JABATAN PERDANA MENTERI
JABATAN WILAYAH PERSEKUTUAN

# POLISI
# KAWALAN KESELAMATAN MAKLUMAT JABATAN WILAYAH PERSEKUTUAN (PKKM JWP)
# VERSI 2025

# KANDUNGAN

KANDUNGAN I
AKRONIM/TERMA/TAKRIFAN V
SEJARAH DOKUMEN POLISI KAWALAN KESELAMATAN MAKLUMAT XIII

**1.0 PENDAHULUAN 1**

1.1 PENGENALAN 1
1.2 TUJUAN 1
1.3 OBJEKTIF 1
1.4 SKOP 2

**2.0 POLISI DAN OBJEKTIF KESELAMATAN MAKLUMAT 5**

2.1 PERNYATAAN POLISI 5
2.2 PRINSIP KESELAMATAN MAKLUMAT 6

**3.0 PENGURUSAN RISIKO KESELAMATAN MAKLUMAT 8**

**4.0 TADBIR URUS 10**

4.1 STRUKTUR TADBIR URUS SISTEM PENGURUSAN KESELAMATAN MAKLUMAT JWP 10
4.2 KEAHLIAN JPICT JWP ADALAH SEPERTI YANG BERIKUT: 10

**5.0 KAWALAN ORGANISASI (ORGANIZATIONAL CONTROL) 12**

5.1 POLISI KESELAMATAN MAKLUMAT (INFORMATION SECURITY POLICY) 12
5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT (INFORMATION SECURITY ROLES AND RESPONSIBILITIES) 14
5.3 PENGASINGAN TUGAS (SEGREGATION OF DUTIES) 23
5.4 TANGGUNGJAWAB PENGURUSAN (MANAGEMENT RESPONSIBILITIES) 24
5.5 HUBUNGAN DENGAN PIHAK BERKUASA (CONTACT WITH AUTHORITIES) 24
5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS (CONTACT WITH SPECIAL INTEREST GROUPS) 27
5.7 PERISIKAN ANCAMAN (THREAT INTELLIGENCE) 29
5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK (INFORMATION SECURITY IN PROJECT MANAGEMENT) 30
5.9 INVENTORI MAKLUMAT DAN ASET LAIN YANG BERKAITAN (INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS) 32
5.10 PENGGUNAAN MAKLUMAT YANG BOLEH DITERIMA DAN ASET LAIN YANG BERKAITAN (ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS) 35
5.11 PEMULANGAN ASET (RETURN OF ASSETS) 36
5.12 PENGELASAN MAKLUMAT (CLASSIFICATION OF INFORMATION) 37
5.13 PELABELAN MAKLUMAT (LABELLING OF INFORMATION) 39
5.14 PEMINDAHAN DATA DAN MAKLUMAT (INFORMATION TRANSFER) 40
5.15 KAWALAN CAPAIAN (ACCESS CONTROL) 42
5.16 PENGURUSAN IDENTITI (IDENTITY MANAGEMENT) 46
5.17 MAKLUMAT PENGESAHAN (AUTHENTICATION INFORMATION) 49
5.18 HAK CAPAIAN (ACCESS RIGHTS) 53
5.19 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PEMBEKAL (INFORMATION SECURITY POLICY FOR SUPPLIER RELATIONSHIPS) 56
5.20 MENANGANI KESELAMATAN DALAM PERJANJIAN (ADDRESSING SECURITY WITHIN SUPPLIER AGREEMENTS) 57

5.21 MENGURUSKAN KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (MANAGING INFORMATION SECURITY IN THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN) 59
5.22 PEMANTAUAN, SEMAKAN DAN PENGURUSAN PERUBAHAN PERKHIDMATAN PEMBEKAL (MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES) 60
5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN PENGKOMPUTERAN AWAN (INFORMATION SECURITY FOR USE OF CLOUD COMPUTING SERVICES) 62
5.24 PERANCANGAN DAN PERSEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT (INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION) 62
5.25 PENILAIAN DAN KEPUTUSAN MENGENAI INSIDEN KESELAMATAN MAKLUMAT (ASSESSMENT OF AND DECISION ON INFORMATION SECURITY EVENTS) 64
5.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT (RESPONSE TO INFORMATION SECURITY INCIDENTS) 64
5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT (LEARNING FROM INFORMATION SECURITY INCIDENTS) 65
5.28 PENGUMPULAN BAHAN BUKTI (COLLECTION OF EVIDENCE) 66
5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN (INFORMATION SECURITY DURING DISRUPTION) 67
5.30 KESEDIAAN ICT BAGI KESINAMBUNGAN PERKHIDMATAN (ICT READINESS FOR BUSINESS CONTINUITY) 69
5.31 KEPERLUAN PERUNDANGAN DAN KONTRAK (LEGAL, STATUTORY, REGULATORY AND CONTRACTUAL REQUIREMENTS) 73
5.32 HAK HARTA INTELEK (INTELLECTUAL PROPERTY RIGHTS) 74
5.33 PERLINDUNGAN REKOD (PROTECTION OF RECORDS) 74
5.34 PRIVASI DAN PERLINDUNGAN PERIBADI YANG BOLEH DIKENAL PASTI (PRIVACY AND PROTECTION OF PERSONAL IDENTIFIABLE INFORMATION (PII)) 75
5.35 KAJIAN SEMULA KESELAMATAN MAKLUMAT SECARA BERKECUALI (INDEPENDENT REVIEW OF INFORMATION SECURITY) 75
5.36 PEMATUHAN POLISI, PERATURAN DAN PIAWAIAN UNTUK KESELAMATAN MAKLUMAT (COMPLIANCE WITH POLICIES, RULES AND STANDARDS FOR INFORMATION SECURITY) 76
5.37 DOKUMENTASI PROSEDUR OPERASI YANG DIDOKUMENKAN (DOCUMENTED OPERATING PROCEDURES) 77

**6.0 KAWALAN SUMBER MANUSIA (PEOPLE CONTROL) 79**

6.1 TAPISAN KESELAMATAN (SECURITY SCREENING) 79
6.2 TERMA DAN SYARAT PERKHIDMATAN (TERMS AND CONDITIONS OF EMPLOYMENT) 79
6.3 KESEDARAN, PENDIDIKAN DAN LATIHAN TENTANG KESELAMATAN MAKLUMAT (INFORMATION SECURITY AWARENESS, EDUCATION AND TRAINING) 80
6.4 PROSES TATATERTIB (DISCIPLINARY PROCESS) 81
6.5 TANGGUNGJAWAB SELEPAS PENAMATAN ATAU PERTUKARAN PEKERJAAN (RESPONSIBILITIES AFTER TERMINATION OR CHANGE OF EMPLOYMENT) 82
6.6 PERJANJIAN KERAHSIAAN ATAU KETAKDEDAHAN (CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS) 83
6.7 BEKERJA JARAK JAUH (REMOTE WORKING) 84
6.8 PELAPORAN KESELAMATAN MAKLUMAT (REPORTING INFORMATION SECURITY EVENTS) 85

**7.0 KAWALAN FIZIKAL (PHYSICAL CONTROL) 87**

7.1 PERIMETER KESELAMATAN FIZIKAL (PHYSICAL SECURITY PERIMETER) 87
7.2 KEMASUKAN FIZIKAL (PHYSICAL ENTRY) 88
7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN (SECURING OFFICES, ROOMS AND FACILITIES) 89
7.4 PEMANTAUAN KESELAMATAN FIZIKAL (PHYSICAL SECURITY MONITORING) 90

7.5 PERLINDUNGAN DARIPADA ANCAMAN FIZIKAL DAN PERSEKITARAN (PROTECTING AGAINST PHYSICAL AND ENVIRONMENTAL THREATS) 91
7.6 BEKERJA DI KAWASAN SELAMAT (WORKING IN SECURE AREAS) 91
7.7 MEJA KOSONG DAN SKRIN KOSONG (CLEAR DESK AND CLEAR SCREEN) 93
7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN ICT (EQUIPMENT SITING AND PROTECTION) 94
7.9 KESELAMATAN ASET DI LUAR PREMIS (SECURITY OF ASSETS OFF-PREMISES) 97
7.10 MEDIA STORAN (STORAGE MEDIA) 97
7.11 UTILITI SOKONGAN (SUPPORTING UTILITIES) 99
7.12 KESELAMATAN KABEL (CABLING SECURITY) 99
7.13 PENYELENGGARAAN PERALATAN (EQUIPMENT MAINTENANCE) 100
7.14 PELUPUSAN YANG SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN (SECURE DISPOSAL OR RE-USE OF EQUIPMENT) 101

**8.0 KAWALAN TEKNOLOGI (TECHNOLOGICAL CONTROL) 105**

8.1 PERANTI TITIK HUJUNG PENGGUNA (USER ENDPOINT DEVICES) 105
8.2 HAK AKSES ISTIMEWA (PRIVILEGED ACCESS RIGHTS) 108
8.3 SEKATAN AKSES MAKLUMAT (INFORMATION ACCESS RESTRICTION) 108
8.4 KAWALAN AKSES KEPADA KOD SUMBER PROGRAM (ACCESS TO SOURCE CODE) 109
8.5 PENGESAHAN SELAMAT (SECURE AUTHENTICATION) 110
8.6 PENGURUSAN KAPASITI (CAPACITY MANAGEMENT) 112
8.7 PERLINDUNGAN DARIPADA PERISIAN HASAD (PROTECTION AGAINST MALWARE) 113
8.8 PENGURUSAN KERENTANAN TEKNIKAL (MANAGEMENT OF TECHNICAL VULNERABILITIES) 115
8.9 PENGURUSAN KONFIGURASI (CONFIGURATION MANAGEMENT) 116
8.10 PENGHAPUSAN PELUPUSAN/SANITASI MAKLUMAT (INFORMATION DELETION) 117
8.11 PENYAMARAN DATA (DATA MASKING) 118
8.12 PENCEGAHAN KETIRISAN DATA (DATA LEAKAGE PREVENTION) 118
8.13 SANDARAN MAKLUMAT (INFORMATION BACKUP) 120
8.14 LEWAHAN BAGI KEMUDAHAN PEMPROSESAN MAKLUMAT (REDUNDANCY OF INFORMATION PROCESSING FACILITIES) 121
8.15 MENYEDIAKAN LOG (LOGGING) 122
8.16 AKTIVITI PEMANTAUAN (MONITORING ACTIVITIES) 124
8.17 PENYERAGAMAN WAKTU (CLOCK SYNCHRONIZATION) 125
8.18 PENGGUNAAN PROGRAM UTILITI YANG MEMPUNYAI HAK ISTIMEWA (USE OF PRIVILEGED UTILITY PROGRAMS) 126
8.19 PEMASANGAN PERISIAN PADA SISTEM YANG BEROPERASI (INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS) 127
8.20 KESELAMATAN RANGKAIAN (NETWORKS SECURITY) 128
8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN (SECURITY OF NETWORK SERVICES) 131
8.22 PENGASINGAN DALAM RANGKAIAN (SEGREGATION OF NETWORKS) 133
8.23 PENYARINGAN WEB (WEB FILTERING) 133
8.24 PENGGUNAAN KRIPTOGRAFI (USE OF CRYPTOGRAPHY) 134
8.25 KITAR HAYAT PEMBANGUNAN SISTEM YANG SELAMAT (SECURE DEVELOPMENT LIFE CYCLE) 135
8.26 KEPERLUAN KESELAMATAN APLIKASI (APPLICATION SECURITY REQUIREMENTS) 137
8.27 PRINSIP REKA BENTUK DAN KEJURUTERAAN SISTEM YANG SELAMAT (SECURE SYSTEM ARCHITECTURE AND ENGINEERING PRINCIPLES) 139
8.28 PENGEKODAN SELAMAT (SECURE CODING) 140
8.29 PENGUJIAN DAN PENERIMAAN KESELAMATAN SISTEM (SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE) 142
8.30 PEMBANGUNAN OLEH PEMBEKAL (OUTSOURCED DEVELOPMENT) 144

8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN, PENGUJIAN DAN PENGELUARAN (SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENTS) 145
8.32 PENGURUSAN PERUBAHAN (CHANGE MANAGEMENT) 147
8.33 MAKLUMAT PENGUJIAN (TEST INFORMATION) 150
8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PENGUJIAN AUDIT (PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING) 151

**LAMPIRAN 153**

## AKRONIM/TERMA/TAKRIFAN

| SINGKATAN dan GLOSARI | KETERANGAN |
|---|---|
| Antivirus | Perisian yang mengimbas virus pada infrastruktur teknologi serta media storan seperti *thumdrive* dan *external hard disk* untuk sebarang kemungkinan adanya virus. |
| API (Application Programming Interface) | Satu set arahan pengaturcaraan dan standard untuk akses menerusi aplikasi web menggunakan perisian aplikasi web. |
| Aset ICT | Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. |
| Sandaran (Backup) | Proses penduaan sesuatu dokumen atau maklumat. Sumber yang boleh digunakan untuk menggantikan sumber utama yang gagal atau terhapus. |
| *Bandwidth* | Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi dalam jangka masa yang ditetapkan. Contoh: video streaming dan teleconference. |
| BDPM | Bahagian Digital dan Pengurusan Maklumat JWP. |
| BYOD (Bring Your Own Device) | Peralatan mudah alih persendirian seperti telefon pintar, tablet, komputer riba dan media storan yang digunakan untuk tujuan rasmi. |
| CSIRT (Computer Security Incident Response Team) | Pasukan Tindak Balas Insiden Keselamatan Siber, iaitu pasukan yang ditubuhkan untuk membantu JWP menguruskan pengendalian insiden keselamatan siber di JWP. |
| CDO (Chief Digital Officer) | Ketua Pegawai Digital, iaitu pegawai yang dilantik untuk menjadi peneraju dalam merancang, melaksana dan memantau program Kerajaan berasaskan ICT dan digital bagi memudahkan |

| SINGKATAN dan GLOSARI | KETERANGAN |
|---|---|
| | pelanggan berurusan dengan JWP. Beliau juga merupakan agen transformasi menerusi inovasi, kreativiti dan inisiatif pembaharuan yang berterusan. |
| CGSO (Chief Government Security Office) | Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia, iaitu sebuah unit di bawah Jabatan Perdana Menteri, Malaysia. |
| *Clear Desk dan Clear Screen* | Tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. |
| *Content Filtering* | Satu teknik yang menyekat atau membenarkan berdasarkan analisis kepada kandungan dan bukannya berdasarkan sumber atau kriteria. Ia digunakan secara meluas untuk capaian Internet dan e-mel. |
| PKKM | Polisi Kawalan Keselamatan Maklumat, iaitu dokumen yang mengandungi dasar dan peraturan dalam menggunakan aset ICT dan ruang siber. |
| DRP (Disaster Recovery Plan) | Pelan Pemulihan Bencana, iaitu dokumentasi pendekatan berstruktur yang menerangkan bagaimana sesebuah organisasi dengan cepatnya memulakan semula kerja setelah berlakunya bencana. DRP merupakan bahagian penting dalam Pelan Pengurusan Kesinambungan Perkhidmatan yang melibatkan aspek-aspek tertentu organisasi yang bergantung kepada infrastruktur ICT. |
| E-mel (Mel Elektronik) | Maklumat atau mesej yang dihantar secara elektronik dari satu terminal komputer ke terminal komputer yang lain. |

| SINGKATAN dan GLOSARI | KETERANGAN |
|---|---|
| Enkripsi (Encryption) | Penukaran data sensitif kepada bentuk kod sulit untuk membolehkan data dikirim dengan selamat tanpa difahami pihak lain. |
| ICT (Information and Communication Technology) | Penggabungan teknologi maklumat dan teknologi komunikasi dalam perolehan, penyimpanan, pemprosesan dan pengagihan maklumat secara elektronik. |
| ICTSO (ICT Security Officer) | Pegawai Keselamatan ICT, iaitu pegawai yang dilantik untuk bertanggungjawab terhadap keselamatan siber. |
| IDS (Intrusion Detection System) | Sistem yang menyiasat semua aktiviti rangkaian dan mengenal pasti pola yang disyaki untuk menunjukkan bahawa rangkaian atau sistem diceroboh. Terdapat dua bentuk IDS yang lazim, iaitu pengesanan salah guna dan pengesanan anomali. Dalam pengesanan salah guna, IDS menganalisis maklumat yang dikumpul dan membandingkannya dengan pangkalan data tandatangan serangan yang besar. Secara khusus IDS mencari serangan tertentu yang telah didokumenkan. Seperti sistem pengesan virus, keberkesanan perisian pengesan salah guna ini hanyalah bergantung kepada sebaik mana pangkalan data tandatangan serangan yang ada untuk membandingkan maklumat yang dikumpul. |
| Insiden Keselamatan Siber | Musibah (adverse event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin satu perbuatan yang melanggar PKKM sama ada yang ditetapkan secara tersurat atau tersirat. |
| Internet | Sistem perangkaian antarabangsa yang membolehkan pengguna di seluruh dunia berhubung antara satu sama lain dan mencapai maklumat di seluruh dunia. |

| SINGKATAN dan GLOSARI | KETERANGAN |
|---|---|
| IPS (Intrusion Prevention System) | Perkakasan keselamatan komputer yang memantau rangkaian dan/ atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan seperti *malicious code*. Contoh: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan. |
| ISMS (Information Security Management System) | Sistem Pengurusan Keselamatan Maklumat. ISO/IEC 27001 (ISMS) menyatakan keperluan untuk mewujud, mengoperasi, memantau, mengkaji semula, menyenggara dan memperbaiki Sistem Pengurusan Keselamatan Maklumat organisasi. Pematuhan kepada standard/ piawaian ISMS ini menunjukkan bahawa sistem pengurusan organisasi perlu memastikan kerahsiaan, integriti dan ketersediaan maklumat. |
| JKISMS | Merujuk kepada Jawatankuasa ISMS (JWP). |
| JPICT | Merujuk kepada Jawatankuasa Pemandu ICT. |
| Jejak Audit (Audit Trail) | Log yang merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. |
| JPM | Jabatan Perdana Menteri, iaitu sebuah kementerian kerajaan persekutuan Malaysia yang diketuai oleh Perdana Menteri Malaysia. |
| Kawasan Larangan | Kawasan yang dihadkan kemasukannya kepada pegawai-pegawai yang tertentu sahaja. |
| Kerentanan | Kelemahan atau kecacatan sistem yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan. |

| SINGKATAN dan GLOSARI | KETERANGAN |
|---|---|
| Kriptografi | Penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak tertentu sahaja. |
| LAN (Local Area Network) | Rangkaian komputer yang berkongsi data dan sumber dalam sesuatu kawasan yang terhad seperti sebuah bangunan dan sebuah pejabat. |
| JWP | Jabatan Wilayah Persekutuan (JWP), Jabatan Perdana Menteri (JPM). |
| Media Storan | Peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti *external hard drive*, *flash disk*, *thumb drive* dan media storan lain. |
| NACSA (National Cyber Security Agency) | Agensi Keselamatan Siber Negara. Ditubuhkan pada Februari 2017 sebagai agensi negara yang menerajui hal ehwal keselamatan siber, dengan objektif memastikan keselamatan dan memperkukuhkan ketahanan Malaysia dalam menghadapi ancaman serangan siber, dengan mengkoordinasi dan mengkonsolidasi pakar-pakar dan sumber negara dalam bidang keselamatan siber. |
| *Outsource* | Menggunakan perkhidmatan luar atau pihak ketiga untuk melaksanakan fungsi tertentu bagi suatu tempoh berdasarkan dokumen perjanjian dengan bayaran yang telah dipersetujui. |
| Pembekal | Individu, entiti perniagaan atau organisasi yang menyediakan produk atau perkhidmatan kepada Pengguna. |
| Pemilik Sistem | Pemilik bisnes (business owner) bagi sistem yang dibangunkan atau Bahagian/ Unit di bawah JWP yang paling banyak memiliki data dalam sesuatu sistem. |

| SINGKATAN dan GLOSARI | KETERANGAN |
|---|---|
| Pemegang Taruh | Semua pihak yang mempunyai kepentingan dengan Jabatan. |
| Pengguna | Warga Bahagian/Unit di bawah JWP termasuk pegawai yang berkhidmat secara kontrak atau pegawai khidmat singkat yang menggunakan aset ICT dan siber secara langsung atau tidak langsung. |
| Pentadbir Sistem ICT | Pentadbir yang membangunkan, melaksanakan dan menyelenggara sistem aplikasi, laman web, media sosial dan aplikasi mudah alih. |
| Peralatan ICT | Merujuk kepada perkakasan dan perisian ICT. |
| Peralatan Mudah Alih | Peralatan mudah alih termasuk komputer riba dan peranti mudah alih seperti tablet, Personal Digital Assistant (PDA), telefon bimbit, telefon pintar, kamera digital, cakera padat serta pemacu Universal Serial Bus (USB) dan sebagainya. |
| Perisian | Set atur cara komputer yang menjalankan sesuatu tugas pada sistem komputer. Terdapat tiga (3) jenis perisian iaitu sistem pengendali (contoh: Linux dan Windows), sistem utiliti (contoh: Disk Cleanup dan Disk Defragmenter) dan perisian aplikasi (contoh: Microsoft Office dan Google Chrome). |
| Perkakasan ICT | Merujuk kepada komponen dalaman peralatan ICT. |
| Pihak Ketiga | Pakar runding, pihak dan individu yang mempunyai urusan dengan perkhidmatan ICT dan siber serta dilantik untuk melaksanakan tugas di JWP dalam jangka masa yang tertentu. |
| PII (Personal Identifiable Information) | Maklumat yang boleh digunakan secara tersendiri atau digunakan dengan maklumat lain untuk mengenal pasti individu tertentu. |

| SINGKATAN dan GLOSARI | KETERANGAN |
|---|---|
| PKI (Public Key Infrastructure) | Infrastruktur Kunci Awam, iaitu sistem enkripsi lengkap khusus untuk mencipta dan mengurus kekunci awam semasa proses penyulitan data dan pertukaran kekunci dalam kalangan pengguna. Ia merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet. |
| PKP | Pengurusan Kesinambungan Perkhidmatan (Business Continuity Management), bertujuan untuk memastikan fungsi-fungsi kritikal, perkhidmatan, sistem dan proses-proses utama agensi dapat segera dipulihkan dalam masa yang ditetapkan sekiranya berlaku gangguan atau bencana. |
| *RC* | *Recover* |
| *Restore* | Aktiviti pemulihan atau penyalinan semula data daripada media penduaan. |
| RP | *Respond* |
| *Router* | Peranti yang digunakan untuk menghantar data antara dua (2) rangkaian yang mempunyai kedudukan rangkaian yang berlainan. contoh: capaian Internet. |
| *Server* | Unit dalam rangkaian yang membekalkan data dan maklumat kepada komputer lain yang mempunyai hubungan rangkaian dengannya. |
| Siber | Ruang maya yang diwujudkan oleh rangkaian komputer sejagat. Ruang tempat berlangsungnya kegiatan pemanfaatan ICT dan Internet ini disebut ruang siber. Ruang siber (cyberspace) atau siber adalah ruang di mana komunikasi saling terhubung menggunakan jaringan (misalnya Internet) untuk melakukan berbagai kegiatan sehari-hari. |

| SINGKATAN dan GLOSARI | KETERANGAN |
|---|---|
| Sistem ICT | Merangkumi Sistem Aplikasi, Sistem Pusat Data, Rangkaian dan Komunikasi ICT. |
| SLA (Service Level Assurance) | Perjanjian Tahap Perkhidmatan, iaitu komponen kontrak perkhidmatan antara pembekal perkhidmatan dan pelanggan. SLA menyediakan aspek khusus dan terukur yang berkaitan dengan penawaran perkhidmatan. |
| *Switch* | Alat yang boleh menapis (filter) dan memajukan (forward) isyarat paket data antara segmen rangkaian LAN. |
| UC (Unified Communication) | Saluran-saluran komunikasi elektronik selain e-mel yang disepadukan dalam satu rangkaian dan antara muka yang sama. |
| UPS (Uninterruptible Power Supply) | Satu alat yang akan membekalkan kuasa secara automatik kepada peralatan komputer khususnya dan peralatan elektrik umumnya apabila bekalan elektrik utama terputus. |
| WAN (Wide Area Network) | Rangkaian komunikasi yang merangkumi kawasan geografi yang luas di seluruh bandar, negara atau rantau. |

## SEJARAH DOKUMEN POLISI KAWALAN KESELAMATAN MAKLUMAT

| TARIKH | VERSI | PEKELILING | TARIKH KUATKUASA |
|---|---|---|---|
| 26 April 2022 | 1.0 | PKS | 26 April 2022 |
| 11 April 2023 | 2023 | PKS | 11 April 2023 |
| 18 April 2024 | 2024 | PKKM | 18 April 2024 |
| 12 Ogos 2025 | 2025 | PKKM | 12 Ogos 2025 |

# 1.0 PENDAHULUAN

## 1.1 Pengenalan

Polisi Kawalan Keselamatan Maklumat (PKKM), Jabatan Wilayah Persekutuan (JWP) mengandungi amalan, prosedur, garis panduan, peraturan dan kawalan bertulis keselamatan maklumat, keselamatan siber dan perlindungan privasi merupakan pendekatan proaktif terhadap perlindungan keselamatan maklumat, meminimumkan risiko pelanggaran kerahsiaan data, akses tanpa kebenaran, dan potensi kerugian kewangan dan reputasi JWP.

## 1.2 Tujuan

Polisi Kawalan Keselamatan Maklumat, Jabatan Wilayah Persekutuan disediakan berpandu kepada piawaian antarabangsa iaitu ISO/IEC 27002:2022 dan bertujuan untuk menerangkan peranan, tanggungjawab, arahan, peraturan-peraturan, garis panduan, dan amalan yang MESTI DIBACA, DIFAHAMI dan DIPATUHI oleh warga Jabatan Wilayah Persekutuan pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan Wilayah Persekutuan dalam melindungi maklumat di ruang siber.

## 1.3 Objektif

Polisi Kawalan Keselamatan Maklumat diwujudkan bagi memastikan keselamatan dan kesinambungan penyampaian Perkhidmatan Jabatan Wilayah Persekutuan terjamin sekaligus meningkatkan tahap keyakinan kepada pihak berkepentingan iaitu jabatan Kerajaan, industri dan orang awam. Objektif utama Polisi Kawalan Keselamatan Maklumat ini adalah untuk:

a) Memastikan keselamatan penyampaian perkhidmatan Jabatan Wilayah Persekutuan ditahap tertinggi dan meningkatkan tahap keyakinan pihak berkepentingan seperti jabatan Kerajaan, industri dan orang awam;

b) Memastikan kelancaran operasi serta menjamin kesinambungan perkhidmatan Jabatan Wilayah Persekutuan dengan meminimumkan kesan insiden keselamatan maklumat, fizikal dan logikal;

c) Memudahkan perkongsian maklumat yang selamat;

d) Mencegah salah guna atau kecurian maklumat Kerajaan;

e) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

f) Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

## 1.4 Skop

Polisi dalam dokumen ini adalah terpakai bagi semua Aset Maklumat Jabatan Wilayah Persekutuan. Aset maklumat Jabatan Wilayah Persekutuan terdiri daripada data dan maklumat sama ada dalam bentuk salinan digital (softcopy) atau salinan bercetak (hardcopy), perkakasan (hardware), perisian (software), infrastruktur ICT, manusia (people) dan premis. Aset-aset ini amat berharga dan penting untuk membolehkan Jabatan Wilayah Persekutuan menjalankan urusan rasmi Kerajaan dengan lancar kepada masyarakat, pihak swasta dan juga jabatan kerajaan yang berkaitan. Dengan itu, Polisi Kawalan Keselamatan Maklumat Jabatan Wilayah Persekutuan menetapkan keperluan-keperluan asas seperti berikut:

i) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

ii) semua data dan maklumat hendaklah dijaga kerahasiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Polisi Kawalan Keselamatan Maklumat Jabatan Wilayah Persekutuan ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur pengendalian semua perkara berikut:

**a) Data atau Maklumat**

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif bahagian.

