. Sebarang log dan trafik yang dikesan boleh memberi ancaman prestasi rangkaian atau aplikasi JPN hendaklah dimaklumkan kepada JKICT dengan segera; ● h. Pemasangan perkakasan dan perisian berkaitan rangkaian hendaklah mendapat kebenaran daripada ICTSM; ● Tanggunjawab : JPNCSIRT 62. Bidang 9 Para 9.2 Pemindahan Maklumat Perubahan tajuk : 9.2 Pemindahan/Perkongsian Data dan Maklumat 63. Bidang 9 Para 9.2.2 Perjanjian Mengenai Pemindahan Maklumat Perubahan tajuk : 9.2.2 Perjanjian Mengenai Pemindahan/Perkongsian Data dan Maklumat Penambahan penyataan : ● JPN perlu mengambil kira keselamatan data dan maklumat atau menandatangani perjanjian bertulis apabila berlaku permindahan data dan maklumat organisasi antara JPN dan pihak luar. ● Perkara-perkara yang perlu dipatuhi: a. Pewujudan punca kuasa kepada aktiviti perkongsian data dan maklumat; b. Penerimaan dan penghantaran data dan maklumat organisasi perlu dikawal; e. Mengenal pasti perlindungan data dan maklumat dalam penggunaan, pergerakan, simpanan dan menghalang ketirisan data dan maklumat.	

Versi	Tarikh	Keterangan	Penulis
		64. Bidang 9 Para 9.2.3 Pengurusan Mel Elektronik (E-mel dan Internet) Penambahan penyataan : ● Maklumat yang terlibat dalam pengurusan mel elektronik dan internet hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian pengurusan mel elektronik dan internet dan undang undang bertulis lain yang berkuat kuasa seperti berikut: a. Garis panduan mengenai Tatacara Pengunaan Internet dan Mel Elektronik di agensi-agensi kerajaan Bilangan 1 Tahun 2003; b. Arahan Setiausaha Majlis Keselamatan Negara Bilangan 1 2023 - pematuhan tatacara penggunaan emel dan internet; c. Surat arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 – langkah-langkah mengenai penggunaan mel elektronik agensi-agensi kerajaan; d. Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (MyGovUC) dan mana-mana undang-undang bertulis yang berkuatkuasa; e. Garis panduan dan prosedur mengenai tatacara penggunaan internet dan e-mel jabatan. 65. Bidang 9 Tambahan para 9.3 Saringan Web 66. Bidang 10 Para 10.1.2 Melindungi Transaksi Aplikasi Perubahan tajuk : 10.1.2 Melindungi Transaksi Perkhidmatan Aplikasi Penambahan penyataan :	

Versi	Tarikh	Keterangan	Penulis
		● 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. 67. Bidang 10 Tambahan para 10.1.3 Penyamaran Data (Data Masking) 68. Bidang 10 Para 10.2.1 Dasar Keselamatan Pembangunan Sistem. Penambahan penyataan : b. Aspek keselamatan hendaklah dimasukkan ke dalam fasa kitar hayat pembangunan system ICT; d. Memastikan *tools* dan *libraries* yang digunakan adalah yang terkini; e. Pengemaskinian *patches* adalah bersesuaian dengan perisian lain; g. Melaksanakan penyemakan ke atas input data sebelum disimpan ke dalam aplikasi bagi menjamin kesahihan dan ketepatan maklumat; h. Melaksanakan kawalan untuk mengesah dan melindungi integriti data dalam sistem aplikasi; 69. Bidang 10 Para 10.2.2 Prosedur Kawalan Perubahan Sistem Penambahan penyataan : d. Setiap perubahan mesti diuji untuk memastikan tiada impak negetif ke atas keselamatan dan perkhidmatan operasi organisasi; f. Perubahan sesuatu sistem hendaklah mendapat kelulusan Jawatankuasa yang dilantik berdasarkan jangkaan impak; g. Penilaian tahap keselamatan maklumat hendaklah dilaksanakan apabila terdapat perubahan ketara terhadap system.	

Versi	Tarikh	Keterangan	Penulis
		70. Bidang 10 Para 10.2.3 Proses Pentauliahan Penambahan penyataan : a. Fungsi pentadbir adalah melaksanakan konfigurasi awal. Pentadbir merupakan satu peranan yang diberikan kepada pengguna tertentu dalam sistem. Peranan pentadbir boleh diberi dan dilucutkan oleh pentadbir lain; 71. Bidang 10 Para 10.2.4 Proses Pelucutan Pentauliahan Penambahan penyataan : a. Proses pelucutan pentauliahan hendaklah dilaksanakan apabila sesuatu sistem tidak digunakan atau perlu ditamatkan 72. Bidang 10 Para 10.2.5 Pembangunan Sistem Secara Sumber Luar Penambahan penyataan : d. Spesifikasi perolehan hendaklah mengandungi klausa berhubung keperluan keselamatan, ketersediaan kod sumber, keperluan pelupusan data, keperluan migrasi data, keutamaan terhadap teknologi dan kepakaran tempatan, serta keperluan kompetensi pasukan pembangunan; e. Pihak ketiga hendaklah menjalani tapisan keselamatan sebelum memulakan kerja-kerja pembangunan system. 73. Bidang 10 Para 10.2.6 Pengujuan Penerimaan Sistem Penambahan penyataan : e. Penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan, bebas ralat dan memenuhi keperluan keselamatan maklumat sebelum sistem diguna pakai.	