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

**b) Salinan Digital (Softcopy)**

Koleksi fakta-fakta dalam digital atau elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif Jabatan Wilayah Persekutuan (Contohnya: Rekod-rekod digital, profil pelanggan, pangkalan data dan fail-fail data, maklumat arkib dan lain-lain);

**c) Salinan Bercetak (Hardcopy)**

Koleksi fakta-fakta dalam bentuk kertas atau bercetak, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif Jabatan Wilayah Persekutuan (Contohnya: Sistem dokumentasi, prosedur operasi, rekod-rekod, profil pelanggan, fail-fail dan lain-lain);

**d) Perkakasan (Hardware)**

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan Jabatan Wilayah Persekutuan Contohnya; komputer, pelayan, peralatan komunikasi dan sebagainya;

**e) Perisian (software)**

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 Jabatan Wilayah Persekutuan.

**f) Infrastruktur ICT**

Merujuk kepada set lengkap perkakasan, perisian, rangkaian, dan kemudahan yang membolehkan penghantaran, penyimpanan, pemprosesan dan mendapatkan semula maklumat dalam organisasi atau merentasi pelbagai organisasi. Ia termasuk sistem komputer, pelayan, pangkalan data, rangkaian (kedua-dua kawasan tempatan dan luas), sambungan Internet, sistem komunikasi, pusat data, perkhidmatan pengkomputeran awan (cloud computing) dan peralatan dan teknologi lain yang diperlukan. Infrastruktur ICT yang direka bentuk dan dilaksanakan untuk menyokong dan membolehkan pelbagai jenis perkhidmatan dan aplikasi teknologi maklumat dan

komunikasi dalam Jabatan Wilayah Persekutuan berfungsi bagi mencapai objektif dan misi yang ditetapkan. Infrastruktur ICT ini termasuk:

i) Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii) Sistem halangan akses seperti sistem kad akses;
iii) Perkhidmatan pengkomputeran awam (SaaS/PaaS/IaaS): dan
iv) Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

**g) Manusia**

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

**h) Premis**

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) - (g) di atas.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah keselamatan.

# 2.0 POLISI DAN OBJEKTIF KESELAMATAN MAKLUMAT

## 2.1 PERNYATAAN POLISI

**Aset maklumat** adalah aset kritikal yang bernilai kepada Jabatan Wilayah Persekutuan dan oleh itu hendaklah dilindungi dengan sewajarnya. Keselamatan aset maklumat ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan aset maklumat adalah suatu proses yang berterusan dan melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan siber sentiasa berubah.

Perlindungan aset maklumat ini merangkumi perlindungan semua bentuk maklumat dan data elektronik yang diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan aset maklumat dalam ruang siber untuk memastikan kerahasiaan, integriti, tidak boleh disangkal, kesahihan dan ketersediaan capaian aset maklumat kepada semua pengguna yang dibenarkan. Penjelasan ciri-ciri utama keselamatan aset maklumat yang perlu dijaga adalah seperti berikut:

a) **Kerahsiaan -** Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
b) **Integriti -** Data dan maklumat hendaklah tepat, lengkap dan kemas kini dan hanya boleh diubah dengan cara yang dibenarkan;
c) **Tidak Boleh Disangkal -** Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal;
d) **Kesahihan -** Data dan maklumat hendaklah dipastikan kesahihannya; dan
e) **Ketersediaan -** Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain itu, langkah-langkah ke arah memelihara keselamatan aset maklumat hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT Jabatan Wilayah Persekutuan ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah-langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan. Penetapan kawalan keselamatan maklumat yang sesuai hendaklah berdasarkan klasifikasi data dan maklumat atau nilai/kepentingan aset maklumat. Klasifikasi data dan maklumat ini boleh merujuk kepada arah/pekeliling/garis panduan kerajaan yang dikuatkuasakan.

Keselamatan aset maklumat adalah tanggungjawab semua warga Jabatan Wilayah Persekutuan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan digital Jabatan Wilayah Persekutuan dalam melindungi aset maklumat di ruang siber.

## 2.2 PRINSIP KESELAMATAN MAKLUMAT

Prinsip-prinsip yang menjadi asas kepada Polisi Kawalan Keselamatan Maklumat Jabatan Wilayah Persekutuan dan perlu dipatuhi adalah seperti berikut:

### a) Akses Atas Dasar Perlu Mengetahui

Akses terhadap penggunaan aset maklumat 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. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan Kerajaan yang sedang berkuatkuasa.

### b) Hak Akses Minimum

Pengguna hendaklah diberikan hak akses minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak askes atau capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

### c) Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset maklumat Jabatan Wilayah Persekutuan. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber/ aset maklumat. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka. Akauntabiliti atau tanggungjawab pengguna termasuklah:

i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii) Memeriksa maklumat dan menentukan ianya 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, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

**d) Pengasingan Tugas**

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

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

**e) Prinsip Amanah Sifar (zero trust)**

Konsep keselamatan yang bertujuan untuk meningkatkan postur keselamatan keseluruhan Jabatan Wilayah Persekutuan dengan menggunakan yang menganggap bahawa setiap peranti dan pengguna, di dalam dan di luar perimeter rangkaian, berpotensi terjejas. Oleh itu, tiada pengguna atau peranti dipercayai secara automatik dan setiap permintaan untuk capaian rangkaian hendaklah disahkan seolah-olah ia berasal dari rangkaian terbuka. Di bawah prinsip ini,

i) semua trafik rangkaian (dalaman dan luaran) dianggap sebagai tidak dipercayai;
ii) akses kepada sumber diberikan berdasarkan set kriteria yang komprehensif, termasuk identiti pengguna, kesihatan peranti, lokasi dan faktor kontekstual yang lain yang bersesuaian. Akses kepada sumber tanpa mengira lokasi hanya diberikan setelah pengesahan pengguna dan peranti berjaya; dan

iii) menekankan prinsip keistimewaan yang paling sedikit, berikan akses kepada sumber yang perlu diakses, apabila diperlukan dan hanya untuk tempoh masa.

**f) Pengauditan**

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

**g) Pematuhan**

Polisi Kawalan Keselamatan Maklumat Jabatan Wilayah Persekutuan hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan maklumat.

**h) Pemulihan**

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

**i) Saling Bergantungan**

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

## 3.0 PENGURUSAN RISIKO KESELAMATAN MAKLUMAT

Jabatan Wilayah Persekutuan hendaklah mengambil kira kewujudan risiko ke atas aset maklumat akibat dari kelemahan (vulnerability) dan ancaman yang semakin meningkat masa kini. Oleh itu, Jabatan Wilayah Persekutuan hendaklah mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset maklumat supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan yang optimum.

Jabatan Wilayah Persekutuan hendaklah melaksanakan penilaian risiko keselamatan maklumat secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan maklumat. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan maklumat berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan maklumat hendaklah dilaksanakan ke atas sistem maklumat Jabatan Wilayah Persekutuan termasuk aset fizikal Jabatan Wilayah Persekutuan, aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuk pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

Jabatan Wilayah Persekutuan bertanggungjawab melaksanakan dan menguruskan risiko keselamatan maklumat selaras dengan keperluan Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam.

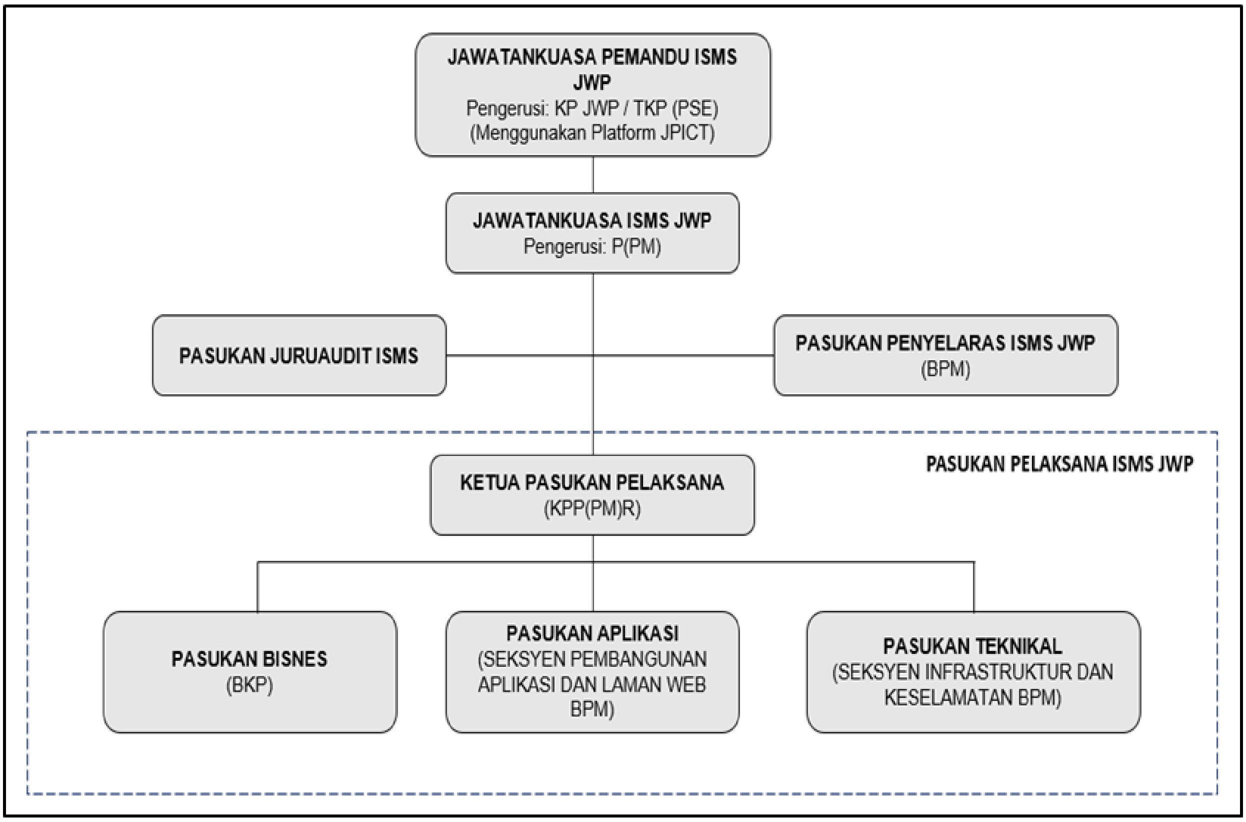
Jabatan Wilayah Persekutuan hendaklah mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
b) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan jabatan;
c) Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
d) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak lain yang berkepentingan.

Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya **sekali setahun** oleh BDPM dan dimaklumkan kepada Mesyuarat Jawatankuasa ISMS.

# 4.0 TADBIR URUS

## 4.1 Struktur Tadbir Urus Sistem Pengurusan Keselamatan Maklumat JWP




Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKKM JWP, struktur tadbir urus iaitu **Jawatankuasa Pemandu ISMS akan menggunakan Platform Jawatankuasa Pemandu ICT (JPICT)** JWP untuk meneraju Tadbir Urus Pengurusan Keselamatan Maklumat JWP:

## 4.2 Keahlian JPICT JWP adalah seperti yang berikut:

a) Pengerusi: KP JWP / TKP (PSE)

b) Ahli:

1. Timbalan Ketua Pengarah (Pengurusan dan Sosio Ekonomi)/CDO
2. Timbalan Ketua Pengarah (Perancangan dan Pembangunan)
3. Pengarah Bahagian Sosio Ekonomi
4. Pengarah Bahagian Perbandaran dan Khidmat Teknikal
5. Pengarah Bahagian Dasar, Perancangan Strategik dan Antarabangsa
6. Pengarah Bahagian Khidmat Pengurusan
7. Pengarah Bahagian Pembangunan
8. Pengarah Bahagian Digital dan Pengurusan Maklumat

9. Pengarah Bahagian Kewangan
10. Pengarah Unit Komunikasi Korporat
11. Penasihat Undang-Undang
12. Ketua Integriti
13. Ketua Penolong Pengarah Seksyen Infrastruktur dan Keselamatan Bahagian Digital dan Pengurusan Maklumat – ICTSO JWP
14. Ketua Penolong Pengarah Seksyen Pembangunan Aplikasi dan Laman Web Bahagian Digital dan Pengurusan Maklumat
15. Pengarah Eksekutif (Pengurusan) Dewan Bandaraya Kuala Lumpur
16. Pengarah Jabatan Pengurusan Maklumat Dewan Bandaraya Kuala Lumpur
17. Naib Presiden Jabatan Perkhidmatan Korporat Perbadanan Putrajaya
18. Pengarah Bahagian Teknologi Maklumat Dan Komunikasi Perbadanan Putrajaya
19. Timbalan Ketua Pegawai Eksekutif (Pengurusan) Perbadanan Labuan
20. Pengarah Jabatan Pengurusan Maklumat Perbadanan Labuan
21. Pengarah Pengurusan dan Komunikasi Korporat Perbadanan Pembangunan Kampong Baharu
22. Penolong Pengarah (Teknologi Maklumat) Perbadanan Pembangunan Kampong Bharu
23. Timbalan Pengarah Majlis Sukan Wilayah Persekutuan
24. Penolong Pegawai (Teknologi Maklumat) Majlis Sukan Wilayah Persekutuan
25. Timbalan Pengarah Sektor Khidmat Pengurusan Pejabat Tanah Dan Galian Wilayah Persekutuan
26. Ketua Penolong Pengarah Bahagian Pengurusan Maklumat, Pejabat Tanah Dan Galian Wilayah Persekutuan

c) Urus Setia:

Seksyen Perancangan Dan Pengurusan ICT
Bahagian Digital dan Pengurusan Maklumat (BDPM), JWP

d) Bidang Tugas Jawatankuasa Pemandu ISMS JWP adalah seperi berikut:

1. Meluluskan Polisi Kawalan Keselamatan Maklumat (PKKM) JWP;
2. Meluluskan Skop ISMS JWP; dan
3. Meluluskan lantikan badan yang melaksanakan Pengauditan ISMS JWP.

# 5.0 KAWALAN ORGANISASI (ORGANIZATIONAL CONTROL)

## 5.1 Polisi Keselamatan Maklumat (Information Security Policy)

**Kawalan:**

Polisi keselamatan maklumat dan polisi khusus hendaklah ditakrifkan, diluluskan oleh pengurusan, diterbitkan, dihebahkan dan dipatuhi oleh kakitangan dan pihak berkepentingan yang berkaitan dan disemak pada selang masa yang dirancang atau jika ada berlaku perubahan ketara.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.1.1** | **Pelaksanan Polisi (Execution of the Policy)**<br>Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak pengurusan JWP kepada pengguna, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan Digital JWP.<br><br>Pelaksanaan polisi hendaklah dikuatkuasakan oleh JWP dan dipantau oleh Ketua Pengarah JWP (KP JWP). | KP JWP, CDO, JK PEMANDU ISMS, ICTSO |
| **5.1.2** | **Pengesahan Polisi (Endorsement of Policy)**<br>Di peringkat tertinggi, polisi itu perlu diluluskan oleh Jawatankuasa Pemandu ISMS. | JK PEMANDU ISMS |
| **5.1.3** | **Penguatkuasaan Polisi (Enforcement Of Policy)**<br>Polisi Kawalan Keselamatan Maklumat JWP mestilah dipatuhi oleh semua pengguna JWP, pemegang taruh dan pihak ketiga yang berurusan dengan perkhidmatan Digital JWP. Setiap pengguna, pemegang taruh dan pihak ketiga yang berurusan dengan JWP hendaklah menandatangan Akuan Pematuhan PKKM seperti di Lampiran C(I) atau Lampiran C(II).<br><br>Sebarang ketidakpatuhan kepada dasar ini boleh mengakibatkan tindakan tatatertib termasuk sebarang remedi/tindakan undang-undang lain di bawah akta/peraturan/undang-undang semasa yang berkuat kuasa. Piawaian dan prosedur yang berkaitan hendaklah dipatuhi. | Pemegang taruh,<br>Warga JWP,<br>Pihak ketiga |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.1.4** | **<u>Penyebaran Polisi (User Awareness)</u>**<br>Program kesedaran tentang polisi ini hendaklah diatur dan diselaraskan. | ICTSO, JK ISMS dan Pasukan Keselamatan ICT JWP |
| **5.1.5** | **<u>Pengecualian Polisi (Exception to Policy)</u>**<br>Polisi Kawalan Keselamatan Maklumat jabatan adalah terpakai kepada semua pengguna perkhidmatan Digital dan ICT jabatan, tiada pengecualian diberikan. | Semua Pengguna |
| **5.1.6** | **<u>Penyelenggaraan Polisi (Maintenance)</u>**<br>Penyelenggaraan dan kajian semula dasar hendaklah dimulakan oleh ICTSO, Pasukan Pelaksana ISMS dan perlu disemak sekurang-kurangnya setahun sekali atau apabila diperlukan.<br><br>Semua dokumen atau rekod hendaklah diwujudkan dan diselenggara untuk menyediakan bukti pematuhan kepada keperluan dan operasi berkesan ISMS.<br><br>Semua dokumen dan rekod hendaklah dilindungi dan dikawal seperti yang dinyatakan dalam dokumen manual ISMS JWP dan undang-undang/arahan/peraturan/garis panduan semasa yang berkuat kuasa. | ICTSO, Pasukan Pelaksana ISMS |
| **5.1.7** | **<u>Kajian Semula/Semakan Polisi (Policy Review)</u>**<br>Polisi ini perlu disemak dan dipinda pada jangka masa yang dirancang atau apabila terdapat perubahan teknologi, aplikasi, prosedur, perundangan dan polisi Kerajaan bagi memastikan kesesuaian, kecukupan dan keberkesanannya berterusan. Berikut ialah prosedur yang berkaitan dengan kajian semula Polisi Kawalan Keselamatan Maklumat JWP:<br><br>a) Memastikan penguatkuasaan pelaksanaan Polisi ini; | Jawatankuasa ISMS, ICTSO, Pasukan Pelaksana ISMS |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | b) Pengarah Bahagian/Ketua Unit mengenal pasti dan menentukan perubahan yang diperlukan;<br>c) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk tindakan dan pertimbangan kepada Jawatankuasa Pemandu ISMS bagi tujuan kelulusan;<br>d) Memaklumkan pindaan yang telah diluluskan oleh Jawatankuasa Pemandu ISMS kepada warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan Digital JWP; dan<br>e) Polisi ini hendaklah dikaji semula setiap LIMA (5) TAHUN SEKALI atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan. | |

### 5.2 Peranan dan Tanggungjawab Keselamatan Maklumat (Information Security Roles and Responsibilities)

**Kawalan:**
Peranan dan tanggungjawab keselamatan maklumat hendaklah ditakrifkan dan diperuntukkan mengikut keperluan jabatan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.2.1** | **Peranan dan Tanggungjawab Keselamatan Maklumat (The Role and Responsibility of Information Security)**<br>Semua peranan dan tanggungjawab keselamatan maklumat hendaklah ditakrifkan dan diperuntukkan mengikut keperluan JWP.<br><br>**Objektif:** Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Polisi Keselamatan Maklumat JWP.<br><br>Peranan dan Tanggungjawab Keselamatan Maklumat: | Ketua Bahagian/Unit, CSIRT, BDPM |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| 5.2.2 | **Ketua Pengarah**<br>Peranan dan tanggungjawab Ketua Pengarah JWP (KP JWP) adalah seperti yang berikut:<br><br>a) Memastikan penguatkuasaan Polisi ini;<br>b) Memastikan warga, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan Digital JWP memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini;<br>c) Memastikan semua keperluan JWP seperti sumber kewangan, personel dan perlindungan keselamatan adalah mencukupi;<br>d) Memastikan pengurusan risiko dan program kawalan keselamatan maklumat dilaksanakan seperti yang ditetapkan di dalam Polisi ini; dan<br>e) Melantik CDO. | KP JWP |
| 5.2.3 | **Ketua Pegawai Digital (CDO)**<br>Peranan dan tanggungjawab CDO adalah seperti yang berikut:<br><br>a) Membantu KP dalam melaksanakan tugas-tugas yang melibatkan keselamatan maklumat seperti yang ditetapkan di dalam Polisi ini;<br>b) Memastikan kawalan keselamatan maklumat dalam JWP diseragam dan diselaraskan dengan sebaiknya;<br>c) Memastikan **Pelan Strategik Pendigitalan** JWP mengandungi aspek keselamatan siber;<br>d) Menyelaras pelan latihan dan program kesedaran kawalan keselamatan maklumat dan keselamatan siber; dan<br>e) Melantik ICTSO. | CDO |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.2.4** | **Pegawai Keselamatan ICT (ICTSO)**<br>Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti yang berikut:<br><br>a) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini;<br>b) Merangka pengurusan risiko dan audit keselamatan maklumat berpandukan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat yang berkuat kuasa;<br>c) Menyedia dan menyebarkan amaran-amaran yang sesuai terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;<br>d) Melaporkan Insiden Keselamatan Siber kepada CSIRT JWP dan seterusnya membantu dalam penyiasatan atau pemulihan;<br>e) Melaporkan Insiden Keselamatan Maklumat kepada CDO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKP);<br>f) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau Insiden Keselamatan Maklumat dan Keselamatan Siber, seterusnya memperakukan langkah-langkah baik pulih dengan segera;<br>g) Melaksanakan pematuhan Polisi ini oleh pengguna, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JWP;<br>h) Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber;<br>i) Menyedia dan merangka latihan dan program kesedaran keselamatan maklumat; | ICTSO |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | j) Merancangkan dan melaksanakan program kesedaran kepada semua warga JWP untuk memahami keperluan standard, garis panduan dan prosedur keselamatan di bawah Polisi Kawalan Keselamatan Maklumat ini;<br>k) Mewujudkan program-program bagi meningkatkan pengetahuan dan pembudayaan mengenai teknologi dan mekanisme kawalan maklumat dan aset ICT, ancaman-ancaman siber dan peranan dan tanggungjawab pengguna dalam mengendalikan kemudahan ICT di JWP; dan<br>l) Mengurus keseluruhan program-program keselamatan maklumat di JWP. | |
| **5.2.5** | **Pengarah Bahagian/Ketua Unit**<br>Peranan dan tanggungjawab Pengarah Bahagian/Unit ialah melaksanakan keperluan Polisi ini dalam operasi semasa seperti yang berikut:<br><br>a) Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru;<br>b) Pembelian atau peningkatan perisian dan sistem komputer;<br>c) Perolehan teknologi dan perkhidmatan komunikasi baru;<br>d) Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; dan<br>e) Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling / garis panduan, dan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa. | Pengarah Bahagian/Ketua Unit |
| **5.2.6** | **Pentadbir Sistem**<br>Peranan dan tanggungjawab Pentadbir Sistem adalah seperti yang berikut: | Pentadbir Sistem |

<table>
<tr><th>ID</th><th>PENERANGAN</th><th>PERANAN</th></tr>
<tr><td></td><td>a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai personel yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;<br>b) Menentukan ketepatan dan kesahihan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ini;<br>c) Memantau aktiviti capaian sistem aplikasi;<br>d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta;<br>e) Menganalisis dan menyimpan rekod jejak audit;<br>f) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan<br>g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada personel di dalam keadaan yang baik.</td><td></td></tr>
<tr><td>5.2.7</td><td>Pemilik Sistem<br>Sesuatu sistem hendaklah dimiliki oleh sesuatu Bahagian/Unit yang mempunyai kepentingan terhadap sistem yang dibangunkan. Pemilik Sistem terdiri daripada Pengarah Bahagian/Ketua Unit yang terlibat dengan sistem yang dibangunkan. Peranan dan tanggungjawab Pemilik Sistem adalah seperti berikut:<br><br>a) Pelaksanaan promosi sistem kepada pengguna sasaran;<br>b) Penentuan pengguna dan kategori atau tahap capaian pengguna sistem;<br>c) Pengurusan senarai pengguna yang terlibat di dalam Latihan Pengguna;<br>d) Penguatkuasaan penggunaan sistem di kalangan pengguna;</td><td>Pemilik Sistem</td></tr>
</table>

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | e) Pemantauan pelaksanaan dan keberkesanan sistem secara berterusan; dan<br>f) Pemakluman sebarang masalah dan keperluan peningkatan sistem kepada Pembangun Sistem. Pemilik Sistem hendaklah melantik seorang pegawai sebagai Pentadbir Sistem untuk tujuan penyenggaraan / penambahbaikan sistem yang dikendalikan tersebut. | |
| **5.2.8** | **Pentadbir Rangkaian**<br>Pentadbir Rangkaian ICT ialah Pegawai ICT yang dilantik. Peranan dan tanggungjawab Pentadbir Rangkaian ICT adalah seperti berikut:<br><br>a) Mentadbir akaun pengguna;<br>b) Merangka, melaksana dan menguatkuasa polisi kawalan keselamatan maklumat seperti perlindungan dan perkongsian data;<br>c) Merancang dan melaksana polisi ancaman keselamatan, memantau keadaan rangkaian dan mengawal penggunaan sumber;<br>d) Pemantauan aktiviti capaian harian pengguna;<br>e) Menyediaan laporan mengenai aktiviti capaian secara berkala;<br>f) Menyelia dan membuat proses backup server; dan<br>g) Memberi bantuan dalam menyelesaikan masalah-masalah yang dilaporkan oleh pengguna. | Pentadbir Rangkaian |
| **5.2.9** | **Jawatankuasa Pemandu ICT (JPICT)**<br>Peranan dan tanggungjawab JPICT seperti yang terkandung dalam Surat Pekeliling Am Bilangan 7 Tahun 2024 Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam ialah memastikan maklumat rahsia rasmi dalam persekitaran ICT ditadbir selaras dengan | JPICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | peruntukan Arahan Keselamatan dan arahan lain berkaitan yang sedang berkuat kuasa merangkumi keselamatan data bagi data dalam penggunaan (data in-use), data dalam pergerakan (data inmotion) dan data dalam simpanan (data at-rest). | |
| **5.2.10** | **Jawatankuasa ISMS**<br>Peranan dan tanggungjawab Jawatankuasa ISMS JWP adalah seperti berikut:<br><br>a) Memantau pelaksanaan pensijilan ISMS ke atas skop yang telah dikenal pasti;<br>b) Menyemak skop, penyataan dasar ISMS dan *Statement of Applicability* (SOA);<br>c) Menetapkan kriteria penerimaan risiko, tahap risiko dan risk treatment plan;<br>d) Memantau dan menyemak penemuan awal penilaian risiko;<br>e) Menyediakan cadangan struktur organisasi ISMS;<br>f) Mengadakan Kajian Semula ISMS mengikut keperluan;<br>g) Memantau, menyemak dan memperakui dokumen dan rekod pelaksanaan ISMS;<br>h) Memohon pensijilan ISMS; dan<br>i) Memantau pelaksanaan tindakan pembetulan/penambaikan dan pencegahan. | JK ISMS |
| **5.2.11** | **Cyber *Security Incident Response Team* (CSIRT) JWP**<br>Keanggotaan CSIRT adalah seperti berikut:<br>Pengarah/Pengurus: Pengarah BDPM<br><br>Ahli:<br>a) Pegawai Bahagian Digital dan Pengurusan Maklumat yang dilantik.<br><br>b) Peranan dan tanggungjawab CSIRT JWP adalah seperti yang berikut: | CSIRT JWP |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | i) Memantau, mengesan insiden, menerima, dan mengesahkan aduan insiden keselamatan siber, seterusnya mengenal pasti jenis insiden serta menilai impak insiden keselamatan siber;<br>ii) Merekod dan menjalankan siasatan awal terhadap insiden yang diterima;<br>iii) Melaksanakan pengurusan dan pengendalian insiden keselamatan siber serta mengambil tindakan awal pemulihan;<br>iv) Menjalankan penilaian untuk memastikan tahap keselamatan siber dan mengambil tindakan pemulihan serta pengukuhan keselamatan siber supaya insiden baharu dapat dielakkan;<br>v) Melaporkan insiden keselamatan siber kepada *National Cyber Coordination and Command Centre (NC4);*<br>vi) Menasihati agensi di bawah seliaannya untuk mengambil tindakan pemulihan dan pengukuhan;<br>vii) Menyebarkan makluman/amaran berkaitan insiden kepada agensi lain di bawah seliaannya;dan<br>viii) Memastikan fail log disimpan sekurang-kurangnya tiga (3) bulan. | |
| **5.2.12** | **Pengguna/Warga**<br>Peranan dan tanggungjawab pengguna adalah seperti yang berikut:<br><br>a) Membaca, memahami dan mematuhi Polisi ini;<br>b) Mengetahui dan memahami implikasi keselamatan maklumat dan keselamatan siber akibat daripada tindakannya; | Pengguna/Warga |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | c) Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumat rasmi terperingkat;<br>d) Mematuhi prinsip-prinsip keselamatan Polisi ini dan menjaga kerahsiaan maklumat Kerajaan;<br>e) Melaksanakan langkah-langkah perlindungan seperti yang berikut:<br><br>i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;<br>ii) Memeriksa maklumat dan menentukan ia tepat, terkini dan lengkap dari semasa ke semasa;<br>iii) Menentukan maklumat sedia untuk digunakan;<br>iv) Menjaga kerahsiaan maklumat;<br>v) Mematuhi dasar, piawaian dan garis panduan keselamatan maklumat dan keselamatan siber yang ditetapkan;<br>vi) Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan<br>vii) Menjaga kerahsiaan kawalan keselamatan maklumat dan siber dari diketahui umum.<br><br>f) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada CSIRT Jabatan dengan segera;<br>g) Menghadiri program-program kesedaran mengenai keselamatan maklumat dan siber; dan<br>h) Bersetuju dengan terma dan syarat Bersetuju dengan terma dan syarat yang terkandung di dalam Polisi ini. | |

## 5.3 Pengasingan Tugas (Segregation of Duties)

**Kawalan:**
Tugas dan bidang tanggungjawab yang berlainan hendaklah diasingkan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.3.1** | **Pengasingan Tugas (Segregation of Duties)**<br>Tugas dan bidang tanggungjawab yang berlainan hendaklah diasingkan bagi mengurangkan peluang mengubah suai tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset.<br><br>Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) skop tugas dan tanggungjawab hendaklah diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas maklumat;<br>b) tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi maklumat daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi;<br>c) perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai produksi;<br>d) pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan<br>e) pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya. | Ketua Bahagian/Unit |

### 5.4 Tanggungjawab Pengurusan (Management Responsibilities)

**Kawalan:**

Pengurusan hendaklah meminta semua kakitangan untuk menggunakan Keselamatan maklumat mengikut polisi kawalan keselamatan maklumat yang ditetapkan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.4.1** | **Tanggungjawab Pengurusan (Management Responsibilities)**<br>a) Pelaksanaan polisi ini akan dikuatkuasakan dan dilaksanakan oleh KP JWP dengan disokong oleh JPICT dan JK ISMS yang terdiri daripada Ketua Pegawai Digital (CDO), Pegawai Keselamatan ICT (ICTSO), Pengarah Bahagian/Unit dan ahli-ahli yang dilantik oleh KP JWP.<br><br>b) Polisi Kawalan Keselamatan Maklumat JWP mestilah dipatuhi oleh semua pengguna, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT JWP.<br><br>c) Pengurusan hendaklah memastikan warga, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan. | Ketua Bahagian/Unit |

### 5.5 Hubungan dengan Pihak Berkuasa (Contact with Authorities)

**Kawalan:**

Jabatan hendaklah mewujudkan dan mengekalkan hubungan dengan pihak berkuasa yang berkaitan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.5.1** | **Hubungan dengan Pihak Berkuasa (Contact with Authorities)** | BKP |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>a) hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab JWP;<br><br>b) mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi dan Multimedia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba, penyedia perkhidmatan telekomunikasi dan perkhidmatan bekalan air; dan<br><br>c) insiden keselamatan maklumat hendaklah dilaporkan tepat pada masanya ke pihak berkaitan seperti Agensi Keselamatan Siber Negara (National Cyber Security Agency - NACSA), selaras dengan Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022 bagi mengurangkan impak insiden.<br><br>d) Senarai Pihak Berkuasa | |

**Jadual 1: Senarai Pihak Berkuasa**

| BIL | AGENSI | ALAMAT | URUSAN |
|---|---|---|---|
| 1 | Jabatan Peguam Negara | 45, Persiaran Perdana, Presint 4,<br>62100 Putrajaya | Perundangan |

| ID | PENERANGAN | | | | PERANAN |
|---|---|---|---|---|---|
| | | | No.Tel.: 0388722000 Email: pro@agc.gov.my | | |
| | 2 | Balai POLIS Putrajaya | Ibu Pejabat Polis Daerah Putrajaya, Presint 7, 65200, Wilayah Persekutuan Putrajaya. No.Tel.: 03-88862222 Email: kpdputrajaya@rmp.gov.my | Jenayah | |
| | 3 | Balai BOMBA Putrajaya | Ketua Balai Balai Bomba dan Penyelamat Presint 7 Lebuh Wawasan, Presint 7, 62250 Wilayah Persekutuan, Putrajaya No. Tel: 03 – 8888 0970 / 8888 0971 Email: oc_putra@bomba.gov.my | Kebakaran | |
| | 4 | Hospital Putrajaya | Hospital Putrajaya Presint 7, 62250 Putrajaya. No. Tel: 03-83124200 Email: hpj_info@hpj.gov.my | Kecedaraan | |

<table>
<tr><th>ID</th><th>PENERANGAN</th><th>PERANAN</th></tr>
<tr><td></td><td>
<table>
<tr><td>5</td><td>JKR Putrajaya</td><td>Jabatan Kerja Raya Wilayah Persekutuan Putrajaya<br>Blok F7, Kompleks F<br>62000 Putrajaya.<br>No. Tel: 603-8885 6800<br>Email: aduanjkrwpp@jkr.gov.my</td><td>Kerosakan Bangunan</td></tr>
<tr><td>6</td><td>TNB Putrajaya</td><td>TNB Putrajaya<br>Pusat Khidmat Pelanggan Putrajaya<br>No. 10, Ground Floor Galeria PJH,<br>Persiaran Perdana<br>Precinct 4<br>62100 Putrajaya<br>Malaysia<br>No. Tel: 03-8889 4690</td><td>Gangguan Bekalan Elektrik</td></tr>
</table>
</td><td></td></tr>
</table>

## 5.6 Hubungan Dengan Kumpulan Berkepentingan Yang Khusus (Contact with Special Interest Groups)

**Kawalan:**

Organisasi hendaklah mewujudkan dan mengekalkan hubungan dengan kumpulan berkepentingan khas atau forum keselamatan pakar lain dan persatuan profesional.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.6.1** | **Hubungan dengan Kumpulan Berkepentingan yang Khusus (Contact with Special Interest Groups)**<br>Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan maklumat dan pertubuhan profesional hendaklah | CSIRT |

| ID | PENERANGAN | PERANAN |
|---|---|---|

dikekalkan. Menganggotai pertubuhan profesional atau pun forum bagi:

a) meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat;
b) memastikan pemahaman tentang persekitaran keselamatan maklumat adalah terkini (27002);
c) menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini;
d) mendapat akses kepada nasihat pakar keselamatan maklumat;
e) berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan
f) berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.

**Jadual 2: Senarai Pihak Berkepentingan**

| BIL. | AGENSI | ALAMAT | URUSAN |
|---|---|---|---|
| 1 | JDN | Bangunan MKN Embassy Techzone<br>Blok B, No. 3200 Jalan Teknokrat 2<br>63000 Cyberjaya, Sepang<br>Selangor Darul Ehsan<br>No. Tel: 603-8000 8000<br>Email: webmasterjdn@digital.gov.my | Pendigitalan |
| 2 | NACSA | National Security Council<br>Prime Minister's Department<br>Level LG & G, West Wing,<br>Perdana Putra Building,<br>Federal Government Administrative Center,<br>62502 Putrajaya, Malaysia<br>No. Tel: 03-8064 4848<br>Email: admin@nacsa.gov.my | Insiden Keselamatan Siber |
| 3 | CGSO | Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia<br>Jabatan Perdana Menteri,<br>Aras -1, 1 dan 2, Setia Perdana 7,<br>Kompleks Setia Perdana, | Insiden Keselamatan Fizikal dan Maklumat |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | Pusat Pentadbiran Kerajaan Persekutuan,<br>62502 Wilayah Persekutuan Putrajaya,<br>Malaysia.<br>No. Tel: 03-88726002 | |

## 5.7 Perisikan Ancaman (Threat Intelligence)

**Kawalan:**

Maklumat yang berkaitan dengan ancaman keselamatan maklumat hendaklah dikumpul dan dianalisis untuk menghasilkan perisikan ancaman.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.7.1** | **Perisikan Ancaman (Threat Intelligence)**<br>Maklumat berkaitan ancaman keselamatan maklumat hendaklah diperoleh dan dianalisis untuk menghasilkan *threat intelligence* (perisikan ancaman). Maklumat tentang ancaman sedia ada atau baharu hendaklah dikumpul dan dianalisis untuk:<br><br>a) memudahkan tindakan dan mengelakkan ancaman daripada mendatangkan kemudaratan kepada jabatan; dan<br>b) mengurangkan impak ancaman tersebut.<br><br>Risikan ancaman hendaklah:<br><br>a) relevan, memberikan pencerahan, kontekstual, dan boleh dilaksanakan untuk meningkatkan perlindungan jabatan;<br>b) melibatkan aktiviti menetapkan objektif, memilih sumber maklumat, mengumpul dan memproses maklumat, serta menganalisisnya untuk memastikan ia bermakna bagi jabatan;<br>c) memastikan hasil analisis dimasukkan ke dalam proses pengurusan risiko keselamatan maklumat jabatan dan sebagai input kepada sistem kawalan teknikal seperti firewall dan | ICTSO dan CSIRT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | sistem pengesan pencerobohan (intrusion detection system - IDS); dan<br>d) dikongsi antara jabatan untuk meningkatkan keseluruhan risikan ancaman mengikut keperluan dan tertakluk kepada arahan yang berkuat kuasa. | |

**5.8 Keselamatan Maklumat dalam Pengurusan Projek (Information Security in Project Management)**

**Kawalan:**

Keselamatan maklumat hendaklah disepadukan ke dalam pengurusan projek.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.8.1** | **Keselamatan Maklumat dalam Pengurusan Projek (Information Security in Project Management)**<br><br>Keselamatan maklumat hendaklah diberi perhatian dalam pengurusan projek tanpa mengira kerumitan, saiz, tempoh, disiplin atau skop pelaksanaannya. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br>a) keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek JWP;<br>b) objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek;<br>c) pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenal pasti kawalan-kawalan yang diperlukan;<br>d) kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi kawalan keselamatan maklumat JWP;<br>e) kesesuaian pertimbangan dan aktiviti keselamatan maklumat hendaklah disusuli | ICTSO |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | pada peringkat yang telah ditetapkan mengikut tadbir urus projek sedia ada (Jawatankuasa Teknikal Projek atau Jawatankuasa Pemandu Projek); dan<br>f) peranan dan tanggungjawab keselamatan maklumat projek hendaklah ditakrif dan ditentukan. | |
| **5.8.2** | <u>**Analisis dan Spesifikasi Keperluan Keselamatan Maklumat (Information Security Requirements Analysis and Specifications)**</u><br>Keperluan keselamatan maklumat hendaklah dimasukkan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada.<br><br>Keperluan keselamatan maklumat bagi pembangunan sistem baharu dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut:<br><br>a) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk pengkonsepan perisian, kajian keperluan, reka bentuk, pelaksanaan, pengujian, penerimaan, pemasangan, penyelenggaraan dan pelupusan;<br>b) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Polisi Kawalan Keselamatan Maklumat JWP;<br>c) Penyediaan reka bentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan maklumat yang telah ditetapkan; dan<br>**d)** Ujian keselamatan maklumat hendaklah dilakukan semasa pembangunan sistem bagi memastikan kesahihan dan integriti data. | Pentadbir Sistem ICT |

## 5.9 Inventori maklumat dan aset lain yang berkaitan (Inventory of information and other associated assets)

**Kawalan:**
Inventori maklumat dan aset lain yang berkaitan, termasuk pemilik, hendaklah disediakan dan diselenggara.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.9.1** | **Inventori Aset (Inventory of Assets)**<br>Menyokong dan memberi perlindungan yang bersesuaian ke atas semua aset ICT jabatan. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut:<br><br>a) Jabatan hendaklah mengenal pasti Pegawai Penerima Aset setiap Bahagian untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT.<br>b) Memastikan semua aset ICT dikenal pasti, diklasifikasi, di dokumen, diselenggara dan dilupuskan. Maklumat aset direkod dan dikemas kini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa.<br>c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja.<br>d) Memastikan inventori maklumat dan aset lain yang berkaitan hendaklah tepat, terkini, dan konsisten.<br>e) Pegawai Aset hendaklah mengesahkan penempatan aset ICT. | Pegawai Aset, Pegawai Penerima Aset dan warga JWP |
| **5.9.2** | **Pemilikan Aset (Ownership of Assets)**<br>Aset yang diselenggara hendaklah hak milik jabatan.<br><br>Tanggungjawab yang perlu dipatuhi oleh pemilik aset adalah termasuk perkara-perkara berikut: | Pegawai Aset dan warga JWP |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | a) memastikan aset di daftarkan dalam senarai aset mengikut klasifikasi aset dan diserahkan kepada pemilik aset;<br>b) memastikan semua jenis aset dipelihara dan diselenggara dengan baik;<br>c) Kenal pasti dan kaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan;<br>d) memastikan pengendalian aset dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan<br>e) Aset bukan hakmilik jabatan hendaklah diurus mengikut Prosedur/arahan-arahan atau Polisi BYOD JWP yang berkuat kuasa. | |
| **5.9.3** | **Aset Bukan Hakmilik Jabatan**<br>Pengguna BYOD hendaklah mematuhi tatacara penggunaan BYOD seperti berikut:<br><br>a) Semua peringkat maklumat rasmi kerajaan adalah hak milik kerajaan;<br>b) Sebarang bahan rasmi yang dimuatnaik/edar/kongsi hendaklah mendapat kebenaran Pengarah Bahagian/Ketua Unit;<br>c) Menandatangani Surat Akuan Pematuhan PKKM dan Akta Rahsia Rasmi 1972;<br>d) Memastikan peranti yang digunakan mempunyai kawalan keselamatan seperti berikut:<br><br>i) Menetapkan mekanisme kawalan akses bagi BYOD dan akan mengunci secara automatik apabila tidak digunakan;<br>ii) Melaksanakan penyulitan dan / atau perlindungan ke atas folder yang mempunyai maklumat rasmi Kerajaan yang disimpan di dalam peranti BYOD; dan<br>iii) Memastikan BYOD mempunyai ciri-ciri keselamatan standard seperti antivirus, patching terkini dan anti theft. | Pengguna BYOD |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | e) Pengguna adalah dilarang daripada melakukan perkara berikut:<br><br>i) Menyimpan maklumat rasmi di dalam BYOD;<br>ii) Menggunakan BYOD untuk mengakses, menyimpan dan menyebarkan maklumat rasmi dan terperingkat kepada pihak yang tidak dibenarkan;<br>iii) Menjadikan BYOD sebagai medium pendua (backup) bagi maklumat rasmi;<br>iv) Merakam komunikasi dan dokumen rasmi untuk tujuan peribadi; dan<br>v) Menjadikan BYOD sebagai access point kepada aset ICT Jabatan untuk capaian ke Internet tanpa kebenaran.<br><br>f) Pengguna adalah tertakluk kepada perkara seperti berikut:<br><br>i) Menggunakan BYOD secara berhemah sepanjang masa dan mematuhi mana-mana peraturan/dasar yang berkuat kuasa;<br>ii) Memadamkan segala maklumat yang berkaitan dengan urusan rasmi Jabatan sekiranya bertukar/ ditamatkan perkhidmatan/ bersara ATAU sewaktu dihantar ke pusat servis untuk penyelenggaraan;<br>iii) Bertanggungjawab dan boleh dikenakan tindakan tatatertib sekiranya didapati menyalahgunakan BYOD yang menyebabkan kehilangan/kerosakan/pendedahan maklumat rasmi Kerajaan;<br>iv) JWP tidak bertanggungjawab atas kehilangan, kerosakan data atau sistem/aplikasi dalam BYOD yang digunakan untuk tujuan urusan rasmi Jabatan; | |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | v) JWP tidak bertanggungjawab mengkonfigurasi atau menyelenggara peranti BYOD; dan<br>vi) JWP berhak merampas mana-mana BYOD pengguna sekiranya didapati atau disyaki tidak mematuhi peraturan yang telah ditetapkan. | |
| **5.9.4** | **<u>Pengelasan Maklumat aset (Information Classification Assets)</u>**<br>Memastikan setiap aset ICT diklasifikasikan mengikut klasifikasi aset. | Pegawai pengkelas/Aset |

**5.10 Penggunaan maklumat yang boleh diterima dan aset lain yang berkaitan (Acceptable use of information and other associated assets)**

**<u>Kawalan:</u>**
Peraturan untuk penggunaan yang boleh diterima dan prosedur untuk mengendalikan maklumat dan aset lain yang berkaitan hendaklah dikenal pasti, didokumenkan dan dilaksanakan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.10.1** | **<u>Penggunaan Aset yang Dibenarkan (Acceptable Use of Assets)</u>**<br>Memastikan pengguna menggunakan aset ICT untuk tujuan rasmi dan mengikut fungsi sebenar. | Pengguna Aset |
| **5.10.2** | **<u>Pengendalian Aset (Handling of Assets)</u>**<br>Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, membuat salinan, menghantar, menyampai, menukar dan memusnah perlu mengambil kira langkah-langkah keselamatan berikut:<br><br>i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;<br>ii) Memeriksa dan menentukan maklumat adalah tepat, terkini dan lengkap dari semasa ke semasa;<br>iii) Menentukan maklumat sedia untuk digunakan; | Pegawai Aset dan Pengguna |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | iv) Menjaga kerahsiaan kata laluan;<br>v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;<br>vi) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, membuat salinan, penghantaran, penyampaian, pertukaran dan pemusnahan;<br>vii) Menjaga kerahsiaan langkah-langkah keselamatan maklumat dan siber daripada diketahui umum;<br>viii) Sekatan akses yang menyokong keperluan perlindungan untuk setiap peringkat pengelasan; dan<br>ix) Penyelenggaraan rekod pengguna yang dibenarkan bagi maklumat dan aset lain yang berkaitan. | |

### 5.11 Pemulangan Aset (Return of assets)

**Kawalan:**

Kakitangan dan pihak lain yang berkepentingan hendaklah memulangkan semua aset jabatan dalam pegangan mereka selepas pertukaran atau penamatan pekerjaan, kontrak atau perjanjian.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.11.1** | **Pemulangan Aset (Return of Assets)**<br><br>a) Pengguna hendaklah memulangkan aset ICT kepada BDPM pada hari terakhir perkhidmatan di jawatan semasa, sama ada disebabkan pertukaran dalaman, pertukaran jabatan, penamatan perkhidmatan/kontrak atau persaraan.<br>b) Pemulangan aset ICT hendaklah dilakukan sendiri oleh pengguna dan tidak boleh diwakilkan kepada orang lain.<br>c) Pengguna yang gagal memulangkan aset ICT atas namanya adalah bertanggungjawab | Pengguna |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | sepenuhnya terhadap sebarang kerosakan atau kehilangan peralatan tersebut.<br>d) Semua aset ICT yang dipinjam atau disewakan hendaklah disanitasi mengikut tatacara yang telah ditetapkan. | |

### 5.12 Pengelasan Maklumat (Classification of Information)

**Kawalan:**

Maklumat hendaklah dikelaskan mengikut keperluan keselamatan maklumat jabatan berdasarkan kerahsiaan, integriti, ketersediaan dan keperluan pihak berkepentingan yang berkaitan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.12.1** | **Pengelasan Maklumat (Classification of Information)**<br><br>a) **JWP** selaku pemilik maklumat bertanggungjawab untuk pengelasan maklumat di JWP.<br><br>b) Maklumat hendaklah dikelas oleh Pegawai Pengelas mengikut keperluan keselamatan maklumat yang telah ditetapkan di dalam Arahan Keselamatan dan berdasarkan kerahsiaan, integriti, ketersediaan/keboleh sediaan dan keperluan pihak berkepentingan lain.<br><br>c) Klasifikasi dan kawalan perlindungan maklumat yang berkaitan hendaklah mengambil kira keperluan perkhidmatan untuk berkongsi atau menyekat maklumat, untuk melindungi kerahsiaan, integriti atau ketersediaan maklumat. Aset selain daripada maklumat boleh diklasifikasikan mengikut klasifikasi maklumat, yang disimpan dalam, diproses oleh atau sebaliknya dikendalikan atau dilindungi oleh aset | Pegawai pengkelas/ Pegawai Rekod Jabatan /Pegawai Pengawal Dokumen |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | d) **JWP** hendaklah mengambil kira keperluan untuk kerahsiaan, integriti dan ketersediaan dalam skim pengelasan.<br><br>i) Maklumat hendaklah dikelaskan oleh Pegawai Pengelas yang dilantik dan ditanda dengan peringkat keselamatan sebagaimana yang ditetapkan di dalam Arahan Keselamatan.<br>ii) Patuhi piawaian, prosedur, tatacara dan garis panduan keselamatan yang dikeluarkan.<br>iii) Memberi perhatian semasa mengendalikan maklumat rahsia terperingkat.<br>iv) Elak pendedahan maklumat kepada pihak yang tidak dibenarkan.<br>v) Pengelasan maklumat adalah berpandukan kepada Arahan Keselamatan, Arkib negara, Akta Rahsia Rasmi 1972 dan Surat Pekeliling Am Bilangan 2 Tahun 1987: Garis Panduan Mengenai Pengelasan Dokumen Rasmi Kerajaan.<br>vi) Fail Satu folder yang diklasifikasikan mengikut kaedah yang tertentu (nombor/abjad dan sebagainya) supaya kandungan di dalamnya mudah dikesan.<br>vii) Kategori fail:<br>a. Fail Rahsia Besar Fail berwarna kuning dengan berpalang merah di sebelah luar kulit hadapan dan belakang - disimpan dalam bilik kebal atau peti besi yang seelok-eloknya dipasang dengan kunci tata kira.<br>b. Fail Rahsia Fail berwarna merah jambu dengan berpalang merah di sebelah luar kulit hadapan dan belakang - disimpan sama seperti dokumen terperingkat RAHSIA | |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | BESAR atau dalam kabinet keluli atau almari keluli yang dipasang dengan palang besi berkunci.<br>c. Fail Rasmi Dokumen rasmi kerajaan yang dikandung, disusun dengan teratur dan didaftarkan. Fail ini diberi tajuk spesifik sepertimana yang telah ditetapkan dalam Klasifikasi Fail.<br>d. Fail Sulit Fail berwarna hijau - disimpan dalam kabinet keluli atau almari keluli.<br>e. Fail Terhad Fail berwarna putih - disimpan dalam kabinet keluli atau almari keluli.<br>f. Fail Terbuka berwarna putih - disimpan dalam kabinet keluli atau almari keluli. | |

### 5.13 Pelabelan Maklumat (Labelling of Information)

**Kawalan:**

Kakitangan dan pihak lain yang berkepentingan mengikut kesesuaian hendaklah memulangkan semua aset organisasi dalam milikan mereka selepas pertukaran atau penamatan pekerjaan, kontrak atau perjanjian mereka.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.13.1** | **Pelabelan Maklumat (Labelling of Information)**<br>Prosedur penandaan peringkat keselamatan pada maklumat hendaklah mematuhi dan berdasarkan Arahan Keselamatan.<br><br>a) Memastikan setiap maklumat diberikan tahap perlindungan yang bersesuaian.<br>b) Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut Arkib Negara.<br>c) Contoh kaedah pelabelan termasuk:<br>i) label fizikal;<br>ii) header dan footer;<br>iii) rubber stamps. | Pengawai pengkelas/ Pegawai Rekod Jabatan /Pegawai Pengawal Dokumen |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | | |

### 5.14 Pemindahan data dan maklumat (Information transfer)

**Kawalan:**

Peraturan, prosedur atau perjanjian pemindahan maklumat hendaklah disediakan untuk semua jenis kemudahan pemindahan dalam jabatan dan antara jabatan dengan lain.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.14.1** | **Polisi dan Prosedur Pemindahan Data dan Maklumat (Information Transfer Policies and Procedures)**<br>a) Memastikan keselamatan perpindahan/pertukaran data maklumat dan perisian antara JWP dan pihak luar terjamin.<br><br>b) Perkara yang hendaklah dipatuhi adalah seperti berikut:<br>i) Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi;<br>ii) Terma pemindahan data, maklumat dan perisian antara jabatan dengan pihak luar hendaklah dimasukkan di dalam Perjanjian;<br>iii) Media yang mengandungi maklumat hendaklah dilindungi; dan<br>iv) Memastikan maklumat yang terdapat dalam e-mel elektronik hendaklah dilindungi sebaik-baiknya. | CDO / ICTSO / Pentadbir Sistem / Pengguna dan pembekal |
| **5.14.2** | **Perjanjian Mengenai Pemindahan Data dan Maklumat (Agreements on Information Transfer)**<br>a) JWP hendaklah mengambil kira keselamatan maklumat atau menandatangani perjanjian bertulis apabila berlaku pemindahan data dan | CDO dan Ketua Bahagian / Ketua Unit |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | maklumat jabatan antara jabatan dengan pihak luar. Perkara yang hendaklah dipertimbangkan adalah:<br><br>i) Pengarah Bahagian hendaklah mengawal penghantaran dan penerimaan maklumat jabatan;<br>ii) Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat jabatan;<br>iii) Mengenal pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan<br>iv) JWP hendaklah mengenal pasti perlindungan data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.<br><br>b) Jabatan hendaklah juga merujuk dan patuh Dasar Perkongsian Data Sektor Awam dan Dasar Perkongsian Data Nasional dalam melaksanakan Perjanjian Mengenai Pemindahan Data dan Maklumat. | |
| **5.14.3** | **Pesanan Elektronik (Electronic Messaging)**<br>Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan undang-undang bertulis lain yang berkuat kuasa adalah seperti berikut:<br><br>a) Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di jabatan-jabatan Kerajaan Bilangan 1 Tahun 2003; | Warga Jabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | b) Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 – Pematuhan Tatacara Penggunaan E-mel dan Internet;<br>c) Surat Arahan Ketua Jabatan bertarikh 1 Jun 2007 - Langkah-langkah mengenai penggunaan Mel Elektronik jabatan-jabatan Kerajaan;<br>d) Pengurusan Perkhidmatan Komunikasi Bersepadu Kerajaan Government Unified Communication (MyGovUC) dan mana-mana undang-undang bertulis yang berkuat kuasa; dan<br>e) Sebarang e-mel rasmi hendaklah direkod ke dalam Digital Document Management System 2.0 untuk tujuan rekod. | |

### 5.15 Kawalan capaian (Access control)

**Kawalan:**

Peraturan untuk mengawal capaian fizikal dan logik kepada maklumat dan aset lain yang berkaitan hendaklah diwujudkan dan dilaksanakan berdasarkan keperluan keselamatan jabatan dan maklumat.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.15.1** | **Polisi Kawalan Akses (Access Control Policy)**<br>a) JWP selaku pemilik maklumat dan aset lain yang berkaitan hendaklah menentukan keselamatan maklumat dan keperluan perkhidmatan/bisnes yang berkaitan dengan kawalan akses. Dasar khusus mengenai kawalan akses hendaklah ditakrifkan dengan mengambil kira keperluan ini dan harus dimaklumkan kepada semua pihak yang berkepentingan yang berkaitan.<br><br>b) Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Kawalan akses ditetapkan berdasar prinsip perlu tahu (diberikan akses atas dasar | Pemilik perkhidmatan digital dan Pentadbir Sistem ICT. |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | keperluan untuk melaksanakan tugas dan keperluan untuk digunakan (hanya diberikan akses kepada infrastruktur teknologi maklumat di mana terdapat keperluan yang jelas).<br><br>c) Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu disemak, dikemas kini dan disahkan setahun sekali atau mengikut keperluan serta menyokong peraturan kawalan capaian pengguna sedia ada.<br><br>d) Perkara-perkara yang perlu dipertimbangkan dalam menentukan kawalan akses adalah seperti berikut:<br>i) Menentukan entiti mana yang memerlukan jenis akses kepada maklumat dan aset lain yang berkaitan;<br>ii) keperluan keselamatan aplikasi ditentukan dan diselaraskan dengan keperluan akses entiti;<br>iii) Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian;<br>iv) akses fizikal, yang perlu disokong oleh kawalan kemasukan fizikal yang sesuai;<br>v) penyebaran maklumat dan kebenaran capaian patuh kepada prinsip-prinsip keselamatan yang ditetapkan (cth. prinsip perlu tahu) dan megikut tahap keselamatan maklumat dan klasifikasi maklumat yang dibenarkan;<br>vi) sekatan kepada akses istimewa hendaklah dihadkan dan diurus (pengurusan hak akses);<br>vii) pengasingan tugas, fungsi kawalan capaian (cth. permintaan capaian, | |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | kebenaran capaian, pentadbiran capaian);<br>viii) Patuh undang-undang, peraturan berkaitan yang berkuat kuasa semasa dan sebarang kewajipan kontrak berkaitan pengehadan akses kepada data atau perkhidmatan<br>ix) kebenaran rasmi untuk permintaan akses<br>x) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran;<br>xi) Pengasingan peranan kawalan capaian;<br>xii) Kebenaran rasmi permohonan akses;<br>xiii) Keperluan semakan hak akses berkala;<br>xiv) Pembatalan hak akses;<br>xv) Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat;<br>xvi) Capaian privilege; dan<br>xvii) pengelogan. | |
| **5.15.2** | **<u>Capaian kepada Rangkaian dan Perkhidmatan Rangkaian (Access to Networks and Network Services)</u>**<br>Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari jabatan. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan:<br><br>a) Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian Jabatan, rangkaian jabatan lain dan rangkaian awam;<br>b) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan | ICTSO, Pengarah Bahagian dan Pentadbir Rangkaian |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT. | |
| **5.15.3** | **<u>Kawalan Capaian (Access Control)</u>**<br>Kawalan capaian adalah untuk menguruskan, mengawasi, dan meningkatkan capaian maklumat dan Aset JWP dengan selamat. Ini merangkumi pelbagai aspek operasi dan pengurusan untuk memastikan JWP mencapai matlamat, sasaran, dan hasil yang diinginkan dengan kawalan seperti berikut:<br><br>a) Mematuhi undang-undang, peraturan, dan polisi yang berkaitan dengan keselamatan maklumat.<br>b) Memastikan bahawa dasar, prosedur, dan amalan keselamatan maklumat dipatuhi dan dilaksanakan dengan betul.<br>c) Mengenalpasti, menilai, dan menguruskan risiko keselamatan maklumat yang berkaitan dengan operasi dan capaian maklumat organisasi.<br>d) Memastikan keselamatan maklumat dan data dalam organisasi dengan mematuhi amalan keselamatan maklumat yang sesuai.<br>e) Meningkatkan kesedaran dan kepahaman kakitangan tentang peningkatan capaian dan amalan keselamatan maklumat dalam organisasi.<br>f) Memantau dan menilai prestasi keselamatan capaian berterusan untuk mengenalpasti peningkatan dan kesan tindakan yang diperlukan. | ICTSO |
| **5.15.4** | **<u>Keperluan Jabatan Untuk Kawalan Akses (Business Requirements of Access Control)</u>**<br>Menghadkan akses pembekal, kakitangan dan pengguna pihak luar kepada kemudahan pemprosesan data dan maklumat dengan | ICTSO / Pemilik perkhidmatan digital dan Pentadbir Sistem ICT/ |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat. | Pengguna / Pembekal |

### 5.16 Pengurusan Identiti (Identity management)

**Kawalan:**

Kitaran hayat penuh identiti hendaklah diuruskan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.16.1** | **Pendaftaran dan Pembatalan Pengguna (User Registration and De-Registration)**<br>a) Setiap pengguna adalah bertanggungjawab ke atas aset ICT yang diamanahkan.<br><br>b) Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:<br><br>i) Akaun pengguna hanya diwujudkan setelah mendapat pengesahan Bahagian Pengurusan Maklumat dan pengguna telah mengesahkan memahami Polisi Kawalan Keselamatan Maklumat (PKKM) seperti Lampiran C(I) atau Lampiran C(II): Surat Akuan Pematuhan Polisi Kawalan Keselamatan Maklumat JWP**;**<br>ii) Akaun yang diperuntukkan oleh JWP sahaja boleh digunakan;<br>iii) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;<br>iv) Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada Ketua Bahagian/Unit dan Pemilik Sistem terlebih dahulu;<br>v) Menentukan setiap akaun yang diwujudkan atau dibatalkan telah | Pengguna dan Pentadbir Sistem |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | mendapat kelulusan Pengarah Bahagian/Unit;<br>vi) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan JWP. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;<br>vii) Penggunaan akaun milik individu lain adalah dilarang;<br>viii) Akaun pengguna tidak boleh dikongsi; dan<br>ix) Akaun pengguna boleh dibeku atau ditamatkan apabila menerima arahan daripada Seksyen Pengurusan Sumber Manusia, BKP atas sebab-sebab berikut:<br>a. Pengguna bercuti panjang dalam tempoh waktu melebihi tiga (3) minggu;<br>b. Bertukar bidang tugas kerja;<br>c. Bertukar ke jabatan lain;<br>d. Bersara;<br>e. Bagi menjalankan siasatan; atau<br>f. Ditamatkan perkhidmatan.<br>x) Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. | |
| **5.16.2** | **<u>Pengurusan Identiti (Identity Management)</u>**<br>a) Menguruskan profiling kakitangan bermula daripada penciptaan rekod kakitangan baharu sehingga penamatan profil apabila kakitangan meninggalkan pekerjaan (pencen, berhenti kerja atau kematian) serta kawalan capaian pengguna ke atas aset ICT JWP**.** | Ketua Jabatan/Penyelia/ Pemilik Sistem |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | b) Pendaftaran, pengemaskinian dan penamatan akaun pengguna dilaksanakan mengikut prosedur yang ditetapkan.<br><br>c) Proses pengurusan identiti harus memastikan bahawa:<br><br>i) Identiti yang diberikan khusus hanya dikaitkan dengan seorang sahaja untuk membolehkan orang itu bertanggungjawab atas tindakan yang dilakukan dengan identiti khusus ini;<br>ii) Identiti yang diberikan kepada berbilang orang (cth. identiti bersama) hanya dibenarkan jika mereka perlu atas sebab perkhidmatan atau operasi dan tertakluk kepada kelulusan khusus dan dokumentasi;<br>iii) identiti yang diberikan kepada entiti bukan manusia tertakluk kepada kelulusan yang diasingkan dengan sewajarnya dan pengawasan berterusan;<br>iv) identiti dipadamkan atau dikeluarkan segera tepat pada masanya jika ia tidak lagi diperlukan (cth. jika entiti berkaitannya dipadamkan atau tidak lagi digunakan, atau jika orang yang dikaitkan dengan identiti telah meninggalkan organisasi atau menukar peranan);<br>v) dalam domain tertentu, identiti tunggal dipetakan kepada entiti tunggal, [i.e. pemetaan berbilang identiti kepada entiti yang sama dalam konteks yang sama (identiti pendua) dielakkan kecuali dengan kelulusan; dan | |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | vi) rekod penggunaan dan pengurusan identiti pengguna dan maklumat pengesahan hendaklah disimpan. | |

**5.17 Maklumat Pengesahan (Authentication Information)**

**Kawalan:**

Peruntukan dan pengurusan maklumat pengesahan hendaklah dikawal oleh proses pengurusan, termasuk menasihati kakitangan mengenai pengendalian maklumat pengesahan yang sesuai.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.17.1** | **Pengurusan Maklumat Pengesahan Rahsia (Management of Secret Authentication Information)**<br>a) Pengurusan maklumat pengesahan rahsia bagi pengguna hendaklah diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.<br><br>b) Prosedure dan proses pengurusan maklumat pengesahan rahsia hendaklah memastikan bahawa:<br><br>i) Kata laluan peribadi atau nombor pengenalan diri (PIN) yang dijana secara automatik semasa proses pendaftaran sebagai maklumat pengesahan rahsia sementara mestilah tidak dapat diteka dan unik untuk setiap orang, dan pengguna dikehendaki menukarnya selepas penggunaan pertama;<br>ii) prosedur yang telah diwujudkan untuk mengesahkan identiti pengguna sebelum memberikan maklumat pengesahan baru, gantian atau sementara;<br>iii) Maklumat pengesahan, termasuk maklumat pengesahan sementara, | ICTSO dan Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | dihantar kepada pengguna secara selamat (contohnya, melalui saluran yang disahkan dan dilindungi), dan penggunaan mesej e-mel elektronik yang tidak dilindungi (clear text) untuk tujuan ini mesti dielakkan;<br>iv) Pengguna mengakui penerimaan maklumat pengesahan;<br>v) Maklumat pengesahan asal (default) seperti yang ditetapkan atau diberikan oleh vendor diubah dengan segera selepas pemasangan sistem atau perisian; dan<br>vi) Rekod peristiwa penting mengenai peruntukan dan pengurusan maklumat pengesahan disimpan dan kerahsiaannya dijamin, serta kaedah penyimpanan rekod disetujui (contohnya, dengan menggunakan alat penyimpanan kata laluan yang diluluskan). | |
| **5.17.2** | **<u>Penggunaan Maklumat Pengesahan Rahsia (Use of Secret Authentication Information)</u>**<br>Peranan dan tanggungjawab pengguna adalah seperti yang berikut:<br><br>a) Membaca, memahami dan mematuhi Polisi Kawalan Keselamatan Maklumat jabatan;<br>b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya;<br>c) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat jabatan;<br>d) Melaksanakan langkah-langkah perlindungan seperti yang berikut:<br><br>i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; | Pengguna, Pentadbir Sistem ICT dan Pengarah Bahagian |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | ii) Memeriksa maklumat dan menentukan ia tepat, terkini dan lengkap dari semasa ke semasa;<br>iii) Menentukan maklumat sedia untuk digunakan;<br>iv) Menjaga kerahsiaan kata laluan;<br>v) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;<br>vi) Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;<br>vii) Menjaga kerahsiaan langkah-langkah keselamatan maklumat dan siber daripada diketahui umum; dan<br>viii) maklumat pengesahan terjejas atau telah dikompromi hendaklah ditubah serta-merta apabila pemberitahuan atau petunjuk sebarang kompromi diterima.<br><br>e) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera;<br>f) Menghadiri program-program kesedaran mengenai keselamatan siber; dan<br>g) Pengguna hendaklah mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahan identiti. | |
| **5.17.3** | **<u>Sistem Pengurusan Kata Laluan (Password Management System)</u>**<br>Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh jabatan seperti yang berikut: | Pengguna, Pentadbir Sistem, ICTSO, Pengarah Bahagian |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;<br>b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;<br>c) Panjang kata laluan mestilah sekurang-kurangnya DUA BELAS (12) AKSARA dengan gabungan antara huruf besar, huruf kecil, aksara khas dan nombor (alphanumeric) contoh: MyP@ssw0rd!9 KECUALI bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad;<br>d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekali pun;<br>e) Kata laluan paparan kunci (lock screen) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;<br>f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara;<br>g) Kuat kuasa pertukaran kata laluan semasa atau selepas login kali pertama atau selepas reset kata laluan;<br>h) kata laluan tidak berdasarkan perkataan kamus atau gabungannya;<br>i) kata laluan yang sama tidak digunakan merentas perkhidmatan dan sistem yang berbeza;<br>j) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;<br>k) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum TIGA (3) KALI sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; | |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | l) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna;<br>m) Mewajibkan pengguna menukar kata laluan sekurang-kurangnya setiap tiga (3) bulan untuk ke semua sistem/aplikasi utama;dan<br>n) Pengguna tidak boleh menggunakan semula lima (5) kata laluan terakhir semasa menetapkan kata laluan baharu. | |

### 5.18 Hak Capaian (Access Rights)

**Kawalan:**

Hak akses kepada maklumat dan aset lain yang berkaitan hendaklah diperuntukkan, disemak, diubah suai dan dikeluarkan mengikut polisi khusus jabatan dan peraturan untuk kawalan akses.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.18.1** | **Peruntukan Akses Pengguna (User Access Provisioning)**<br>a) Hak akses kepada maklumat dan aset JWP yang berkaitan hendaklah diperuntukkan, disemak, diubah suai dan dikeluarkan mengikut dasar/ peraturan atau garis panduan kawalan akses yang berkuat kuasa.<br><br>b) Pentadbir Sistem ICT perlu mewujudkan Prosedur Pendaftaran dan Penamatan Pengguna sistem masing-masing.<br><br>c) Proses peruntukkan akses pengguna dan pembatalan hak akses fizikal dan logik yang diberikan kepada entiti yang telah disahkan identitinya hendaklah termasuk:<br><br>i) Hak Akses yang berkaitan dengan setiap sistem atau produk yang perlu diberikan hendaklah dikenal pasti dan dibenarkan. | Pentadbir Sistem ICT dan Pengarah Bahagian |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | ii) Hak akses maklumat dan aset JWP mesti dihadkan berdasarkan keperluan untuk mengetahui dan prinsip-prinsip keselamatan yang ditetapkan.<br>iii) Individu yang bukan warga JWP TIDAK boleh diberikan ID pengguna atau diberi keistimewaan untuk menggunakan atau mengakses Aset JWP (komputer, maklumat atau sistem komunikasi) melainkan ia dibenarkan.<br>iv) Kebenaran rasmi mestilah telah ditandatangani oleh wakil yang diberi kuasa di organisasi pihak ketiga sebelum akses diberikan kepada mana-mana pihak ketiga.<br>v) Hak akses hendaklah ditamatkan apabila entiti/individu tidak lagi perlu mengakses maklumat dan aset yang berkaitan tepat pada masanya.<br>vi) hak akses sementara untuk tempoh masa terhad boleh dipertimbangkan bila diperlukan dan hendaklah dibatalkan pada tarikh tamat tempoh.<br>vii) Tahap akses yang diberikan hendaklah mengikut dasar kawalan akses yang ditetapkan, peranan dan konsisten dengan keperluan keselamatan maklumat lain seperti pengasingan tugas.<br>viii) hak akses pengguna hendaklah diubah suai selari dengan peranan atau pekerjaan.<br>ix) hak akses diaktifkan hanya selepas kebenaran diperolehi.<br>x) rekod hak akses logik dan fizikal pengguna hendaklah disimpan. | |
| **5.18.2** | **<u>Kajian Semula Hak Akses Pengguna (Review of User Access Rights)</u>** | ICTSO dan Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | a) Pemilik aset hendaklah menyemak hak akses pengguna pada selang masa yang ditetapkan. Pentadbir Sistem perlu mewujudkan Rekod Pendaftaran dan Penamatan Pengguna sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna pada selang masa yang ditetapkan.<br><br>b) Semakan ke atas hak akses fizikal dan logik hendaklah mempertimbangkan perkara berikut:<br>i) hak akses pengguna selepas sebarang perubahan dalam organisasi (cth. pertukaran pekerjaan, kenaikan pangkat, penurunan pangkat) atau penamatan pekerjaan.<br>ii) kebenaran untuk hak akses istimewa. | |
| **5.18.3** | <u>**Pembatalan atau Pelarasan Hak Akses (Removal or Adjustment of Access Rights)**</u><br>a) Hak akses pengguna kepada maklumat dan aset JWP yang berkaitan hendaklah disemak dan diselaraskan atau ditamatkan sebelum sebarang perubahan atau penamatan pekerjaan berdasarkan penilaian faktor risiko seperti:<br><br>i) sama ada penamatan atau perubahan penempatan oleh pengguna atau pengurusan dan sebab penamatan;<br>ii) tanggungjawab semasa pengguna; dan<br>iii) nilai semasa aset yang dibenarkan diakses oleh pengguna.<br><br>b) Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/ dibatalkan selepas penamatan perkhidmatan, | Pentadbir Sistem ICT dan Pengarah Bahagian |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam Jabatan. | |
| **5.18.4** | **<u>Tanggungjawab Pengguna (User Responsibilities)</u>**<br>Pengguna bertanggungjawab melindungi maklumat pengesahan hak capaian masing-masing. | Pengguna |

**5.19 Keselamatan Maklumat Dalam Hubungan Pembekal (Information Security Policy for Supplier Relationships)**

**<u>Kawalan:</u>**

Proses dan prosedur hendaklah ditakrifkan dan dilaksanakan untuk mengurus risiko keselamatan maklumat yang berkaitan dengan penggunaan produk atau perkhidmatan pembekal.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.19.1** | **<u>Polisi Keselamatan Maklumat Untuk Hubungan Pembekal (Information Security Policy for Supplier Relationships)</u>**<br>a) Keperluan keselamatan maklumat hendaklah ditakrifkan, dilaksanakan, dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset JWP. Perkara yang hendaklah dipertimbangkan adalah seperti yang berikut:<br><br>i) Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori;<br>ii) Proses kitaran hayat (lifecycle) yang seragam untuk menguruskan pembekal;<br>iii) Mengawal dan memantau akses pembekal;<br>iv) Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian;<br>v) Jenis-jenis obligasi kepada pembekal; | Pengarah Bahagian, Pemilik Projek dan Pembekal |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | vi) Pelan kontigensi (contingency plan) bagi memastikan ketersediaan kemudahan pemprosesan maklumat;<br>vii) Melaksanakan program kesedaran terhadap Polisi Kawalan Keselamatan Maklumat jabatan kepada pembekal;<br>viii) Menandatangani Surat Akuan Pematuhan Polisi Kawalan Keselamatan Maklumat Jabatan Lampiran C(I) atau Lampiran C(II); dan<br>ix) Pembekal hendaklah mematuhi arahan keselamatan yang berkuat kuasa.<br><br>b) Jabatan hendaklah mengenal pasti dan melaksanakan proses dan prosedur bagi mengurus risiko yang berkaitan dengan penggunaan produk dan perkhidmatan pembekal termasuk penamatan penggunaan produk dan perkhidmatan pembekal.<br><br>c) Memastikan penamatan hubungan pembekal yang selamat, termasuk:<br><br>i) membatalkan peruntukan hak akses;<br>ii) pengendalian maklumat yang selamat;<br>iii) menentukan pemilikan harta intelek yang dibangunkan semasa tempoh perjanjian;<br>iv) maklumat dialihkan dengan selamat sekiranya berlaku pertukaran pembekal atau penyumberan;<br>v) pengurusan rekod;<br>vi) pemulangan aset;<br>vii) pelupusan selamat maklumat dan aset lain yang berkaitan; dan<br>viii) keperluan kerahsiaan berterusan. | |

### 5.20 Menangani Keselamatan Dalam Perjanjian (Addressing Security Within Supplier Agreements)

**<u>Kawalan:</u>**

Keperluan keselamatan maklumat yang berkaitan hendaklah diwujudkan dan dipersetujui dengan setiap pembekal berdasarkan jenis perkhidmatan pembekal.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.20.1** | a) Menangani Keselamatan Dalam Perjanjian Pembekal (Addressing Security Within Supplier Agreements)<br><br>b) Semua keperluan keselamatan maklumat yang berkaitan hendaklah ditakrifkan, disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat jabatan.<br><br>c) Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak jabatan selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa.<br><br>d) Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Kerajaan mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang hendaklah dipatuhi adalah seperti yang berikut:<br><br>i) Jabatan hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan;<br>ii) Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan;<br>iii) Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada jabatan berkaitan; | Syarikat Pembekal/ Pemilik Projek |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | iv) Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi;<br>v) Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal;<br>vi) Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses, memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan jabatan dan Lampiran B (Perakuan Akta Rahsia Rasmi 1972 (Akta 88)); dan<br>Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh jabatan. | |

**5.21 Menguruskan Keselamatan Maklumat Dalam Rantaian Bekalan Teknologi Maklumat dan Komunikasi (Managing information security in the information and communication technology (ICT) supply chain)**

**Kawalan:**

Proses dan prosedur hendaklah ditakrifkan dan dilaksanakan untuk mengurus risiko keselamatan maklumat yang berkaitan dengan rantaian bekalan produk dan perkhidmatan ICT.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.21.1** | **Rantaian Bekalan Teknologi Maklumat dan Komunikasi (Information and Communication Technology Supply Chain)**<br>Proses dan prosedur hendaklah ditakrifkan dan dilaksanakan untuk menguruskan risiko keselamatan maklumat yang berkaitan dengan rantaian bekalan produk dan perkhidmatan ICT. Perkara-perkara yang hendaklah diambil kira adalah seperti yang berikut: | Pemilik Projek dan Pembekal |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan;<br>b) Pembekal utama hendaklah memastikan risiko keselamatan maklumat berkaitan dengan produk ICT dan rantaian pembekalan produk ditangani; dan<br>c) Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik. | |

### 5.22 Pemantauan, Semakan dan Pengurusan Perubahan Perkhidmatan Pembekal (Monitoring, Review and Change Management of Supplier Services)

**Kawalan:**
Jabatan hendaklah sentiasa memantau, menyemak, menilai dan mengurus perubahan dalam amalan keselamatan maklumat pembekal dan penyedia perkhidmatan

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.22.1** | **Memantau dan Mengkaji Semula Perkhidmatan Pembekal (Monitoring and Review Supplier Services)**<br>a) Jabatan hendaklah memantau, menyemak, menilai, dan mengurus perubahan dalam amalan keselamatan maklumat pembekal dan penyedia perkhidmatan secara berterusan.<br><br>b) Jabatan hendaklah sentiasa memantau, mengkaji semula, mengaudit perkhidmatan pembekal secara berkala dan mengurus perubahan dalam amalan risiko keselamatan maklumat pembekal dan penyedia perkhidmatan. Perkara-perkara yang hendaklah diambil kira adalah seperti yang berikut: | Pengarah Bahagian, Pembekal dan Pemilik Projek |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | i) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan;<br>ii) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan; dan<br>iii) Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian. | |
| **5.22.2** | **<u>Menguruskan Perubahan Kepada Perkhidmatan Pembekal (Managing Changes to Supplier Services)</u>**<br>Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses jabatan yang terlibat dan penilaian semula risiko. Perkara yang hendaklah diambil kira adalah seperti yang berikut:<br><br>a) Perubahan dalam perjanjian dengan pembekal;<br>b) Perubahan yang dilakukan oleh jabatan bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan<br>c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baharu, perkakasan baharu, perubahan lokasi, pertukaran pembekal dan subkontraktor. | Pengarah Bahagian, Pembekal dan Pemilik Projek |

## 5.23 Keselamatan Maklumat bagi Penggunaan Perkhidmatan Pengkomputeran Awan (Information Security for Use of Cloud Computing Services)

**Kawalan:**

Proses untuk pemerolehan, penggunaan, pengurusan dan penamatan daripada perkhidmatan awan hendaklah diwujudkan mengikut keperluan keselamatan maklumat jabatan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.23.1** | **Keselamatan maklumat bagi penggunaan perkhidmatan pengkomputeran awan (Information Security for Use of Cloud Computing Services)**<br>a) Memastikan pematuhan terhadap keperluan perundangan, peraturan, garis panduan dan perjanjian kontrak berkaitan dengan perkhidmatan pengkomputeran awan yang berkuat kuasa serta pengurusan perkhidmatan yang disediakan oleh pembekal seperti di 5.21 dan 5.22;<br>b) Menentu/mentakrif dan memaklumkan cara/kaedah berkaitan pengurusan risiko bagi perkhidmatan pengkomputeran awan;<br>c) Memastikan keperluan keselamatan maklumat yang berkaitan dengan penggunaan perkhidmatan pengkomputeran awan dilaksanakan; dan<br>d) Melaksanakan kawalan terhadap keperluan langganan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan. | ICTSO/BDPM/Ketua Jabatan/Pengguna |

## 5.24 Perancangan dan Persediaan Pengurusan Insiden Keselamatan Maklumat (Information Security Incident Management Planning and Preparation)

**Kawalan:**

Proses untuk pemerolehan, penggunaan, pengurusan dan penamatan daripada perkhidmatan awan hendaklah diwujudkan mengikut keperluan keselamatan maklumat jabatan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.24.1** | **<u>Tanggungjawab dan Prosedur (Responsibilities and Procedures)</u>**<br>Tanggungjawab dan prosedur pengurusan pengendalian insiden hendaklah diwujudkan untuk memastikan tindakan yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat dengan mentakrif, mewujud dan menyampaikan proses pengurusan insiden keselamatan maklumat, peranan dan tanggungjawab. Pengurusan insiden jabatan hendaklah berdasarkan kepada Prosedur Operasi Standard yang berkuat kuasa. Antara perkara yang hendaklah dilaksanakan adalah seperti yang berikut:<br><br>a) Memberikan kesedaran dan pemahaman berkaitan Prosedur Operasi Standard: Pengurusan dan Pengendalian Insiden Keselamatan Siber CSIRT Jabatan dan hebahan kepada warga jabatan secara berkala; dan<br>b) Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan. | ICTSO, Pengarah Bahagian, CSIRT jabatan,<br>dan Pemilik Projek/Sistem Aplikasi |
| **5.24.2** | **<u>Perancangan dan Persediaan Pengurusan Insiden Keselamatan Maklumat (Information Security Incident Management Planning and Preparation)</u>**<br>a) Menyediakan Pelan Perancangan Pengurusan Insiden Keselamatan Maklumat Jabatan yang merangkumi keperluan latihan, simulasi dan pelaksanaan Security Posture Assessment (SPA).<br>b) Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kerentanan kelemahan keselamatan. | ICTSO / CSIRT jabatan |

### 5.25 Penilaian dan Keputusan mengenai Insiden Keselamatan Maklumat (Assessment of and Decision on Information Security Events)

**Kawalan:**
Jabatan hendaklah menilai insiden keselamatan maklumat dan memutuskan sama ada ia akan dikategorikan sebagai insiden keselamatan maklumat.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.25.1** | **Penilaian dan Keputusan Mengenai Insiden Keselamatan Maklumat (Assessment of and Decision on Information Security Events)**<br>Insiden Keselamatan Maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat. Ia hendaklah direkodkan sebagaimana Prosedur Operasi Standard: Pengurusan dan Pengendalian Insiden Keselamatan Siber Jabatan. | ICTSO, pemilik sistem, pentadbir sistem & CSIRT jabatan |

### 5.26 Tindak Balas Terhadap Insiden Keselamatan Maklumat (Response to Information Security Incidents)

**Kawalan:**
Insiden keselamatan maklumat hendaklah ditangani mengikut prosedur yang didokumenkan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.26.1** | **Tindak Balas Terhadap Insiden Keselamatan Maklumat (Response to Information Security Incidents)**<br>a) Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Operasi Standard: Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam.<br><br>b) Kawalan-kawalan yang hendaklah diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut: | ICTSO, CSIRT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | i) Mengumpul bukti secepat mungkin selepas insiden keselamatan maklumat berlaku;<br>ii) Menjalankan siasatan forensik sekiranya perlu;<br>iii) Menghubungi pihak yang berkenaan dengan secepat mungkin;<br>iv) Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti;<br>v) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;<br>vi) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;<br>vii) Menyediakan tindakan pemulihan segera;<br>viii) Memaklumkan atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu; dan<br>ix) sebaik sahaja insiden itu berjaya ditangani, ia hendaklah ditutup secara rasmi dan direkodkan. | |

## 5.27 Pembelajaran Daripada Insiden Keselamatan Maklumat (Learning from Information Security Incidents)

**Kawalan:**

Pengetahuan yang diperoleh daripada insiden keselamatan maklumat hendaklah digunakan untuk mengukuhkan dan menambah baik kawalan keselamatan maklumat.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.27.1** | **Pembelajaran Daripada Insiden Keselamatan Maklumat (Learning from Information Security Incidents)**<br>a) Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian insiden keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya. | ICTSO, CSIRT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | b) Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.<br><br>c) Maklumat yang diperoleh daripada penilaian insiden keselamatan maklumat hendaklah digunakan untuk:<br><br>i) mempertingkatkan pelan pengurusan insiden termasuk senario dan prosedur insiden:<br>ii) mengenal pasti insiden berulang atau serius dan puncanya untuk mengemas kini penilaian risiko keselamatan maklumat organisasi dan menentukan serta melaksanakan kawalan tambahan yang diperlukan untuk mengurangkan kemungkinan atau akibat kejadian serupa pada masa hadapan. Mekanisme untuk membolehkan itu termasuk mengumpul, mengukur dan memantau maklumat tentang jenis kejadian, volum dan kos; dan<br>iii) tingkatkan kesedaran dan latihan pengguna dengan memberikan contoh tentang perkara yang boleh berlaku, cara bertindak balas terhadap insiden tersebut dan cara pencegahan pada masa hadapan. | |

### 5.28 Pengumpulan Bahan Bukti (Collection of Evidence)

**<u>Kawalan:</u>**

Jabatan hendaklah mewujudkan dan melaksanakan prosedur untuk pengenalpastian, pengumpulan, pemerolehan dan pemeliharaan bukti yang berkaitan dengan insiden keselamatan maklumat.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.28.1** | **<u>Pengumpulan Bahan Bukti (Collection of Evidence)</u>**<br>Jabatan hendaklah menentukan, mewujudkan dan melaksanakan prosedur untuk mengenal pasti pengumpulan, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan. | ICTSO, CSIRT Jabatan |

## 5.29 Keselamatan Maklumat Semasa Gangguan (Information security during disruption)

**<u>Kawalan:</u>**

Jabatan hendaklah merancang bagaimana untuk mengekalkan keselamatan maklumat pada tahap yang sesuai semasa gangguan

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.29.1** | **<u>Keselamatan Maklumat Semasa Gangguan (Information security during disruption)</u>**<br>a) Keselamatan maklumat semasa gangguan merujuk kepada langkah-langkah dan prosedur yang diambil untuk melindungi dan mengekalkan keselamatan maklumat, data, dan sistem komputer semasa terjadi gangguan, bencana, atau insiden yang boleh mengancam integriti dan ketersediaan maklumat. Ini termasuk pelbagai situasi seperti serangan siber, bencana alam, kebakaran, banjir, kecurian, atau insiden teknikal yang tidak diingini.<br><br>b) Berikut adalah beberapa aspek penting berkaitan dengan keselamatan maklumat semasa gangguan:<br><br>i) Pembangunan dan pelaksanaan pelan Perancangan Kesinambungan Perkhidmatan (Business Continuity Planning) untuk memastikan | CDO, ICTSO, dan CSIRT jabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | perkhidmatan atau operasi organisasi berfungsi dengan minimum gangguan ketika terjadi insiden.<br>ii) Pemulihan Bencana (Disaster Recovery) melibatkan pelan dan tindakan untuk memulihkan sistem aplikasi dan data setelah bencana atau insiden yang merosakkan.<br>iii) Perlindungan Data (Data Protection) melibatkan salinan data secara berkala, pengekalan data yang baik, dan pelaksanaan tindakan keselamatan yang sesuai untuk melindungi data yang sensitif.<br>iv) Pencegahan Serangan Siber (Cybersecurity Measures) melibatkan tindakan untuk mencegah serangan siber dan melindungi data dari ancaman siber.<br>v) Pemulihan Sistem Cepat (Quick System Recovery) untuk mengurangkan masa henti ketika terjadi gangguan<br>vi) Kawalan Fizikal (Physical Security) ke bilik server dan peralatan komputer terhad kepada individu yang sah untuk mencegah akses yang tidak diinginkan.<br>vii) Pemulihan Data (Data Recovery) memastikan keupayaan untuk memulihkan data yang hilang atau terjejas dalam insiden.<br>viii) Kesedaran Keselamatan (Security Awareness) di dalam Jabatan untuk mengurangkan ancaman dalaman dan mencegah insiden yang disebabkan oleh kesilapan manusia.<br>ix) Pelan Komunikasi Krisis (Crisis Communication Plan) yang jelas untuk mengurus krisis dan insiden dengan pantas. | |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | c) Keselamatan maklumat semasa gangguan adalah aspek penting dalam perancangan keselamatan dan keselamatan data, yang memastikan organisasi mampu menjaga integriti, kerahsiaan, dan ketersediaan maklumat penting dalam pelbagai situasi yang mengancam. | |

### 5.30 Kesediaan ICT Bagi Kesinambungan Perkhidmatan (ICT Readiness for Business Continuity)

**<u>Kawalan:</u>**
Ketersediaan ICT hendaklah dirancang, dilaksanakan, diselenggara dan diuji berdasarkan objektif kesinambungan perkhidmatan dan keperluan kesinambungan ICT.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.30.1** | **<u>Kesinambungan Keselamatan Maklumat (Information Security Continuity)</u>**<br>a) Kesinambungan keselamatan maklumat hendaklah diterapkan dalam Sistem Pengurusan Kesinambungan Perkhidmatan Jabatan.<br><br>b) Kesediaan ICT hendaklah dirancang, dilaksana, diselenggara dan diuji berdasarkan objektif kesinambungan perkhidmatan dan keperluan kesinambungan perkhidmatan organisasi hendaklah memastikan bahawa:<br><br>i) Struktur organisasi yang mencukupi disediakan untuk menyediakan, mengurangkan dan bertindak balas terhadap gangguan yang disokong oleh kakitangan yang mempunyai tanggungjawab, kuasa dan kecekapan yang diperlukan;<br>ii) Pelan Kesinambungan Perkhidmatan atau Pelan Pemulihan Bencana, | CDO, ICTSO & CSIRT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | termasuk tindak balas dan prosedur pemulihan yang memperincikan bagaimana organisasi merancang untuk menguruskan gangguan perkhidmatan ICT, hendaklah:<br><br>a. kerap dinilai melalui latihan dan ujian; dan<br>b. diluluskan oleh pihak pengurusan;<br><br>iii) Pelan Kesinambungan Perkhidmatan atau Pelan Pemulihan Bencana mempunyai maklumat bagi kesinambungan perkhidmatan seperti berikut:<br><br>a. spesifikasi prestasi dan kapasiti untuk memenuhi keperluan dan objektif kesinambungan perkhidmatan seperti yang dinyatakan dalam Kajian Impak Perkhidmatan (Business Impact Analysis - BIA); dan<br>b. Objektif Masa Pemulihan (RTO) bagi setiap perkhidmatan ICT yang diutamakan dan prosedur untuk memulihkan komponen tersebut.<br>c. Objektif Titik Pemulihan (RPO) sumber ICT hendaklah ditetapkan. | |
| **5.30.2** | **<u>Perancangan Kesinambungan Keselamatan Maklumat (Planning Information Security Continuity)</u>**<br>a) Jabatan hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, Jabatan hendaklah | Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan bencana ICT (ICTSO & CSIRT) |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi Jabatan.<br><br>b) Jabatan juga hendaklah mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang-undang dan peraturan yang terpakai. Perkara yang hendaklah dipertimbangkan adalah seperti berikut:<br><br>i) Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) Jabatan;<br>ii) Menetapkan polisi PKP;<br>iii) Mengenal pasti perkhidmatan kritikal;<br>iv) Melaksanakan Kajian Impak Perkhidmatan (Business Impact Analysis - BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal;<br>v) Membangunkan Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT.<br>vi) Melaksanakan program kesedaran dan latihan pasukan PKP dan Pengguna; dan<br>vii) Melaksanakan simulasi dan penyenggaraan ke atas Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT. | |
| **5.30.3** | **Pelaksanaan Kesinambungan Keselamatan Maklumat (Implementing Information Security Continuity)**<br>Jabatan hendaklah menyedia, mendokumentasi, melaksana dan menyelenggara proses, prosedur | Koordinator PKP<br>Pasukan Tindak balas Kecemasan,<br>Pasukan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang hendaklah dipertimbangkan adalah seperti yang berikut:<br><br>a) Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal jabatan yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini;<br>b) Melaksanakan post-mortem selepas pelaksanaan PKP; dan<br>c) Mengemaskini pelan-pelan PKP jika berlaku sebarang perubahan (organisasi, sumber manusia, teknologi, dan fizikal) yang memberi kesan kepada PKP.<br>d) Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP. | Komunikasi Krisis, Pasukan Pemulihan bencana ICT |
| **5.30.4** | **<u>Menentusah, Mengkaji Semula dan Menilai Kesinambungan Keselamatan Maklumat (Verify, Review and Evaluate Information Security Continuity)</u>**<br>Jabatan hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan secara berkala bagi memastikan ia sah dan berkesan semasa situasi kecemasan. | Pengurusan Atasan jabatan, Koordinator PKP, Pasukan Tindak balas Kecemasan, Pasukan Komunikasi Krisis, Pasukan Pemulihan bencana ICT, Pemilik Perkhidmatan Kritikal jabatan dalam PKP dan warga jabatan |

## 5.31 Keperluan Perundangan dan Kontrak (Legal, Statutory, Regulatory and Contractual Requirements)

**Kawalan:**

Keperluan undang-undang, berkanun, kawal selia dan kontrak yang berkaitan dengan keselamatan maklumat dan pendekatan organisasi untuk memenuhi keperluan ini hendaklah dikenal pasti, didokumenkan dan sentiasa dikemas kini.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.31.1** | **Pematuhan Terhadap Keperluan Perundangan dan Kontrak (Compliance with Legal and Contructual Requirements)**<br>Meningkat dan memantapkan tahap keselamatan siber bagi mengelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat dengan menyediakan *Non-disclosure Agreement* (NDA) mengikut keperluan projek dan menguatkuasakan Perakuan Akta Rahsia Rasmi 1972 (Akta 88). | Pengguna, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan |
| **5.31.2** | **Pengenalpastian Keperluan Undang-Undang dan Kontrak Yang Terpakai (Identification of Applicable Legislation and Contractual Agreement)**<br>Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga jabatan, pengguna, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di jabatan dan pembekal seperti Lampiran A. | pengguna<br>Warga agensi, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan |
| **5.31.3** | **Peraturan Kawalan Kriptografi (Regulation of Cryptographic Controls)Peranan**<br>Kriptografi ialah bidang yang mempunyai keperluan undang-undang khusus. Pematuhan kepada perjanjian, undang-undang dan peraturan yang berkaitan yang berkaitan dengan perkara berikut hendaklah diambil kira: | Warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | a) sekatan ke atas import atau eksport perkakasan dan perisian komputer untuk melaksanakan fungsi kriptografi;<br>b) sekatan ke atas import atau eksport perkakasan dan perisian komputer yang direka bentuk untuk menambah fungsi kriptografi;<br>c) sekatan ke atas penggunaan kriptografi;<br>d) kaedah mandatori atau budi bicara akses oleh pihak berkuasa negara kepada maklumat yang disulitkan; dan<br>e) kesahihan tandatangan digital, meterai dan sijil. | |

### 5.32 Hak Harta Intelek (Intellectual Property Rights)

**<u>Kawalan:</u>**
Organisasi hendaklah melaksanakan prosedur yang sesuai untuk melindungi hak harta intelek.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.32.1** | **<u>Hak Harta Intelek (Intellectual Property Rights)</u>**<br>Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan pelesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan. | Warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan |

### 5.33 Perlindungan Rekod (Protection of Records)

**<u>Kawalan:</u>**
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa kebenaran dan pelepasan tanpa kebenaran.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.33.1** | **<u>Perlindungan Rekod (Protection of Records)</u>**<br>Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa izin dan | pengguna<br>Warga jabatan, pembekal, pakar |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak. | runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan |

### 5.34 Privasi dan Perlindungan Peribadi yang boleh dikenal pasti (Privacy and protection of personal identifiable information (PII))

**Kawalan:**

Organisasi hendaklah mengenal pasti dan memenuhi keperluan berkenaan pemeliharaan privasi dan perlindungan maklumat peribadi (PII) mengikut undang-undang dan peraturan serta keperluan kontrak yang berkenaan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.34.1** | **Privasi dan Perlindungan Maklumat Peribadi (Privacy and Protection of Personally Identifiable Information)**<br>a) Maklumat peribadi yang boleh dikenalpasti merujuk kepada data yang boleh digunakan untuk mengenalpasti individu seperti nombor kad pengenalan, rekod perubatan dan lain-lain.<br>b) Jika terdapat keperluan terhadap pengenalan tersebut hendaklah terlebih dahulu mendapat persetujuan daripada individu berkenaan.<br>c) Jabatan hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti termaktub di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia. | Warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan |

### 5.35 Kajian Semula Keselamatan Maklumat Secara Berkecuali (Independent Review of Information Security)

**Kawalan:**

Pendekatan jabatan untuk mengurus keselamatan maklumat dan pelaksanaannya termasuk orang, proses dan teknologi hendaklah disemak oleh pihak ketiga (secara

berkecuali) pada selang masa yang dirancang, atau apabila perubahan ketara berlaku.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.35.1** | **Kajian Semula Keselamatan Maklumat Secara Berkecuali (Independent Review of Information Security)**<br>Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur. | Pengarah Bahagian dan Pemilik Perkhidmatan |

## 5.36 Pematuhan Polisi, Peraturan dan Piawaian Untuk Keselamatan Maklumat (Compliance With Policies, Rules and Standards for Information Security)

**Kawalan:**

Pematuhan kepada polisi keselamatan maklumat, polisi khusus, peraturan dan piawaian organisasi hendaklah sentiasa disemak.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **5.36.1** | **Pematuhan Polisi dan Standard Keselamatan (Compliance with Security Policies and Standards)**<br>Jabatan hendaklah membuat kajian semula secara berkala terhadap pematuhan polisi dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian. | Pengarah Bahagian dan Pemilik Perkhidmatan |
| **5.36.2** | **Kajian Semula Pematuhan Teknikal (Technical Compliance Review)**<br>JWP hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan keselamatan maklumat. | Pengarah Bahagian dan Pemilik Perkhidmatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| 5.36.3 | **<u>Memastikan semua polisi, peraturan, akta kawalan keselamatan maklumat dipatuhi dan dilaksana oleh semua peringkat proses perkhidmatan</u>**<br><br>Pemantauan audit dalaman dilaksanakan sekali dalam tempoh 12 bulan bagi memastikan semua bahagian mematuhi polisi, prosedur, peraturan dan undang-undang keselamatan maklumat yang telah dikuatkuasakan. | CDO/ICTSO/Ketua Jabatan/Ketua Bahagian |

## 5.37 Dokumentasi Prosedur Operasi yang Didokumenkan (Documented Operating Procedures)

**<u>Kawalan:</u>**
Prosedur pengendalian untuk kemudahan pemprosesan maklumat hendaklah didokumenkan dan disediakan kepada kakitangan yang memerlukannya.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| 5.37.1 | **<u>Dokumentasi Prosedur Operasi (Documented Operating Procedures)</u>**<br>Penyedia dokumen hendaklah memastikan prosedur operasi yang didokumenkan dan disediakan kepada kakitangan yang memerlukannya sahaja serta mematuhi perkara-perkara berikut:<br><br>a) semua prosedur keselamatan maklumat yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal;<br>b) setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan | Pengarah Bahagian dan Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | c) semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan. | |

# 6.0 KAWALAN SUMBER MANUSIA (PEOPLE CONTROL)

## 6.1 Tapisan Keselamatan (Security Screening)

**Kawalan:**

Semakan pengesahan latar belakang ke atas semua calon untuk menjadi kakitangan hendaklah dijalankan sebelum dilantik dan secara berterusan dengan mengambil kira undang-undang, peraturan dan etika yang terpakai dan selaras dengan keperluan jabatan, klasifikasi maklumat yang akan diakses dan risiko yang dijangkakan.

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

## 6.2 Terma dan Syarat Perkhidmatan (Terms and Conditions of Employment)

**Kawalan:**

Perjanjian kontrak pekerjaan hendaklah menyatakan tanggungjawab kakitangan dan jabatan terhadap keselamatan maklumat.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| 6.2.1 | **<u>Terma dan Syarat Perkhidmatan (Terms and Conditions of Employment)</u>**<br>Persetujuan mengikat perjanjian dengan warga, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab jabatan terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut:<br>i) menyatakan dengan lengkap dan jelas peranan serta tanggung jawab warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan yang terlibat dalam menjamin keselamatan aset ICT; dan<br>ii) mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan. | Warga, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT |
| 6.2.2 | **<u>Dalam Tempoh Perkhidmatan (During Deployment)</u>**<br>Memastikan warga Jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan mematuhi tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa. | Warga Jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Jabatan |

### 6.3 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat (Information Security Awareness, Education and Training)

**<u>Kawalan:</u>**

Warga Jabatan dan pihak berkepentingan lain yang berkaitan hendaklah menerima kesedaran, pendidikan dan latihan kawalan keselamatan maklumat yang sesuai serta kemaskini berkala polisi kawalan keselamatan maklumat, dasar dan prosedur khusus jabatan yang berkaitan dengan fungsi tugas mereka.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **6.3.1** | **<u>Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat (Information Security Awareness, Education and Training)</u>**<br>Warga, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan hendaklah diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai kawalan keselamatan maklumat secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang hendaklah dipatuhi adalah seperti yang berikut:<br><br>a) memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Kawalan Keselamatan Maklumat JWP, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka;<br>b) memastikan kesedaran yang berkaitan Polisi Kawalan Keselamatan Maklumat JWP hendaklah diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan<br>c) memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat. | Warga, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT |

### 6.4 Proses Tatatertib (Disciplinary Process)

**<u>Kawalan:</u>**
Proses tatatertib hendaklah diformalkan dan dimaklumkan untuk mengambil tindakan terhadap kakitangan dan pihak berkepentingan lain yang berkaitan yang telah melakukan pelanggaran polisi kawalan keselamatan maklumat.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **6.4.1** | **<u>Proses Tatatertib (Disciplinary Process)</u>**<br>Proses tatatertib yang formal dan disampaikan kepada warga jabatan/pihak berkepentingan terlibat yang lain hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga jabatan/pihak berkepentingan terlibat yang lain yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>a) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga jabatan/pihak berkepentingan terlibat yang lain sekiranya berlaku pelanggaran terhadap perundangan dan peraturan yang ditetapkan oleh jabatan; dan<br>b) Warga jabatan/pihak berkepentingan terlibat yang lain yang melanggar polisi ini akan dikenakan tindakan tatatertib atau digantung daripada mendapat capaian kepada kemudahan ICT jabatan. | Unit Integriti |

## 6.5 Tanggungjawab selepas Penamatan atau Pertukaran Pekerjaan (Responsibilities after Termination or Change of Employment)

**<u>Kawalan:</u>**
Tanggungjawab dan tugas keselamatan maklumat yang kekal sah selepas penamatan atau pertukaran jawatan hendaklah ditakrifkan, dikuatkuasakan dan dimaklumkan kepada kakitangan yang berkaitan dan pihak lain yang berkepentingan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **6.5.1** | **<u>Penamatan atau Pertukaran Tanggung Jawab Perkhidmatan (Termination or Change of Employment Responsibilities)</u>**<br><br>a) Warga jabatan yang telah tamat perkhidmatan hendaklah mematuhi perkara-perkara berikut: | BKP dan warga jabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | i) Memastikan semua kemudahan ICT dikembalikan kepada jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan<br>ii) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan jabatan dan/atau terma perkhidmatan yang ditetapkan.<br>iii) Maklumat rasmi dalam peranti tidak dibenarkan dibawa keluar dari jabatan.<br><br>b) Warga jabatan yang telah bertukar perkhidmatan hendaklah:<br><br>i) memastikan semua aset ICT yang berkaitan dengan tugas terdahulu dikembalikan kepada jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan<br>ii) menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan.<br>iii) Maklumat rasmi dalam peranti tidak dibenarkan dibawa keluar dari jabatan kecuali dengan kelulusan Pengarah Bahagian atau pemilik maklumat. | |

**6.6 Perjanjian Kerahsiaan atau Ketakdedahan (Confidentiality Or Non-Disclosure Agreements)**

**Kawalan:**

Perjanjian kerahsiaan atau *Non-Disclosure Agreements (NDA)* menunjukkan keperluan organisasi untuk perlindungan maklumat hendaklah dikenal pasti, didokumenkan, disemak secara berkala dan ditandatangani oleh kakitangan dan pihak yang berkepentingan lain yang berkaitan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **6.6.1** | **<u>Perjanjian Kerahsiaan atau Ketakdedahan (Confidentiality Or Non-Disclosure Agreements)</u>**<br>a) Syarat-syarat perjanjian kerahsiaan atau non-disclosure perlu mengambil kira keperluan organisasi dan hendaklah dikenal pasti, didokumentasi, disemak secara berkala dan ditandatangani oleh wakil JWP dan pihak berkepentingan terlibat yang lain.<br>b) Pihak berkepentingan hendaklah bersetuju dan mematuhi semua keperluan kawalan keselamatan maklumat yang berkuatkuasa dan relevan. | ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT, Pengguna dan Pembekal |

**6.7 Bekerja Jarak Jauh (Remote working)**

**<u>Kawalan:</u>**
Langkah keselamatan hendaklah dilaksanakan apabila kakitangan bekerja dari jarak jauh untuk melindungi maklumat yang diakses, diproses atau disimpan di luar premis organisasi.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **6.7.1** | **<u>Bekerja Jarak Jauh (Remote working)</u>**<br>a) Langkah-langkah kawalan keselamatan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di luar premis jabatan apabila warga agensi/pihak berkepentingan yang bekerja secara jarak jauh (remote working).<br><br>b) Warga Jabatan yang bekerja jarak jauh hendaklah:<br><br>i) memastikan kawalan keselamatan maklumat jabatan dipatuhi dan tidak disebarkan kepada pihak ketiga; dan<br>ii) memastikan arahan bekerja dari luar dipatuhi mengikut garis panduan yang ditetapkan. | Warga JWP |

## 6.8 Pelaporan Keselamatan Maklumat (Reporting Information Security Events)

**Kawalan:**

Organisasi hendaklah menyediakan mekanisme untuk kakitangan melaporkan insiden keselamatan maklumat yang dijangka atau disyaki melalui saluran yang sesuai tepat pada masanya.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **6.8.1** | **Pelaporan Keselamatan Maklumat (Reporting Information Security Events)**<br>a) Insiden keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT jabatan. CSIRT jabatan kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:<br><br>i) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa;<br>ii) Maklumat disyaki hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa;<br>iii) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;<br>iv) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan;<br>v) Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan; Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar;<br>vi) Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak dijangka;<br>vii) kesilapan manusia; | ICTSO, Pengarah Bahagian dan CERT jabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | viii) ketidakpatuhan polisi kawalan keselamatan maklumat, dasar khusus atau piawaian yang berkenaan;<br>ix) pelanggaran langkah keselamatan fizikal;<br>x) perubahan sistem yang belum melalui proses pengurusan perubahan; dan<br>xi) disyaki jangkitan malware.<br><br>b) Prosedur pelaporan insiden keselamatan siber berdasarkan:<br><br>i) Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022; dan<br>ii) Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan Siber CSIRT agensi. | |
| **6.8.2** | **<u>Pelaporan Kelemahan Keselamatan Maklumat (Reporting Security Weakness)</u>**<br>Warga JWP/pihak berkepentingan terlibat yang lain yang menggunakan sistem dan maklumat agensi dikehendaki mengambil maklum dan melaporkan sebarang insiden atau kelemahan keselamatan maklumat melalui saluran pelaporan yang betul dengan kadar segera. | Pengguna, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan jabatan |

# 7.0 KAWALAN FIZIKAL (PHYSICAL CONTROL)

## 7.1 Perimeter Keselamatan Fizikal (Physical Security Perimeter)

**Kawalan:**

Perimeter keselamatan fizikal hendaklah ditakrifkan dan digunakan untuk melindungi kawasan yang mengandungi maklumat dan aset lain yang berkaitan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.1.1** | **Perimeter Keselamatan Fizikal (Physical Security Perimeter)**<br>Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap premis dan aset ICT Jabatan.<br>Perimeter keselamatan fizikal digunakan untuk melindungi aset, individu, dan persekitaran fizikal dari ancaman, bahaya, atau kemungkinan kerosakan. Ia melibatkan pelbagai strategi dan tindakan untuk memastikan keselamatan dalam ruang fizikal seperti bangunan, lokasi jabatan, infrastruktur, atau kawasan/tempat penting lain. Perkara-perkara yang hendaklah dipatuhi termasuk yang berikut:<br><br>a) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat;<br>b) Melindungi kawasan terperingkat melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;<br>c) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;<br>d) Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, gangguan/ancaman manusia dan sebarang bencana alam; | Pegawai Keselamatan Jabatan, BKP |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | e) Menyediakan garis panduan perlindungan fizikal untuk kakitangan yang bekerja di dalam kawasan terperingkat;<br>f) Memastikan kawasan-kawasan penghantaran, pemunggahan dan tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya;<br>g) Memasang kamera litar tertutup (CCTV) dan alat penggera penceroboh; dan<br>h) semua cadangan pembinaan, pengubahsuaian, penyewaan, pembangunan dan penaiktarafan hendaklah mendapat khidmat nasihat Ketua Pengarah Keselamatan Kerajaan (Arahan Keselamatan (Semakan dan Pindaan 2017)) | |

### 7.2 Kemasukan Fizikal (Physical Entry)

**Kawalan:**

Kawasan selamat hendaklah dilindungi oleh kawalan kemasukan dan pintu akses yang sesuai.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.2.1** | **Kawalan Kemasukan Fizikal (Physical Entry Controls)**<br>Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis jabatan. Perkara yang hendaklah dipatuhi adalah seperti yang berikut:<br><br>a) Setiap pegawai dan kakitangan jabatan hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada jabatan apabila bertukar, tamat perkhidmatan atau bersara;<br>b) Setiap pelawat hendaklah mendaftar, mendapatkan pas keselamatan pelawat di kaunter Keselamatan serta mempamerkan pas keselamatan sepanjang berada di premis | Penyelaras: BKP.<br>Warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan Jabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | kerajaan dan hendaklah dikembalikan selepas tamat lawatan;<br>c) Hanya pengguna yang telah diberi kebenaran sahaja boleh menggunakan aset ICT Jabatan;<br>d) Kehilangan pas keselamatan hendaklah dilaporkan segera kepada Pihak Berkuasa.<br>e) Setiap pegawai dan kakitangan Jabatan yang hadir bertugas di luar waktu pejabat hendaklah memohon kebenaran kemasukan ke premis Jabatan sebelum dan melaporkan diri di kaunter keselamatan/pelawat bagi tujuan rekod kehadiran; dan<br>f) Setiap pelawat hendaklah mendaftar kehadiran dalam buku atau sistem pelawat di kaunter keselamatan/pelawat. | |
| **7.2.2** | **<u>Kawasan Penyerahan dan Pemunggahan (Delivery and Loading Areas)</u>**<br>Jabatan hendaklah memastikan lokasi/pintu kemasukan (access point) seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah diasingkan daripada pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan. | BKP |

## 7.3 Keselamatan Pejabat, Bilik dan Kemudahan (Securing Offices, Rooms and Facilities)

**<u>Kawalan:</u>**
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah direka bentuk dan dilaksanakan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.3.1** | **<u>Keselamatan Pejabat, Bilik dan Kemudahan (Securing Office, Rooms and Facilities)</u>**<br>Ini bertujuan untuk menghalang akses tanpa kebenaran, gangguan secara fizikal dan kerosakan terhadap pejabat, bilik dan kemudahan. Perkara | BKP,<br>Warga Jabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | yang hendaklah dipatuhi adalah seperti yang berikut:<br><br>a) Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data hendaklah dihadkan daripada diakses tanpa kebenaran;<br>b) Kawasan tempat bekerja, bilik dan tempat operasi ICT hendaklah dihadkan daripada diakses oleh orang luar; dan<br>c) Petunjuk lokasi bilik operasi dan tempat larangan hendaklah mematuhi arahan keselamatan. | |

## 7.4 Pemantauan keselamatan fizikal (physical security monitoring)

**Kawalan:**
Premis hendaklah dipantau secara berterusan untuk akses fizikal yang tidak dibenarkan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.4.1** | **Pemantauan keselamatan fizikal (physical security monitoring)**<br>a) Premis fizikal hendaklah dipantau secara berterusan oleh sistem pengawasan termasuk pengawal, penggera pencerobohan, sistem pemantauan video seperti kamera litar tertutup (CCTV) dan perisian pengurusan maklumat keselamatan fizikal sama ada diurus secara dalaman atau oleh penyedia perkhidmatan pemantauan.<br><br>b) Sistem pemantauan hendaklah dilindungi daripada capaian yang tidak dibenarkan untuk mengelakkan maklumat pengawasan, seperti suapan video, daripada diakses oleh orang yang tidak dibenarkan atau sistem dilumpuhkan dari jarak jauh. | BKP |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | c) Perkara-perkara yang hendaklah dipatuhi adalah dengan memasang CCTV untuk memantau dan merakam akses ke kawasan sensitif di dalam dan di luar premis Jabatan. | |

## 7.5 Perlindungan Daripada Ancaman Fizikal Dan Persekitaran (Protecting Against Physical and Environmental Threats)

**Kawalan:**
Perlindungan terhadap ancaman fizikal dan alam sekitar, seperti bencana alam dan ancaman fizikal lain yang disengajakan atau tidak disengajakan kepada infrastruktur hendaklah direka bentuk dan dilaksanakan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.5.1** | **Perlindungan Daripada Ancaman Fizikal Dan Persekitaran (Protecting Against Physical and Environmental Threats)**<br>Jabatan hendaklah mereka bentuk dan melaksanakan perlindungan fizikal daripada sebarang ancaman seperti kebakaran, banjir, letupan, gangguan perbuatan manusia, bencana, binatang dan serangga perosak. | Penyelaras: BKP.<br>Pentadbir Pusat Data dan pegawai keselamatan Jabatan |

## 7.6 Bekerja di Kawasan Selamat (Working In Secure Areas)

**Kawalan:**
Langkah keselamatan untuk bekerja di kawasan selamat hendaklah direka bentuk dan dilaksanakan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.6.1** | **Bekerja di Kawasan Selamat (Working in Secure Area)**<br>a) Langkah-langkah kawalan keselamatan bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada warga jabatan yang tertentu sahaja. Ini dilakukan untuk | Pentadbir Pusat Data dan BKP |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | melindungi aset ICT yang terdapat dalam premis jabatan termasuklah Pusat Data.<br><br>b) Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencana alam. Langkah-langkah kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut:<br><br>i) Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran;<br>ii) Akses adalah terhad kepada warga jabatan yang telah diberi kuasa sahaja dan dipantau pada setiap masa;<br>iii) Pemantauan dibuat menggunakan (CCTV) kamera atau lain-lain peralatan yang sesuai;<br>iv) CCTV dan log akses hendaklah diperiksa secara berjadual;<br>v) Butiran pelawat yang keluar masuk ke kawasan larangan hendaklah direkodkan;<br>vi) Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan;<br>vii) Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam;<br>viii) Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan;<br>ix) Memperkukuh dinding dan siling; dan<br>x) Mengehadkan pintu keluar masuk. | |

## 7.7 Meja Kosong dan Skrin Kosong (Clear Desk and Clear Screen)

**Kawalan:**

Peraturan meja yang kosong untuk kertas dan media storan boleh alih dan peraturan skrin yang kosong untuk kemudahan pemprosesan maklumat hendaklah ditakrifkan dan dikuatkuasakan dengan sewajarnya

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.7.1** | **Dasar Meja Kosong dan Skrin Kosong (Policy Clear Desk dan Clear Screen)**<br>*Clear Desk* bermaksud tidak meninggalkan dan mendedahkan bahan-bahan yang sensitif sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Langkah-langkah yang perlu diambil termasuk seperti yang berikut:<br>a) Simpan dokumen sensitif di dalam laci berkunci atau kabinet apabila tidak digunakan.<br>b) Pastikan meja kerja kosong daripada kertas, fail atau peranti mudah alih yang mengandungi maklumat terperingkat apabila meninggalkan tempat kerja.<br>c) Kunci komputer (Lock Screen) apabila meninggalkan meja walaupun untuk tempoh singkat.<br>d) Elakkan menampal kata laluan atau maklumat sulit di nota pelekat pada skrin, papan kekunci atau meja.<br>e) Gunakan mesin pencetak dengan fungsi keselamatan (contoh: secure print) untuk mengelakkan dokumen ditinggalkan tanpa dipantau.<br>f) Koyak atau lupuskan dokumen yang tidak diperlukan menggunakan mesin pencincang kertas (shredder).<br>g) Elakkan pendedahan skrin komputer kepada orang yang tidak berkenaan (gunakan privacy screen jika perlu).<br>h) Pastikan peranti storan mudah alih (USB, external drive) disimpan dengan selamat selepas digunakan. | Warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT agensi |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.7.2** | **<u>Peralatan Pengguna Tanpa Kawalan (Unattended User Equipment)</u>**<br>Pengguna hendaklah memastikan peralatan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna hendaklah memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:<br><br>a) Tamatkan sesi aktif apabila selesai tugas;<br>b) *Log-off* komputer peribadi, komputer riba dan pelayan apabila sesi bertugas selesai; dan<br>c) Komputer peribadi, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan. | Warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan |

### 7.8 Penempatan dan Perlindungan Peralatan ICT (Equipment Siting and Protection)

**<u>Kawalan:</u>**
Peralatan hendaklah diletakkan dengan selamat dan dilindungi.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.8.1** | **<u>Penempatan dan Perlindungan Peralatan ICT (Equipment Sitting and Protection)</u>**<br>a) Peralatan ICT hendaklah ditentukan tempatnya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran dan peluang kemasukan yang tidak dibenarkan.<br><br>b) Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut:<br><br>i) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;<br>ii) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran pengguna | Warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | perkakasan dan konfigurasi yang telah ditetapkan;<br>iii) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;<br>iv) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem;<br>v) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (activated) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;<br>vi) Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubah suai tanpa kebenaran dan salah guna;<br>vii) Setiap pengguna adalah bertanggungjawab atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;<br>viii) Peralatan-peralatan kritikal perlu disokong oleh Uninterruptable Power Supply (UPS) dan Generator Set (Gen-Set);<br>ix) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;<br>x) Peralatan rangkaian seperti suis, penghala, hab dan peralatan-peralatan lain perlu diletakkan di dalam rak khas dalam bilik berkunci;<br>xi) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai; | |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | xii) Peralatan ICT yang hendak dibawa ke luar premis jabatan, perlulah mendapat kelulusan Pegawai Aset dan direkodkan bagi tujuan pemantauan;<br>xiii) Peralatan ICT yang hilang semasa di luar waktu pejabat hendaklah dikendalikan mengikut prosedur pelaporan insiden;<br>xiv) Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;<br>xv) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal komputer tersebut ditempatkan tanpa kebenaran Bahagian Digital dan Pengurusan Maklumat;<br>xvi) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Bahagian Digital dan Pengurusan Maklumat melalui Sistem Helpdesk JWP untuk dibaik pulih;<br>xvii) Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;<br>xviii) Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal;<br>xix) Pengguna dilarang sama sekali mengubah password *administrator* yang telah ditetapkan oleh Bahagian Digital dan Pengurusan Maklumat; dan<br>xx) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi dan jabatan sahaja. | |

## 7.9 Keselamatan Aset di Luar Premis (Security of Assets Off-Premises)

**Kawalan:**
Aset yang berada di luar pejabat hendaklah dilindungi.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.9.1** | **Keselamatan Aset di Luar Premis (Security of Equipment Off-Premises)**<br>Keselamatan aset di luar premis hendaklah dilindungi dengan mengambil kira pelbagai risiko bekerja di luar premis jabatan. Peralatan yang dibawa keluar dari premis jabatan adalah terdedah kepada pelbagai risiko. Perkara yang hendaklah dipatuhi adalah seperti yang berikut:<br><br>a) Peralatan perlu dilindungi dan dikawal sepanjang masa;<br>b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan<br>c) Keselamatan peralatan yang dibawa keluar adalah di bawah tanggungjawab pegawai yang berkenaan. | Warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan |

## 7.10 Media storan (Storage Media)

**Kawalan:**
Media storan hendaklah diuruskan melalui kitaran hayat pemerolehan, penggunaan, pengangkutan dan pelupusan mengikut skim klasifikasi organisasi dan keperluan pengendalian

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.10.1** | **Pengurusan Media Boleh Alih (Management of Removal Media)**<br>a) Untuk mengelakkan kerosakan pada aset dan gangguan kepada aktiviti perkhidmatan, media hendaklah dikawal dan dilindungi secara fizikal. Pemacu media boleh alih harus dibolehkan jika terdapat keperluan untuk berbuat demikian. Media boleh alih mesti dikendalikan mengikut klasifikasi maklumat. | Pentadbir Sistem ICT dan Pengguna |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | b) Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut:<br><br>i) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;<br>ii) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja;<br>iii) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja;<br>iv) Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan<br>v) Menyimpan semua jenis media di tempat yang selamat. | |
| **7.10.2** | **<u>Pelupusan Media (Disposal of Media)</u>**<br>a) Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Kerajaan.<br><br>b) Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa. | Pentadbir Sistem ICT dan Jawatankuasa yang dilantik untuk pelupusan aset. |
| **7.10.3** | **<u>Pengalihan Aset (Removal of Assets)</u>**<br>Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Langkah-langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:<br>a) Peralatan ICT yang hendak dibawa keluar dari premis jabatan untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Jabatan atau pegawai yang diturunkan kuasa dan | Pengguna, Pegawai Aset |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan; dan<br>b) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan. | |
| **7.10.4** | **<u>Pengendalian Media (Media Handling)</u>**<br>Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan. | Pentadbir Sistem ICT dan Pengguna (BTM / Pegawai Aset) |

### 7.11 Utiliti Sokongan (Supporting Utilities)

**<u>Kawalan:</u>**
Kemudahan pemprosesan maklumat hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.11.1** | **<u>Utiliti Sokongan (Supporting Utilities)</u>**<br>Peralatan ICT khususnya di Pusat Data hendaklah dilindungi daripada kegagalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan. Semua alat sokongan perlu diselenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali). | BKP |

### 7.12 Keselamatan Kabel (Cabling Security)

**<u>Kawalan:</u>**
Kabel yang membawa kuasa, data atau perkhidmatan maklumat sokongan hendaklah dilindungi daripada pemintasan, gangguan atau kerosakan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.12.1** | **<u>Keselamatan Kabel (Cabling Security)</u>**<br>a) Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi | Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | daripada pintasan, gangguan atau kerosakan.<br><br>b) Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi.<br><br>c) Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut:<br><br>i) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;<br>ii) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan;<br>iii) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan<br>iv) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat. | |

## 7.13 Penyelenggaraan Peralatan (Equipment Maintenance)

**Kawalan:**

Peralatan hendaklah diselenggara dengan betul untuk memastikan ketersediaan, integriti dan kerahsiaan maklumat.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.13.1** | **Penyelenggaraan Peralatan (Equipment Maintenance)**<br>Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan ketersediaan dan keutuhannya berterusan. Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Langkah- | Pegawai Aset, Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | langkah keselamatan yang perlu diambil termasuklah seperti yang berikut:<br><br>a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau selepas tamat tempoh jaminan;<br>b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara;<br>c) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja;<br>d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan<br>e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan. | |

### 7.14 Pelupusan yang Selamat atau Penggunaan Semula Peralatan (Secure Disposal or Re-Use of Equipment)

**Kawalan:**
Semua peralatan yang mengandungi media storan hendaklah disahkan untuk memastikan bahawa semua data sensitif dan perisian berlesen telah dipadam sepenuhnya atau ditulis ganti dengan selamat sebelum dilupuskan atau digunakan semula.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **7.14.1** | **Pelupusan yang Selamat atau Penggunaan Semula Peralatan (Secure Disposal or Re-Use of Equipment**<br>a) Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (overwrite) sebelum dilupuskan atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan | Pegawai Aset, Pentadbir Sistem ICT dan warga agensi |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh jabatan dan ditempatkan di jabatan.<br><br>b) Peralatan ICT yang hendak dilupuskan hendaklah mematuhi prosedur pelupusan yang berkuat kuasa. Pelupusan hendaklah dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan jabatan. Langkah-langkah seperti yang berikut hendaklah diambil:<br><br>i) Bagi peralatan ICT yang akan dilupuskan sebelum dipindah-milik, data-data dalam storan hendaklah dipastikan telah dihapuskan dengan cara yang selamat;<br>ii) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;<br>iii) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;<br>iv) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;<br><br>v) Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti yang berikut:<br><br>a. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi.<br>b. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, | |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | Hardisk, Motherboard dan sebagainya.<br>c. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di agensi.<br>d. Memindah keluar dari pejabat bagi mana-mana peralatan ICT yang hendak dilupuskan; dan<br>e. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab jabatan.<br><br>vi) Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti *external hardisk* atau *thumbdrive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.<br>vii) Data dan maklumat dalam aset ICT yang akan dipindah milik atau dilupuskan hendaklah dihapuskan secara kekal;<br>viii) Sekiranya maklumat perlu disimpan, maka pengguna boleh membuat salinan;<br>ix) Maklumat lanjut berhubung pelupusan bolehlah dirujuk pada pekeliling berkaitan Tatacara Pengurusan Aset Alih Kerajaan (TPA) yang berkuat kuasa;<br>x) Pelupusan dokumen-dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; dan | |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | xi) Pegawai aset bertanggungjawab merekod butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pemantauan Pengurusan Aset – SPPA. | |

# 8.0 KAWALAN TEKNOLOGI (TECHNOLOGICAL CONTROL)

## 8.1 Peranti Titik Hujung Pengguna (User Endpoint Devices)

**Kawalan:**

Maklumat yang disimpan pada, diproses oleh atau boleh diakses melalui peranti *endpoint* merangkumi Tablet, Komputer Riba, Komputer Peribadi pengguna hendaklah dilindungi.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.1.1** | **Polisi Peranti *Endpoint* (Mobile Device Policy)**<br>Polisi dan langkah-langkah keselamatan sokongan hendaklah digunakan bagi mengurus risiko yang timbul melalui penggunaan peranti ***Endpoint***.<br><br>**a) Peranan: Sokongan Teknikal**<br>Membangun serta menyebarkan dasar dan langkah-langkah keselamatan sokongan bagi mengurus risiko yang timbul melalui penggunaan peranti *endpoint* merangkumi perkara berikut:<br><br>i) jenis dan tahap pengelasan maklumat yang dibenarkan untuk dikendalikan, diproses dan disimpan atau disokong menggunakan peranti *endpoint*;<br>ii) peraturan untuk sambungan kepada perkhidmatan maklumat, rangkaian awam atau mana-mana rangkaian lain di luar premis;<br>iii) penyulitan peranti storan;<br>iv) perlindungan terhadap malware;<br>v) membatalkan keupayaan capaian jarak jauh (remote disabling), pemadaman dan sekatan (lockout);<br>vi) sandaran (back up);<br>vii) penggunaan perkhidmatan web dan aplikasi web;<br>viii) analisis tingkah laku pengguna akhir;<br>ix) penggunaan perkhidmatan boleh alih, termasuk peranti memori boleh alih, dan kemungkinan membatalkan keupayaan port fizikal; | Pengguna |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | x) penggunaan keupayaan pembahagian, jika disokong oleh peranti *endpoint*, yang boleh memisahkan maklumat organisasi dan aset berkaitan lain daripada maklumat lain dan aset berkaitan pada peranti dengan selamat.<br><br>**b) Peranan: Warga**<br>Perkara-perkara yang hendaklah dipatuhi:<br><br>i) pendaftaran ke atas peranti endpoint;<br>ii) keperluan ke atas perlindungan secara fizikal;<br>iii) kawalan ke atas pemasangan perisian peranti endpoint;<br>iv) kawalan ke atas versi dan patches perisian;<br>v) sekatan ke atas akses perkhidmatan maklumat secara dalam talian;<br>vi) kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi; dan<br>vii) peranti endpoint hendaklah disimpan di tempat yang selamat apabila tidak digunakan. | |
| **8.1.2** | **<u>Peralatan Pengguna Tanpa Kawalan (Unattended User Equipment)</u>**<br>Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut:<br><br>a) Tamatkan sesi aktif apabila selesai tugas;<br>b) *Log-off* atau *Locked Screen* komputer peribadi, komputer riba dan pelayan apabila sesi bertugas selesai; dan | Warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICTjabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | c) Komputer peribadi, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan. | |
| **8.1.3** | Pengguna adalah bertanggungjawab melindungi maklumat yang disimpan pada peranti pengguna, terdapat beberapa langkah yang boleh diambil seperti:<br><br>a) **Menggunakan kata laluan yang kukuh:** Kata laluan yang kukuh boleh membantu melindungi maklumat daripada capaian tanpa kebenaran. Pastikan kata laluan anda mengandungi huruf besar dan kecil, nombor dan simbol.<br><br>b) **Mengaktifkan pengesahan dua faktor:** Pengesahan dua faktor adalah satu lagi lapisan keselamatan yang boleh membantu melindungi maklumat daripada akses tanpa kebenaran. Apabila pengesahan dua faktor diaktifkan, pengguna perlu memasukkan kod pengesahan tambahan selain daripada kata laluan untuk mengakses akaun.<br><br>c) **Menggunakan perisian antivirus:** Perisian antivirus boleh membantu melindungi peranti endpoint daripada serangan virus dan malware.<br><br>d) **Mengemas kini sistem operasi:** Mengemas kini sistem operasi secara berkala boleh membantu memastikan peranti endpoint dilindungi daripada kelemahan keselamatan terkini. | Pengguna |

## 8.2 Hak Akses Istimewa (Privileged Access Rights)

**Kawalan:**
Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan diuruskan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.2.1** | **Pengurusan Hak Akses Istimewa (Management of Privileged Access Rights)**<br>Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal.<br>Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas merujuk kepada Prosedur Pendaftaran, penyelenggaraan dan Penamatan Pengguna. | Pentadbir Sistem ICT |

## 8.3 Sekatan Akses Maklumat (Information Access Restriction)

**Kawalan:**
Akses kepada maklumat dan aset lain yang berkaitan hendaklah dihadkan mengikut dasar kawalan capaian yang ditetapkan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.3.1** | **Sekatan Akses Maklumat (Information Access Restriction)**<br>a) Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian merangkumi perkara berikut:<br>i) tidak membenarkan pengguna yang tidak berdaftar mencapai maklumat sensitif;<br>ii) menyediakan mekanisme konfigurasi untuk mengawal capaian kepada maklumat dalam sistem, aplikasi dan perkhidmatan;<br>iii) mengawal data yang boleh diakses oleh pengguna tertentu;<br>iv) mengawal identiti atau kumpulan identiti yang mempunyai akses, seperti | Pengguna, Pentadbir Sistem, ICTSO, Ketua Jabatan/ Ketua Bahagian |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | membaca, menulis, memadam dan melaksanakan (execute); dan<br>v) menyediakan kawalan capaian fizikal atau logikal untuk mengasingkan aplikasi sensitif, data aplikasi, atau sistem.<br><br>b) Penggunaan proses dan teknik pengurusan capaian yang dinamik (*Dynamic Access Management*) bagi melindungi maklumat sensitif perlu dilaksanakan sekiranya diperlukan dengan mengambil kira keperluan berikut:<br><br>i) perlindungan sepanjang kitar hayat maklumat dengan menetapkan peraturan berdasarkan kes penggunaan;<br>ii) mewujudkan operasi, proses memantau dan melapor serta infrastruktur sokongan teknikal; dan<br>iii) melindungi data dengan menetapkan keperluan pengesahan, menghadkan capaian, melaksanakan penyulitan, menetapkan kebenaran mencetak, merekod pengguna yang mencapai dan penggunaan maklumat serta memberikan amaran sekiranya terdapat percubaan untuk menyalahgunakan maklumat. | |

## 8.4 Kawalan Akses kepada Kod Sumber Program (Access to Source Code)

**<u>Kawalan:</u>**
Akses baca dan tulis kepada kod sumber, perisian pembangunan dan perpustakaan perisian (software libraries) hendaklah diuruskan dengan sewajarnya.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.4.1** | **<u>Kawalan Akses Kepada Kod Sumber Program (Access Control to Source Code)</u>**<br>Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut:<br><br>a) Log audit perlu dikekalkan kepada semua akses kepada kod sumber;<br>b) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan;<br>c) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik jabatan;<br>d) Menguruskan capaian kepada kod sumber program dan perpustakaan sumber program (*program source libraries*) mengikut prosedur yang ditetapkan; dan<br>e) Memberikan akses baca dan tulis kepada kod sumber berdasarkan keperluan dan berupaya mengawal risiko mengubah atau menyalahguna dan mengikut prosedur yang ditetapkan. | Pengarah Projek, Pengurus Projek dan Pentadbir Sistem ICT |

### 8.5 Pengesahan Selamat (Secure Authentication)

**<u>Kawalan:</u>**
Teknologi dan prosedur pengesahan selamat hendaklah dilaksanakan berdasarkan sekatan capaian maklumat dan polisi khusus mengenai kawalan capaian.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.5.1** | **<u>Prosedur Log Masuk yang Selamat (Secure Log-On Procedure)</u>**<br>Kawalan terhadap capaian aplikasi sistem pertu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti yang berikut: | Pentadbir Sistem, ICTSO, Pengarah Bahagian |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Jabatan;<br>b) Menjana amaran (alert) sekiranya berlaku perlanggaran semasa proses log maşuk terhadap aplikasi sistem;<br>c) Mengawal capaian ke atas aplikasi sistem mengikut prosedur yang ditetapkan;<br>d) Mewujudkan teknik pengesahan pelbagai faktor (*multi factor authentication* - MFA) berdasarkan klasifikasi maklumat yang bersesuaian bagi mengesahkan pengenalan diri pengguna;<br>e) Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan yang kukuh dan berkualiti; dan<br>f) Mewujudkan jejak audit ke atas semua capaian aplikasi sistem. | |
| **8.5.2** | **Sistem Pengurusan Kata Laluan (*Password Management System*)**<br>Pengurusan kata laluan mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh jabatan seperti yang berikut:<br><br>a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;<br>b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;<br>c) Panjang kata laluan mestilah sekurang-kurangnya DUA BELAS (12) AKSARA dengan gabungan antara huruf, aksara khas dan nombor (alphanumeric) KECUALI bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad;<br>d) Tiga (3) kata laluan yang pernah digunakan sebelum ini tidak digunakan semula. | Pengarah Bahagian/ ICTSO/ Pengguna/ Pemilik Sistem / Pentadbir Sistem |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | e) Kata laluan hendaklah diingat dan <u>TIDAK BOLEH</u> dicatat, disimpan atau didedahkan dengan apa cara sekali pun;<br>f) Kata laluan paparan kunci (lock screen) hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;<br>g) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara;<br>h) Kuat kuasakan pertukaran kata laluan semasa atau selepas login kali pertama atau selepas reset kata laluan;<br>i) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;<br>j) Had kemasukan kata laluan bagi capaian kepada sistem aplikasi adalah maksimum <u>TIGA (3) KALI</u> sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula;<br>k) Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna; dan<br>l) Mewajibkan pengguna menukar kata laluan sekurang-kurangnya setiap tiga (3) bulan untuk ke semua sistem/aplikasi utama. | |

## 8.6 Pengurusan Kapasiti (Capacity Management)

**<u>Kawalan:</u>**

Penggunaan sumber hendaklah dipantau dan diselaraskan selaras dengan keperluan kapasiti semasa dan unjuran.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.6.1** | **<u>Pengurusan Kapasiti (Capacity Management)</u>**<br>Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki | Pemilik Sistem, Pentadbir Sistem |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan<br>b) kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. | |

### 8.7 Perlindungan daripada Perisian Hasad (Protection Against Malware)

**<u>Kawalan:</u>**
Perlindungan terhadap Perisian *Malware* hendaklah dilaksanakan dan disokong oleh kesedaran pengguna.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.7.1** | **<u>Perlindungan daripada Perisian Hasad (Protection Against Malware)</u>**<br>a) Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan malware hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut.<br><br>b) Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya ini adalah seperti berikut:<br><br>i) Memasang sistem keselamatan untuk mengesan perisian atau program malware seperti antivirus, *Intrusion* | Pentadbir Sistem ICT, Pengguna |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | *Detection System* (IDS) dan *Intrusion Prevention System* (IPS) dan Web Application Firewall (WAF) serta mengikut prosedur penggunaan yang betul dan selamat;<br>ii) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa;<br>iii) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya;<br>iv) Mengemaskini antivirus dengan signature/pattern antivirus yang terkini;<br>v) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;<br>vi) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;<br>vii) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;<br>viii) menyediakan pelan kesinambungan perkhidmatan yang sesuai untuk pulih daripada serangan perisian hasad;<br>ix) menentukan prosedur dan tanggungjawab untuk menangani perlindungan terhadap perisian hasad pada sistem;<br>x) melaksanakan prosedur secara berkala untuk mengumpul maklumat tentang perisian *malware* baharu; dan | |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | xi) mengesahkan ketepatan sumber maklumat yang berkaitan dengan perisian *malware*. | |

## 8.8 Pengurusan Kerentanan Teknikal (Management of Technical Vulnerabilities)

**Kawalan:**
Maklumat tentang kelemahan teknikal sistem maklumat yang digunakan hendaklah diperolehi, pendedahan sistem maklumat jabatan kepada kelemahan tersebut hendaklah dinilai dan langkah yang sewajarnya hendaklah diambil.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.8.1** | **Pengurusan Kerentanan Teknikal (Management of Technical Vulnerabilities)**<br>a) 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.<br><br>b) Kawalan terhadap keterdedahan teknikal perlu dilaksanakan untuk melindungi sistem maklumat, perisian, dan infrastruktur teknikal organisasi daripada ancaman dan serangan yang berkaitan dengan kerentanan. Perkara yang perlu dipatuhi ialah seperti yang berikut:<br><br>i) Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi;<br>ii) Mengenal pasti, menilai dan menganalisis tahap risiko kerentanan yang wujud dalam sistem, perisian, dan rangkaian Jabatan;<br>iii) Melaksanakan tindakan penambahbaikan untuk mengatasi kerentanan yang telah dikenal pasti, | Pentadbir Sistem ICT dan C jabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | termasuk penambahbaikan keselamatan dan konfigurasi semula;<br>iv) Memantau sistem dan perisian secara berterusan untuk mengenalpasti kerentanan yang mungkin muncul dalam masa sebenar; dan<br>v) Melaksana dan memastikan amalan terbaik dalam keselamatan teknikal dan pengurusan kerentanan. | |

### 8.9 Pengurusan konfigurasi (Configuration Management)

**<u>Kawalan:</u>**
Konfigurasi, termasuk konfigurasi keselamatan, perkakasan, perisian, perkhidmatan dan rangkaian hendaklah diwujudkan, didokumenkan, dilaksanakan, dipantau dan disemak.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.9.1** | **Pengurusan konfigurasi (Configuration Management)**<br>Pengurusan konfigurasi bertujuan untuk memastikan perkakasan, perisian, perkhidmatan dan rangkaian berfungsi dengan betul mengikut tetapan keselamatan yang bersesuaian bagi memastikan konfigurasi tidak diubah oleh pihak yang tidak dibenarkan. Perkara yang perlu dipatuhi adalah seperti berikut:<br><br>a) Tadbir urus yang memantau dan meluluskan sebarang perubahan konfigurasi yang ingin dilaksanakan;<br>b) Prosedur untuk melaksana, memantau dan menyemak semula konfigurasi bagi peralatan, perisian, perkhidmatan dan rangkaian perlu ditetapkan;<br>c) Kaedah penyimpanan konfigurasi perkakasan, perisian, perkhidmatan dan rangkaian hendaklah mematuhi prosedur/arahan semasa berdasarkan nilai/klasifikasi maklumat dengan mengambilkira keperluan agensi; | Pentadbir Sistem, Pentadbir Server, Pentadbir Rangkaian |

## 8.10 Penghapusan Pelupusan/Sanitasi Maklumat (Information Deletion)

**Kawalan:**
Maklumat yang disimpan dalam sistem maklumat, peranti atau dalam mana-mana media storan lain hendaklah dipadamkan apabila tidak lagi diperlukan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.10.1** | **Penghapusan/Pelupusan/ Sanitasi Maklumat (*Information Deletion*)**<br>a) Penghapusan/pelupusan/sanitasi maklumat bertujuan untuk mengelakkan pendedahan maklumat sensitif dan mematuhi keperluan undang-undang, statutori, peraturan, dan kontrak untuk pelupusan maklumat.<br><br>b) Semua maklumat rasmi/rahsia rasmi kerajaan yang disimpan di dalam pelayan, cakera keras, rangkaian, USB atau media storan yang lain hendaklah dilupuskan mengikut ketetapan di dalam Surat Pekeliling Am Bilangan 4 Tahun 2022: Garis Panduan Sanitasi Media Elektronik dalam Perkhidmatan Awam atau peraturan yang sedang berkuatkuasa. Perkara yang hendaklah dipatuhi adalah seperti berikut:<br><br>i) Menentukan kaedah penghapusan maklumat yang sesuai selaras dengan keperluan Jabatan<br>ii) Merekod keputusan sebagai bukti penghapusan maklumat; dan<br>iii) Mendapatkan bukti penghapusan maklumat jika menggunakan perkhidmatan pembekal.<br>iv) Melindungi capaian terhadap fail konfigurasi mengikut kawalan yang ditetapkan; dan<br>v) Memantau konfigurasi untuk mengesahkan tetapan konfigurasi dan menilai kawalan keselamatan. | Semua Pengguna |

### 8.11 Penyamaran data (data masking)

**<u>Kawalan:</u>**
Penyamaran data hendaklah mengambil kira keperluan perkhidmatan dan polisi kawalan capaian serta polisi lain yang berkaitan tertakluk kepada keperluan perundangan dan peraturan yang berkuat kuasa.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.11.1** | **<u>Penyamaran data (data masking)</u>**<br>a) Penyamaran data (data masking) dilaksana bagi melindungi data sensitif seperti data *Personal Identifiable Information* (PII), dan data terperingkat dengan mengambil kira keperluan perkhidmatan dan polisi kawalan capaian serta polisi lain yang berkaitan tertakluk kepada keperluan perundangan dan peraturan yang berkuat kuasa.<br><br>b) Penyamaran data diperlukan bagi melindungi data PII dan data terperingkat daripada terdedah kepada pihak yang tidak bertanggung jawab yang akan menyebabkan imej jabatan terjejas.<br><br>c) Menggunakan teknik *data masking* yang bersesuaian seperti penyulitan, *deleting characters* dan *replacing value* dan pelaksanaan teknik *data masking* perlu mengambilkira peraturan/arahan semasa, menghadkan capaian pengguna berdasarkan keperluan data. | Pentadbir Sistem / Pengurus Rekod Jabatan |

### 8.12 Pencegahan Ketirisan data (Data Leakage Prevention)

**<u>Kawalan:</u>**
Langkah pencegahan ketirisan data hendaklah digunakan pada sistem, rangkaian dan sebarang peranti lain yang memproses, menyimpan atau menghantar maklumat sensitif.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.12.1** | **<u>Pencegahan ketirisan data (Data Leakage Prevention)</u>**<br>a) Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam sistem, infrastruktur rangkaian dan peralatan lain daripada sebarang ancaman ketirisan data. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:<br><br>i) **Pengendalian Akses:** setiap pengguna hanya memiliki akses yang diperlukan untuk tugas mereka.<br>ii) **Firewall:** Gunakan *firewall* untuk melindungi jaringan atau memantau lalu lintas dan mencegah akses yang tidak sah ke jaringan dan data.<br><br>b) Jabatan hendaklah melaksanakan perkara berikut untuk mengesan dan mencegah risiko ketirisan data:<br><br>i) Mengenal pasti dan mengelaskan maklumat untuk melindungi daripada ketirisan data (contoh: maklumat peribadi, kos projek dan minit mesyuarat terperingkat);<br>ii) Memantau saluran ketirisan data (contoh: e-mel, pemindahan fail, peranti mudah alih dan peranti storan mudah alih); dan<br>iii) bertindak untuk mencegah ketirisan maklumat dengan misalnya kuarantin e-mel yang mengandungi maklumat sensitif daripada berlaku ketirisan.<br>iv) Semua aktiviti yang melibatkan eksport data dan membawa keluar maklumat rasmi JWP oleh pegawai yang tamat perkhidmatan di JWP hendaklah mendapat kelulusan pemilik data/Pengarah Bahagian dan | Pentadbir Sistem / Pengurus Rekod Jabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | memastikan pengguna bertanggungjawab sekiranya berlaku ketirisan data.<br><br>c) Alat pencegahan ketirisan data hendaklah digunakan untuk:<br><br>i) mengenal pasti dan memantau maklumat sensitif yang berisiko untuk didedahkan tanpa kebenaran;<br>ii) mengesan pendedahan maklumat sensitif; dan<br>iii) menyekat tindakan pengguna atau penghantaran rangkaian yang mendedahkan maklumat sensitif. | |

### 8.13 Sandaran Maklumat (Information Backup)

**Kawalan:**

Salinan sandaran maklumat, perisian dan sistem hendaklah diselenggara dan diuji secara berkala mengikut prosedur yang dipersetujui mengenai sandaran.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.13.1** | **Sandaran Maklumat (Information Backup)**<br>Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara berkala mengikut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dipulihkan semula setelah berlakunya bencana, sandaran hendaklah dilakukan setiap kali konfigurasi berubah. Sandaran hendaklah direkodkan dan disimpan di *off site*. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>a) Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;<br>b) Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi; | Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | c) Menguji sistem sandaran sedia ada secara berkala bagi memastikannya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana; dan<br>d) Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya TIGA (3) bulan. | |

**8.14 Lewahan bagi Kemudahan Pemprosesan Maklumat (Redundancy of Information Processing Facilities)**

**Kawalan:**
Kemudahan pemprosesan maklumat hendaklah dilaksanakan dengan Lewahan yang mencukupi untuk memenuhi keperluan ketersediaan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.14.1** | **Lewahan bagi Kemudahan Pemprosesan Maklumat (Redundancy of Information Processing Facilities)**<br>Jabatan hendaklah mengenal pasti keperluan, mereka bentuk dan melaksanakan lewahan untuk memastikan kesinambungan perkhidmatan dan ketersediaan kemudahan pemprosesan maklumat.<br>Kemudahan lewahan hendaklah mengambil kira perkara berikut:<br><br>a) Menyediakan mekanisme yang bersesuaian untuk memberi amaran gangguan atau kegagalan kemudahan pemprosesan maklumat kepada Jabatan untuk memastikan lewahan tersebut boleh mengambil alih fungsi kemudahan utama dibaiki atau diganti; dan<br><br>b) Menguji keberkesanan (failover testing) kemudahan lewahan perlu diuji secara berkala. | Pentadbir Pusat Data, Pemilik Perkhidmatan dan Pentadbir Sistem ICT |

## 8.15 Menyediakan log (Logging)

**Kawalan:**

Log yang merekodkan aktiviti, pengecualian, ralat dan peristiwa lain yang berkaitan hendaklah dihasilkan, disimpan, dilindungi dan dianalisis.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.15.1** | **Menyediakan Log (Logging)**<br>a) Jabatan hendaklah menyedia, menyimpan, melindungi dan menganalisis log yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa berkaitan keselamatan maklumat. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti-aktiviti yang tidak normal serta aktiviti-aktiviti yang tidak dapat dijelaskan.<br><br>b) 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:<br><br>i) Fail log sistem pengoperasian;<br>ii) Fail log servis (contoh: web, e-mel);<br>iii) Fail log aplikasi (audit trail); dan<br>iv) Fail log rangkaian (contoh: switch, firewall, IPS).<br><br>c) Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut:<br><br>i) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; | Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | ii) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan<br>iii) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada pasukan CSIRT Jabatan. | |
| **8.15.2** | **Perlindungan Maklumat Log (Protection of Log Information)**<br>Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada perubahan dan capaian tanpa izin merangkumi perkara berikut:<br><br>a) Pengguna, termasuk mereka yang mempunyai hak akses istimewa, tidak diberi kebenaran untuk memadam atau menyahaktifkan log aktiviti mereka sendiri; dan<br>b) Kemudahan pengelogan beroperasi dengan baik. | Pentadbir Sistem ICT |
| **8.15.3** | **Log Pentadbir dan Pengendali (Administrator and Operator Logs)**<br>a) Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula secara berkala.<br><br>b) Memantau penggunaan kemudahan memproses maklumat secara berkala:<br><br>i) Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak secara berkala dan laporan perlu disediakan jika perlu; | Pentadbir Sistem ICT dan CSIRT jabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | ii) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya;<br>iii) Log Audit yang merekodkan semua aktiviti perlu diwujudkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan<br>iv) Aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah di laporkan kepada pasukan CSIRT Jabatan. | |

**8.16 Aktiviti Pemantauan (Monitoring Activities)**

**Kawalan:**
Rangkaian, sistem dan aplikasi hendaklah dipantau dan tindakan sewajarnya diambil untuk menilai kemungkinan insiden keselamatan maklumat.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.16.1** | **Aktiviti Pemantauan (Monitoring Activities)**<br>a) Tujuan aktiviti pemantauan dibuat adalah untuk mengesan tingkah laku tidak normal (anomali) dan kemungkinan berlaku insiden keselamatan maklumat.<br><br>b) Perkara yang perlu diperhatikan dalam aktiviti pemantauan perlu merangkumi perkara seperti berikut tetapi tidak terhad:<br><br>i) Trafik keluar (outbound) dan masuk (inbound) bagi rangkaian, sistem dan aplikasi;<br>ii) capaian kepada sistem, pelayan, peralatan rangkaian, sistem pemantauan dan aplikasi kritikal;<br>iii) fail konfigurasi rangkaian dan capaian pentadbir kepada sistem kritikal; | Pentadbir Sistem, Pentadbir Rangkaian & Pentadbir Server. ICTSO, CSIRT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | iv) log daripada peralatan keselamatan [cth. antivirus, IDS, sistem pencegahan pencerobohan (IPS), penapis web, firewall, pencegahan kebocoran data];<br>v) log peristiwa yang berkaitan dengan sistem dan aktiviti rangkaian;<br>vi) kod yang digunakan telah disahkan untuk pelaksanaan dan tidak diubah tanpa kebenaran; dan<br>vii) penggunaan prestasi sumber ICT (Unit Pemprosesan Pusat, cakera keras, memori capaian rawak dan lebar jalur). | |

### 8.17 Penyeragaman Waktu (Clock Synchronization)

**Kawalan:**

Tetapan waktu bagi sistem pemprosesan maklumat yang digunakan oleh organisasi hendaklah diseragamkan dengan sumber masa yang diluluskan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.17.1** | **Penyeragaman Waktu (Clock Synchronisation)**<br>a) Waktu bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain jabatan atau domain keselamatan hendaklah diseragamkan mengikut waktu piawai Malaysia.<br><br>b) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam JWP atau domain keselamatan hendaklah diseragamkan dengan penetapan masa yang diluluskan (contoh: SIRIM Network Time Protocol);<br><br>c) Kawalan ini bertujuan untuk membolehkan korelasi dan analisis insiden berkaitan insiden keselamatan maklumat dan data lain yang direkodkan, dan untuk menyokong proses penyiasatan terhadap insiden keselamatan maklumat. | Pentadbir Pusat Data |

## 8.18 Penggunaan Program Utiliti yang Mempunyai Hak Istimewa (Use of Privileged Utility Programs)

**Kawalan:**

Penggunaan program utiliti yang boleh mengatasi kawalan sistem dan aplikasi hendaklah dihadkan dan dikawal ketat.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.18.1** | **Penggunaan Program Utiliti yang Mempunyai Hak Istimewa (Use of Privileged Utility Programs)**<br>a) Penggunaan program utiliti yang boleh mengatasi (overriding) kawalan sistem dan aplikasi hendaklah dikawal dan dihadkan kepada pegawai yang dibenarkan sahaja<br><br>b) Garis panduan berikut untuk penggunaan program utiliti yang boleh mengatasi kawalan sistem dan aplikasi perlu dipertimbangkan:<br><br>i) had penggunaan program utiliti kepada bilangan praktikal minimum pengguna yang dipercayai dan dibenarkan;<br>ii) penggunaan prosedur pengenalan, pengesahan dan kebenaran untuk program utiliti, termasuk pengenalan unik orang yang menggunakan program utiliti;<br>iii) mentakrif dan mendokumentasikan tahap kebenaran untuk program utiliti;<br>iv) kebenaran untuk penggunaan ad hoc program utiliti;<br>v) tidak menyediakan program utiliti kepada pengguna yang mempunyai akses kepada aplikasi pada sistem di mana pengasingan tugas diperlukan;<br>vi) mengalih keluar atau melumpuhkan semua program utiliti yang tidak diperlukan;<br>vii) sekurang-kurangnya, pengasingan logik program utiliti daripada perisian aplikasi. Jika praktikal, mengasingkan | Pentadbir Sistem ICT, Pengarah Bahagian |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | komunikasi rangkaian untuk program sedemikian daripada trafik aplikasi;<br>viii) had ketersediaan program utiliti;dan<br>ix) pengelogan semua penggunaan program utiliti. | |

## 8.19 Pemasangan Perisian pada Sistem yang Beroperasi (Installation of Software on Operational Systems)

**Kawalan:**

Prosedur dan langkah-langkah hendaklah dilaksanakan untuk menguruskan pemasangan perisian dengan selamat pada sistem yang beroperasi.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.19.1** | **Pemasangan Perisian pada Sistem yang Beroperasi (Installation of Software on Operational Systems)**<br><br>Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem yang beroperasi. Langkah-langkah pemasangan hendaklah dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut:<br><br>a) Strategi *rollback* perlu hendaklah dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian;<br>b) Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan<br>c) Setiap konfigurasi ke atas sistem dan perisian hendaklah dikawal dan didokumentasikan dengan teratur.<br>d) Pengemaskinian sistem yang beroperasi hanya boleh dilaksanakan oleh pentadbir terlatih dengan kebenaran pengurusan;<br>e) memastikan bahawa hanya *executable code* yang telah diluluskan dan tiada kod | Pengarah Bahagian dan Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | pembangunan atau penyusun (compilers) dipasang pada sistem yang beroperasi;<br>f) mengemas kini semua perpustakaan sumber (source libraries) program yang sepadan;<br>g) menggunakan sistem kawalan konfigurasi untuk mengekalkan kawalan semua sistem yang beroperasi serta dokumentasi sistem;<br>h) mengarkibkan versi lama sistem, bersama-sama dengan semua maklumat dan parameter, prosedur, butiran konfigurasi dan perisian sokongan yang diperlukan sebagai langkah luar jangka (contigency), dan selagi sistem itu diperlukan untuk membaca atau memproses data yang diarkibkan. | |
| **8.19.2** | **Sekatan ke atas Pemasangan Perisian (Restriction on Software Installation)**<br>Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>a) Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan.<br>b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang- undang bertulis yang berkuat kuasa; dan<br>c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya. | Pentadbir Sistem ICT, warga jabatan, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT jabatan |

### 8.20 Keselamatan Rangkaian (Networks Security)

**Kawalan:**

Rangkaian dan peranti rangkaian hendaklah dilindungi, diurus dan dikawal untuk melindungi maklumat dalam sistem dan aplikasi.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| 8.20.1 | **Kawalan Rangkaian (Network Control)**<br>a) Kawalan infrastruktur rangkaian hendaklah dilaksanakan untuk memastikan keselamatan maklumat dalam rangkaian dan untuk melindungi perkhidmatan yang disambungkan dalam infrastruktur rangkaian daripada capaian yang tidak dibenarkan.<br><br>b) Perkara yang hendaklah dipatuhi adalah seperti berikut:<br><br>i) Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan;<br>ii) Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk;<br>iii) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja;<br>iv) Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;<br>v) Firewall hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian;<br>vi) Semua trafik keluar dan masuk rangkaian hendaklah melalui firewall di bawah kawalan jabatan;<br>vii) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna KECUALI mendapat kebenaran daripada Pegawai Keselamatan ICT (ICTSO); | Pengarah Bahagian dan Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | viii) Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam keselamatan data dan maklumat jabatan;<br>ix) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;<br>x) Sebarang penyambungan rangkaian yang bukan di bawah kawalan Jabatan adalah tidak dibenarkan;<br>xi) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di jabatan sahaja dan penggunaan modem adalah dilarang sama sekali;<br>xii) Kemudahan bagi wireless LAN hendaklah dipantau dan dikawal penggunaannya;<br>xiii) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan;<br>xiv) Menempatkan atau memasang antara muka (interfaces) yang bersesuaian di antara rangkaian jabatan, rangkaian jabatan lain dan rangkaian awam;<br>xv) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;<br>xvi) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja;<br>xvii) Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh;<br>xviii) Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang | |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | dikongsi dan menjangkau sempadan jabatan; dan<br>xix) Mewujud dan melaksana kawalan pengalihan laluan (routing control) bagi memastikan pematuhan terhadap peraturan jabatan.<br>xx) Semua peralatan yang hendak disambung kepada rangkaian perlu bebas daripada virus dan mempunyai antivirus yang sah;<br>xxi) Capaian kepada rangkaian perlu dilaksanakan mengikut kategori yang telah ditetapkan iaitu Intranet, Internet dan DMZ;<br>xxii) Sistem yang terdapat di dalam rangkaian Intranet tidak dibenarkan dicapai dari Internet;<br>xxiii) Pihak ketiga adalah tidak dibenarkan untuk mencapai rangkaian Intranet kecuali untuk kerja-kerja pembangunan atau penyelenggaraan sistem dengan kebenaran Jabatan; dan<br>xxiv) Capaian kepada wireless hendaklah dikawal mengikut kategori pengguna. | |

### 8.21 Keselamatan Perkhidmatan Rangkaian (Security of Network Services)

**Kawalan:**

Mekanisme keselamatan, tahap perkhidmatan dan keperluan perkhidmatan perkhidmatan rangkaian hendaklah dikenal pasti, dilaksanakan dan dipantau.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.21.1** | **Keselamatan Perkhidmatan Rangkaian (Security of Network Services)**<br>Pengurusan bagi semua perkhidmatan rangkaian (inhouse atau outsource) yang merangkumi mekanisme keselamatan dan tahap serta keperluan perkhidmatan rangkaian hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan. | ICTSO, Pengarah Bahagian, Pentadbir Sistem ICT dan Pembekal |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.21.2** | **<u>Peralatan dalam rangkaian</u>**<br>Bagi memastikan bahawa peralatan yang disambungkan kepada rangkaian Jabatan tidak menjejaskan keselamatan maklumat dan capaian perkara-perkara berikut hendaklah dipatuhi:<br><br>a) Setiap peralatan yang hendak disambung kepada rangkaian Jabatan hendaklah didaftarkan;<br>b) Semua peralatan hendaklah disahkan bebas daripada virus dan perisian antivirus yang sah hendaklah dipasang dan masih aktif sepanjang masa;<br>c) Hanya peralatan yang telah berdaftar dibenarkan untuk sambungan (join) kepada rangkaian;<br>d) Setiap peralatan yang hendak disambung ke rangkaian perlu menggunakan protokol TCP/IP dan akan menggunakan IP address dan nama domain yang ditetapkan oleh pentadbir rangkaian; dan<br>e) Semua konfigurasi peralatan dalam rangkaian selepas *switches* adalah menjadi tanggungjawab pengguna | Pentadbir Rangkaian |
| **8.21.3** | **<u>Capaian ke PORT untuk tujuan diagnostik</u>**<br>Bagi memastikan bahawa port rangkaian tidak dicapai tanpa pengawasan, perkara berikut perlu dipatuhi oleh semua pengguna:<br>a) Semua port yang tak digunakan perlu dinyahaktifkan;<br>b) Capaian fizikal dan logikal ke atas port untuk tujuan diagnostik perlu mendapat kebenaran pegawai yang diberikan kuasa;<br>c) Capaian oleh pegawai Jabatan hanya dibenarkan berasaskan kepada tugas dan skop kerja; dan<br>d) Capaian oleh pihak ketiga perlu mendapat kelulusan dari pegawai yang diberikan kuasa. | Pentadbir Rangkaian |

## 8.22 Pengasingan dalam Rangkaian (Segregation of Networks)

**Kawalan:**

Kumpulan perkhidmatan maklumat, pengguna dan sistem maklumat hendaklah diasingkan dalam rangkaian jabatan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.22.1** | **Pengasingan dalam Rangkaian (Segregation in Networks)**<br>Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian jabatan. | ICTSO, Pengarah Bahagian dan Pentadbir Sistem ICT |

## 8.23 Penyaringan Web (Web filtering)

**Kawalan:**

Akses kepada laman web luaran hendaklah diuruskan untuk mengurangkan pendedahan kepada kandungan berniat jahat.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.23.1** | a) Kawalan penyaringan web dalam bentuk perisian atau sebagainya perlu dilaksanakan bagi mengesan dan menyekat akses ke laman web yang dianggap tidak selamat dan tidak sesuai. Ini bagi melindungi jabatan daripada sebarang ancaman keselamatan siber.<br><br>b) Jabatan hendaklah menghalang akses kepada laman web yang mengandungi maklumat yang dilarang (yang telah dikenal pasti oleh jabatan), diketahui mengandungi virus atau aktiviti memancing data (phishing).<br><br>c) Jabatan hendaklah mengenal pasti jenis laman web yang tidak boleh diakses. Jabatan hendaklah mempertimbangkan untuk menyekat akses kepada jenis laman web yang mempunyai ciri - ciri berikut melainkan telah mendapat kebenaran: | Pentadbir Rangkaian |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | i) laman web yang diketahui atau disyaki berniat jahat;<br>ii) laman web / pelayan yang diketahui atau disyaki mempunyai ciri perintah dan kawal (command and control);<br>iii) laman web berniat jahat yang diperoleh daripada perisian atau perkhidmatan perisikan ancaman (threat intelligence); dan<br>iv) laman web yang berkongsi kandungan yang tidak dibenarkan. | |

**8.24 Penggunaan Kriptografi (Use of Cryptography)**

**Kawalan:**

Peraturan untuk penggunaan kriptografi yang berkesan, termasuk pengurusan kunci kriptografi, hendaklah ditakrifkan dan dilaksanakan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.24.1** | **Polisi Penggunaan Kawalan Kriptografi (Policy on The Use of Cryptographic Control)**<br>Kriptografi merangkumi kaedah-kaedah seperti yang berikut:<br><br>a) Enkripsi<br>Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (encryption).<br><br>b) Tandatangan Digital<br>Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. | Pengarah Projek |
| **8.24.2** | **Pengurusan Kunci Awam (Public Key Management)**<br>Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam/Public Key Infrastructure (PKI) hendaklah | Warga jabatan |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut. | |
| **8.24.3** | Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan, dan/atau keutuhan maklumat. Kriptografi merangkumi kaedah-kaedah seperti yang berikut:<br><br>i) Enkripsi<br>ii) Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (encryption).<br>iii) Tandatangan Digital<br>iv) Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. | Pengarah Projek |

## 8.25 Kitar Hayat Pembangunan Sistem Yang Selamat (Secure Development Life Cycle)

**Kawalan:**
Peraturan untuk pembangunan perisian dan sistem yang selamat hendaklah diwujudkan dan digunakan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.25.1** | **Dasar Pembangunan Sistem yang Selamat (Secure Development Policy)**<br>Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam jabatan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:<br><br>i) Keselamatan persekitaran pembangunan;<br>ii) Keselamatan pangkalan data;<br>iii) Keperluan keselamatan dalam fasa reka bentuk; | ICTSO, Pengarah Bahagian dan Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | iv) Keperluan *check point* keselamatan dalam carta perbatuan projek;<br>v) Keperluan pengetahuan ke atas keselamatan aplikasi;<br>vi) Keselamatan dalam kawalan versi; dan<br>vii) Bagi pembangunan secara penyumberluaran (outsource), pembekal yang dilantik hendaklah berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem. | |
| **8.25.2** | **<u>Kitar Hayat Pembangunan Sistem yang selamat (Secure Development Life Cycle)</u>**<br>a) Jabatan hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.<br><br>b) Jabatan hendaklah melaksanakan penilaian risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira:<br><br>i) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem;<br>ii) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran;<br>iii) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;<br>iv) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem;<br>v) Pegawai yang bekerja di dalam persekitaran Pembangunan sistem ialah yang boleh dipercayai; dan<br>vi) Kawalan ke atas capaian kepada persekitaran pembangunan sistem. | Pentadbir Sistem ICT dan Pemilik Sistem |

## 8.26 Keperluan Keselamatan Aplikasi (Application Security Requirements)

**Kawalan:**
Keperluan keselamatan maklumat hendaklah dikenal pasti, dinyatakan dan diluluskan apabila membangunkan atau memperoleh sistem aplikasi.

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

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | f) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak. | |
| **8.26.2** | **<u>Melindungi Transaksi Perkhidmatan Aplikasi (Protecting Application Services Transactions)</u>**<br>a) 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 papar mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:<br><br>i) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi;<br>ii) Memastikan semua aspek transaksi dipatuhi:<br><br>a. maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan;<br>b. mengekalkan kerahsiaan maklumat;<br>c. mengekalkan privasi pihak yang terlibat; dan<br>d. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi.<br><br>b) Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan. | ICTSO, Pengarah Bahagian dan Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.26.3** | **<u>Keperluan Keselamatan Aplikasi (Application Security Requirements)</u>**<br>Spesifikasi reka bentuk aplikasi hendaklah mengandungi keperluan keselamatan sistem maklumat. Sekiranya sesuatu produk off- the-shelf diperolehi, pembekal perlu dimaklumkan berkenaan keperluan keselamatan produk. | Pentadbir Sistem ICT |

**8.27 Prinsip Reka Bentuk dan Kejuruteraan Sistem yang Selamat (Secure System Architecture and Engineering Principles)**

**<u>Kawalan:</u>**

Prinsip untuk kejuruteraan sistem yang selamat hendaklah diwujudkan, didokumenkan, diselenggara dan digunakan untuk aktiviti pembangunan sistem maklumat.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.27.1** | **<u>Prinsip Kejuruteraan Sistem yang Selamat (Secure System Engineering Principles)</u>**<br>Prinsip untuk kejuruteraan sistem yang selamat hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk aktiviti pembangunan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation* (IV&V) sektor awam yang terkini. | Pentadbir Sistem ICT, Pengarah Bahagian |
| **8.27.2** | **<u>Prinsip Kejuruteraan Sistem Yang Selamat (Secure System Engineering Principles)</u>**<br>a) Kawalan perubahan kepada sistem maklumat hendaklah dilaksanakan bagi mengurangkan risiko kerosakan pada sistem maklumat.<br><br>b) Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: | Pentadbir Sistem ICT, Pengarah Bahagian |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | i) Proses pengemaskinian sistem maklumat hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang diberi tanggungjawab dan mengikut prosedur yang telah ditetapkan;<br>ii) Kod atau atur cara sistem yang telah dikemas kini hanya boleh digunakan selepas diuji dan diluluskan;<br>iii) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan;<br>iv) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan<br>v) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal dan semua konfigurasi sistem perlu didaftar dan didokumenkan. | |

**8.28 Pengekodan Selamat (Secure Coding)**

**Kawalan:**

Prinsip pengaturcaraan yang selamat hendaklah digunakan dalam pembangunan sistem.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.28.1** | **Kawalan capaian kepada kod sumber (Source Code)**<br>a) Kawalan capaian kepada kod sumber atau atur cara program perlu dilaksanakan bagi mengelakkan kecurian, pengubahsuaian dan penghapusan tanpa kebenaran.<br><br>b) Kod sumber bagi semua aplikasi dan perisian adalah menjadi hak milik Jabatan.<br><br>c) Perancangan Sebelum Pengekodan | Pentadbir Sistem, ICTSO |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | Prinsip pengekodan selamat hendaklah digunakan untuk pembangunan baru dan dalam senario penggunaan semula. Prinsip-prinsip ini hendaklah diterapkan dalam aktiviti pembangunan baik dalam jabatan dan untuk produk serta perkhidmatan yang dibekalkan oleh jabatan kepada pihak lain. Perancangan dan prasyarat sebelum pengekodan hendaklah merangkumi perkara seperti berikut tetapi tidak terhad kepada:<br><br>i) keperluan khusus jabatan dan prinsip yang diluluskan untuk pengekodan selamat digunakan untuk pembangunan *in-house* dan *outsource*;<br>ii) sebarang kelemahan pengekodan yang pernah berlaku dan membawa kepada kerentanan keselamatan maklumat hendaklah dielakkan; dan<br>iii) berpandukan piawaian dan amalan terbaik pengekodan selamat yang berkuatkuasa.<br><br>d) Perancangan Semasa Pengekodan<br><br>Pertimbangan semasa pengekodan hendaklah merangkumi:<br><br>i) amalan pengekodan selamat yang khusus untuk bahasa pengaturcaraan dan kaedah yang digunakan;<br>ii) mendokumentasikan kod dan menghapuskan kecacatan pengaturcaraan, yang boleh menyebabkan kelemahan keselamatan maklumat dieksploitasi;<br>iii) Penggunaan teknik reka bentuk yang selamat (contohnya tidak menggunakan kata laluan yang dikodkan, sampel kod | |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | yang tidak diluluskan dan perkhidmatan web tanpa pengesahan).<br>iv) Pengujian keselamatan hendaklah dilaksanakan semasa dan selepas pembangunan untuk mengesan kelemahan perisian / sistem.<br><br>e) Semakan dan penyelenggaraan<br><br>Selepas kod telah beroperasi:<br><br>i) Sebarang pengemaskinian kepada kod hendaklah dipakej dan dipasang dengan selamat;<br>ii) Kelemahan keselamatan maklumat yang dilaporkan hendaklah dibaik pulih;<br>iii) Ralat dan cubaan serangan hendaklah direkodkan serta dibuat semakan log secara berkala dan membuat pengemaskinian pada kod jika perlu; dan<br>iv) Kod sumber hendaklah dilindungi daripada akses dan perubahan tidak sah. | |

**8.29 Pengujian dan Penerimaan Keselamatan Sistem (Security Testing in Development and Acceptance)**

**Kawalan:**

Proses ujian fungsi keselamatan hendaklah ditakrifkan dan dilaksanakan dalam kitaran hayat pembangunan sistem.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.29.1** | **Pengujian Keselamatan Sistem (System Security Testing)**<br>Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem.<br>Perkara yang perlu dipatuhi adalah seperti yang berikut: | Pentadbir Sistem ICT, ICTSO |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | a) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat;<br>b) Membuat semakan pengesahan di dalam aplikasi untuk mengenal pasti kesilapan maklumat;<br>c) menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan;<br>d) melakukan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem; dan<br>e) menjalankan ujian penembusan untuk mengenal pasti kod dan reka bentuk yang tidak selamat. | |
| **8.29.2** | **<u>Pengujian Penerimaan Sistem (System Accepting Testing)</u>**<br>Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>a) pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat dan kepatuhan kepada Polisi Pembangunan Selamat;<br>b) penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai;<br>c) melakukan pengimbasan kelemahan untuk mengenal pasti konfigurasi yang tidak selamat dan kelemahan sistem; dan<br>d) menjalankan ujian penembusan untuk mengenal pasti kod dan reka bentuk yang tidak selamat. | Pengguna, Pentadbir Sistem ICT, ICTSO |

## 8.30 Pembangunan oleh Pembekal (Outsourced Development)

**Kawalan:**
Jabatan hendaklah mengarah, memantau dan menyemak aktiviti yang berkaitan dengan pembangunan sistem secara penyumberan luar.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.30.1** | **Pembangunan oleh Khidmat Luaran (Outsourced Software Development)**<br>Jabatan hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dilaksanakan secara penyumberan luar oleh pihak luar. Kod sumber (source code) adalah menjadi HAK MILIK jabatan. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>a) Perjanjian hendaklah termasuk perjanjian pelesenan sistem bagi menangani pemilikan ke atas kod sumber dan hak harta intelek sistem dengan memastikan lesen yang dibeli dan digunakan untuk pembangunan sistem, kod sumber dan hak harta intelek sistem yang dibangunkan secara penyumberan luar adalah HAK MILIK jabatan;<br>b) Bagi semua perkhidmatan sumber luaran, perisian sebagai satu perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori **“Pembekal hendaklah membenar Kerajaan hak mencapai kod sumber dan melaksanakan pengolahan risiko”;**<br>c) Keperluan perjanjian untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pembekal dilantik mengikut amalan terbaik;<br>d) Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem;<br>e) Jika perlu dan sesuai, pihak Kerajaan dan pihak pembekal boleh mengguna pakai prinsip dan tatacara escrow (escrow ialah satu perjanjian kewangan di mana terdapat | Pentadbir Sistem ICT, Pengarah Bahagian, ICTSO |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | pihak ketiga yang memegang dan menguruskan transaksi dana bagi dua pihak sehingga satu perjanjian kontrak tercapai);<br>f) Mematuhi keberkesanan kawalan keselamatan dan undang-undang dalam melaksanakan pengesahan pengujian.<br>g) penyediaan model ancaman untuk dipertimbangkan, diamalkan dan dipatuhi oleh pembekal;<br>h) peruntukan bukti bahawa tahap minimum yang boleh diterima bagi keupayaan keselamatan dan privasi diwujudkan;<br>i) Menyimpan bukti tentang cara ujian yang mencukupi telah dilakukan untuk melindungi sistem yang dihantar kepada Kerajaan bebas daripada kandungan berniat jahat;<br>j) peruntukan bukti bahawa ujian yang mencukupi telah digunakan untuk melindungi daripada kelemahan yang diketahui;<br>k) Perjanjian dengan pembekal hendaklah mengandungi hak jabatan untuk melaksanakan audit ke atas proses dan kawalan pembangunan;<br>l) Mewujudkan dan melaksanakan keperluan keselamatan untuk persekitaran pembangunan; dan<br>m) Jabatan dan pembekal hendaklah menguruskan dan melaksanakan pembangunan sistem secara sumber luaran berdasarkan undang-undang, peraturan dan pekeliling berkaitan yang sedang berkuat kuasa. | |

## 8.31 Pengasingan Persekitaran Pembangunan, Pengujian dan Pengeluaran (Separation of Development, Test and Production Environments)

**<u>Kawalan:</u>**

Persekitaran pembangunan, ujian dan pengeluaran hendaklah diasingkan dan selamat

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.31.1** | **Pengasingan Persekitaran Pembangunan, Pengujian dan Operasi (Separation of Development, Test and Operational Facilities)**<br>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:<br><br>a) Perkakasan dan perisian yang digunakan bagi tugas mentakrifkan, mendokumentasikan, membangun, mengemaskini, menyelenggara dan menguji sistem perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (production).<br>b) Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan<br>c) Data yang mengandungi maklumat rahsia rasmi tidak boleh digunakan di dalam persekitaran pembangunan melainkan telah mengambil kira kawalan keselamatan maklumat.<br>d) menguji perubahan kepada sistem pengeluaran dan aplikasi dalam persekitaran ujian atau pementasan sebelum digunakan pada sistem pengeluaran;<br>e) tidak menguji dalam persekitaran pengeluaran kecuali dalam keadaan yang telah ditentukan dan diluluskan;<br>f) penyusun (compiler), editor dan alat pembangunan atau program utiliti lain yang tidak boleh diakses daripada sistem pengeluaran apabila tidak diperlukan;<br>g) Untuk mengurangkan kesilapan, label persekitaran yang betul hendaklah dipaparkan dengan jelas dalam menu; dan<br>h) Tiada aset maklumat sensitif dipindahkan ke dalam mana-mana pembangun atau sistem | Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | ujian melainkan langkah keselamatan yang setara disediakan. | |
| **8.31.2** | **<u>Persekitaran Pembangunan Selamat (Secure Development Environment)</u>**<br>a) Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.<br><br>b) Jabatan hendaklah menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira:<br><br>i) Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem;<br>ii) Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran;<br>iii) Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem;<br>iv) Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem;<br>v) Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan<br>vi) Kawalan ke atas capaian kepada persekitaran pembangunan sistem. | Pentadbir Sistem ICT dan Pengarah Bahagian |

### 8.32 Pengurusan Perubahan (Change Management)

**<u>Kawalan:</u>**
Perubahan kepada kemudahan pemprosesan maklumat dan sistem maklumat hendaklah tertakluk kepada prosedur pengurusan perubahan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.32.1** | **<u>Pengurusan Perubahan (Change Management)</u>**<br>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:<br><br>a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;<br>b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;<br>c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan<br>d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak sengaja. | Pentadbir Sistem ICT |
| **8.32.2** | **<u>Prosedur Kawalan Perubahan Sistem (*System Change Control Procedures*)</u>**<br>Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>a) perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah | Pengarah Bahagian dan Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai;<br>b) aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan maklumat jabatan. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal;<br>c) mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan yang dibenarkan sahaja; dan<br>d) capaian kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang dibenarkan sahaja. | |
| **8.32.3** | **<u>Kajian Semula Keperluan Teknikal bagi Aplikasi Selepas Perubahan Platform Operasi (Technical Review of Applications After Operating Platform Change)</u>**<br>Apabila platform operasi berubah, aplikasi penting jabatan hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan maklumat jabatan. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>a) Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform;<br>b) Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan<br>c) Memastikan perubahan yang sesuai dibuat kepada Pelan Kesinambungan Perkhidmatan jabatan dan Pelan Pemulihan Bencana Sistem yang berkaitan berdasarkan Pelan | Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | Pengurusan Keselamatan Maklumat (ISMP) sistem tersebut. | |
| **8.32.4** | **<u>Sekatan Ke atas Perubahan Dalam Pakej Perisian (Restrictions on Changes to Software Packages)</u>**<br>Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat. | Pentadbir Sistem ICT, Pengarah Bahagian |

**8.33 Maklumat Pengujian (Test Information)**

**<u>Kawalan:</u>**

Maklumat untuk tujuan pengujian hendaklah dipilih, dilindungi dan diurus dengan sewajarnya.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.33.1** | **<u>Perlindungan Data Ujian (Protection of Test Data)</u>**<br>Untuk memastikan perlindungan ke atas maklumat yang digunakan untuk pengujian. Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut:<br><br>a) Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian;<br>b) Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian;<br>c) Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan<br>d) Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar. | Pengguna, Pentadbir Sistem ICT, ICTSO |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | e) Melindungi maklumat sensitif melalui penyingkiran atau penyamaran data jika digunakan untuk ujian; dan<br>f) Memadam maklumat operasi daripada persekitaran ujian serta-merta dengan betul selepas ujian selesai untuk mengelakkan penggunaan maklumat ujian tanpa kebenaran. | |

**8.34 Perlindungan Sistem Maklumat Semasa Pengujian Audit (Protection of Information Systems During Audit Testing)**

**Kawalan:**
Ujian audit dan aktiviti jaminan lain yang melibatkan penilaian sistem operasi hendaklah dirancang dan dipersetujui antara penguji dan jabatan.

| ID | PENERANGAN | PERANAN |
|---|---|---|
| **8.34.1** | **Kawalan Audit Sistem Maklumat (Information Systems Audit Controls)**<br>a) Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas operasi sistem dan proses jabatan.<br><br>b) Garis panduan berikut hendaklah dipatuhi:<br><br>i) bersetuju dengan permintaan audit untuk mendapat akses kepada sistem dan data dengan pengurusan yang sesuai;<br>ii) bersetuju dan mengawal skop ujian audit teknikal;<br>iii) Jabatan hanya boleh menyediakan akses baca sahaja kepada maklumat dan perisian. Jika tidak mungkin untuk menggunakan teknik baca sahaja, pentadbir yang mempunyai hak akses yang diperlukan boleh mendapatkan akses kepada sistem/aplikasi atau data bagi pihak juruaudit; | ICTSO dan Pentadbir Sistem ICT |

| ID | PENERANGAN | PERANAN |
|---|---|---|
| | iv) Jika permintaan akses dibenarkan, Jabatan hendaklah terlebih dahulu mengesahkan bahawa peranti yang digunakan untuk mengakses sistem/aplikasi memenuhi keperluan keselamatan sebelum menyediakan akses;<br>v) hanya membenarkan akses selain daripada baca sahaja untuk salinan terpencil fail sistem, memadamkannya apabila audit selesai, atau memberi mereka perlindungan yang sewajarnya jika terdapat kewajiban untuk menyimpan fail tersebut dibawah keperluan dokumentasi audit;<br>vi) mengenal pasti dan bersetuju dengan permintaan untuk pemprosesan khas atau tambahan, seperti menjalankan alat audit;<br>vii) Jika audit menghadapi risiko menjejaskan ketersediaan sistem/aplikasi, audit hendaklah dijalankan di luar waktu operasi pejabat untuk mengekalkan ketersediaan maklumat;<br>viii) memantau dan mengelog semua akses untuk tujuan audit dan ujian. | |

# LAMPIRAN

**LAMPIRAN A**

**RUJUKAN**

**SENARAI PERUNDANGAN DAN PERATURAN**

1. Akta 854 - Akta Keselamatan Siber 2024 (26 Jun 2024)
2. Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam
3. Pekeliling Am Bilangan 4 Tahun 2022 Pengurusan dan pengendalian Insiden Keselamatan Siber Sektor Awam
4. Arahan MKN No. 26 Pengurusan Keselamatan Siber Negara 21 Disember 2021
5. Pekeliling Am Bilangan 2 Tahun 2021 - Manual Pengurusan Aset Menyeluruh Kerajaan versi 2.0
6. Surat Pekeliling Am Bilangan 1 Tahun 2021 - Larangan Penggunaan Telefon Bimbit, Peralatan Eletronik yang Mampu Merakam Maklumat dalan Mesyuarat Penting Kerajaan
7. Pekeliling Transformasi Pentadbiran Awam Bil. 3 Tahun 2018 - Panduan Pelaksanaan Pengurusan Projek ICT Sektor Awam (PPrISA). (1 Mac 2018)
8. Arahan Keselamatan (Semakan dan Pindaan 2017)
9. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSA) versi 1.0 April 2016
10. Pekeliling Am Bil. 1 Tahun 2015 - Pelaksanaan Data Terbuka Sektor Awam
11. Surat Pekeliling Perbendaharaan - Garis Panduan Mengenai Pengurusan Perolehan Information Telecommunication Technology ICT Kerajaan SPP 3/2013
12. Pekeliling Perbendaharaan Malaysia PK 2/2013 - Kaedah Perolehan Kerajaan.
13. Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013
14. Arahan Ketua Pegawai Keselamatan Kerajaan 5 Jun 2012 - Langkah-Langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba Dan Peranti Mudah Alih Di Sektor Awam
15. Surat Arahan Ketua Pengarah MAMPU - Amalan Terbaik Penggunaan Media Jaringan Sosial (Tarikh: 8 April 2011)

16. Surat Arahan Ketua Pengarah MAMPU - Pemantapan Penggunaan Dan Pengurusan E-Mel Di Agensi-Agensi Kerajaan. (Tarikh: 1 Julai 2010)
17. Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat 24 Nov 2010
18. Akta 709 - Akta Perlindungan Data Peribadi 2010
19. Surat Arahan Ketua Pengarah MAMPU 2010 - Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam
20. Surat Arahan Ketua Pengarah MAMPU - Garis Panduan Transisi Protokol Internet Versi 6 (IPV6) Sektor Awam. (Tarikh: 4 Januari 2010)
21. Garis Panduan Penggunaan ICT Ke Arah ICT Hijau Dalam Perkhidmatan Awam (Ogos 2010)
22. Surat Pekeliling Am Bilangan 7 Tahun 2024 Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam
23. Surat Pekeliling Am Bilangan 3 Tahun 2009 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009
24. Surat Arahan Ketua Pengarah MAMPU - Penggunaan Media Jaringan Sosial Di Sektor Awam. (Tarikh: 19 November 2009)
25. Surat Arahan Ketua Pengarah MAMPU - Penggunaan Smartphone, Personel Digital Assistant Dan Alat Komunikasi Mudah Alih Sebagai Saluran Komunikasi Tambahan (Tarikh: 15 September 2009)
26. Surat Arahan Ketua Pengarah MAMPU 2007 - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007
27. Surat Arahan Ketua Pengarah MAMPU 2007 - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi - Agensi Kerajaan yang bertarikh 23 November 2007
28. Arahan Teknologi Maklumat Dan Akta Aktiviti Kerajaan Elektronik (Akta 680) (Tahun 2007)

29. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi - Agensi Kerajaan, 23 November 2007
30. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006
31. Garis Panduan IT Outsourcing (Oktober 2006)
32. Surat Pekeliling Am Bilangan 3 Tahun 2024 Garis Panduan Pengurusan Risiko keselamatan Maklumat Sektor Awam
33. Garis Panduan Keselamatan MAMPU 2004
34. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan
35. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan
36. Akta Komunikasi dan Multimedia 1998
37. Akta Jenayah Komputer 1997
38. Akta Tandatangan Digital 1997
39. Akta Hak Cipta (Pindaan) Tahun 1997
40. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan
41. Akta Rahsia Rasmi 1972
42. Perintah - Perintah Am
43. Arahan Perbendaharaan
44. Garis Panduan Penyimpanan dan Pemeliharaan Rekod Elektronik Sektor Awam
45. Arahan 20 (Semakan Semula) - Dasar dan Mekanisme Pengurusan Bencana Negara
46. Arahan 24 - Dasar Dan Mekanisme Pengurusan Krisis Siber Negara.
47. Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam
48. Akta 658 – Akta Perdagangan Elektronik 2006

49. Akta 629 - Akta Arkib Negara 2003
50. Akta 606 - Akta Cakera Optik 2000
51. Surat Pekeliling Am Bilangan 2/1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan Akta Rahsia Rasmi (Pindaan 1987)
52. Surat Pekeliling Am Bilangan 2 Tahun 1987: Garis Panduan Mengenai Pengelasan Dokumen Rasmi Kerajaan
53. Akta 298 - Kawasan Larangan Tempat Larangan 1959
54. Akta 56 - Akta Keterangan 1950
55. National Cyber Security Policy (NCSP)
56. Guideline to Determine Information Security Professionals Requirement for the CNII Agencies/Organisations
57. Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara
58. Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi
59. Perintah Am Bab D

**LAMPIRAN B**

JABATAN PERDANA MENTERI
JABATAN WILAYAH PERSEKUTUAN

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

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

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

Tandatangan : ………………………………………………….

Nama : ………………………………………………….
No. Kad Pengenalan : ………………………………………………….
Jawatan : ………………………………………………….
Syarikat : …………………………………………………..
Tarikh : …………………………………………………..

Disaksikan oleh: ………………………………………………….
(Tandatangan)

Nama : …………………………………………………..
No. Kad Pengenalan : …………………………………………………..
Jawatan : …………………………………………………..
Jabatan : …………………………………………………..
Tarikh : …………………………………………………..
Cop Jabatan : ……………………………………………………

**LAMPIRAN C(I)**

## AKUAN PEMATUHAN

## POLISI KAWALAN KESELAMATAN MAKLUMAT (PKKM) JABATAN WILAYAH PERSEKUTUAN

**Nama (Huruf Besar)** : ..............................

**No. Kad Pengenalan** : ..............................

**Jawatan** : ..............................

**Bahagian** : ..............................

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam PKKM; dan

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

Tandatangan : ..................................................

Tarikh : ..................................................

---

Pengesahan Pegawai Keselamatan ICT

................................................

(Tandatangan & Cop Jawatan)

Jabatan Wilayah Persekutuan

Tarikh: .........................

* PKKM boleh dicapai menerusi http://