Versi	Tarikh	Keterangan	Penulis
		74. Bidang 10 Para 10.3 Data Ujian Penambahan penyataan : a. Data dan kod pengaturcaraan yang hendak diuji perlu ditentukan, dilindungi dan dikawal; b. Hanya data yang diperlukan untuk tujuan pengujian sahaja digunakan; d. Setelah data pengujian tidak lagi diperlukan, data tersebut hendaklah dihapuskan. 75. Bidang 11 Para 11.1.1 Dasar Keselamatan Maklumat Untuk Pembekal Penambahan penyataan : h. Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber JPN kepada pembekal; i. Proses kitaran hayat (lifecycle) yang seragam untuk menguruskan pembekal; dan j. Jenis-jenis obligasi kepada pembekal. 76. Bidang 11 Para 11.1.2 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal Penambahan penyataan : ● 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: (i) JPN hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; (ii) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; (iii) Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan;	

Versi	Tarikh	Keterangan	Penulis
		(iv) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; (v) 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 (vi) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan JPN; dan (vii) Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh JPN. 77. Bidang 11 Tambahan para 11.3 Keselamatan Maklumat dan Pengurusan Penyampaian Perkhidmatan Pengkomputeran Awan (Cloud) 78. Bidang 12 Para 12.1 Pengurusan dan Penambahbaikan Insiden Keselamatan Maklumat Penambahan penyataan pada tajuk : 12.1 Pengurusan dan Penambahbaikan Insiden Keselamatan Siber Penambahan penyataan :	

Versi	Tarikh	Keterangan	Penulis
		a. Memastikan insiden keselamatan maklumat yang dilaporkan dapat diuruskan mengikut prosedur yang telah disediakan; b. Meminimumkan kesan insiden yang berlaku; c. Menambah baik kelemahan apabila berlaku insiden 79. Bidang 12 Para 12.1.1 Tangungjawab dan Prosedur Penambahan penyataan : a. Tanggungjawab dan prosedur pengurusan hendaklah dirujuk untuk memastikan maklum balas terhadap insiden keselamatan dipatuhi mengikut prosedur yang telah disediakan; dan 80. Bidang 12 Para 12.1.2 Mekanisme Pelaporan Insiden Penambahan penyataan : Prosedur pelaporan insiden keselamatan ICT berdasarkan: a. Surat Pekeliling Am Bilangan 4 Tahun 2022- Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam; dan 81. Bidang 12 Para 12.1.3 Melaporkan Kelemahan Keselamatan ICT Perubahan tajuk : 12.1.3 Melaporkan Kelemahan Keselamatan Siber 82. Bidang 12 Para 12.1.4 Penilaian dan Keputusan Mengenai Aktiviti Keselamatan Maklumat Perubahan tajuk : 12.1.4 Penilaian dan Keputusan Mengenai Aktiviti Keselamatan Siber Penambahan penyataan : ● Penetapan insiden adalah berdasarkan keutamaan berikut : a. Keutamaan 1 - Insiden keselamatan siber yang memberi impak tinggi terhadap pertahanan dan keselamatan negara,	

Versi	Tarikh	Keterangan	Penulis
		kestabilan ekonomi negara, imej negara, keupayaan kerajaan untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu. b. Keutamaan 2 - Insiden keselamatan siber yang tidak memberi impak seperti mana yang dinyatakan dalam Keutamaan 1 ● Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk. ICTSO melaporkan kepada KDNCSIRT / NACSA apabila berlaku insiden keselamatan siber sekiranya perlu. 83. Bidang 12 Perubahan tajuk : Para 12.1.5 Tindak Balas Insiden Keselamatan Siber 84. Bidang 12 Perubahan tajuk : Para 12.1.6 Pengalaman Dari Insiden Keselamatan Siber 85. Bidang 13 Para 13.1 Keselamatan Maklumat Bagi Kesinambungan Perkhidmatan Penambahan penyataan : JPN hendaklah menentukan keperluan untuk memastikan keselamatan maklumat terpelihara dalam situasi kecemasan dengan mengambil kira faktor dalaman dan luaran yang boleh memberikan impak kepada kesinambungan sistem penyampaian perkhidmatan dan fungsi Jabatan. Perubahan tanggunjawab : Bahagian Pentadbiran BP	

Versi	Tarikh	Keterangan	Penulis
		86. Bidang 13 Para 13.1.1 Pengurusan Kesinambungan Perkhidmatan Penambahan penyataan : Mengurus dan memastikan keperluan pihak berkepentingan dilindungi dan imej JPN terpelihara dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan JPN di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP); dan b. Melaksana Kajian Impak Perkhidmatan (*Business Impact Analysis, BIA) dan Penilaian Risiko terhdap perkhidmatan kritikal.* Perubahan tanggunjawab : Bahagian Pentadbiran BP 87. Bidang 13 Tambahan para 13.1.3 Ketersediaan ICT Untuk Kesinambungan Operasi. 88. Bidang 14 Para 14.1.3 Privasi dan Perlindungan Maklumat Peribadi Perubahan penyataan : Semua kakitangan JPN dan Pihak Ketiga hendaklah memberi jaminan dalam melindungi maklumat peribadi individu seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia 89. Kemaskini borang Perakuan PKS (LAmpiran 1) : Tambah Gred Adalah dengan sesungguhnya dan sebenarnya saya mengaku bahawa:- 1. Telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber JPN;	

Versi	Tarikh	Keterangan	Penulis
		2. Berjanji akan menghayati Polisi Keselamatan Siber JPN sepenuhnya pada setiap masa demi menjaga nama baik Jabatan dan Negara; 3. Akur akan sebarang pindaan Polisi Keselamatan Siber JPN; dan 4. Jika saya ingkar kepada peraturan-peraturan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya. 90. Lampiran 2 Tambahan : 55. Surat Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam	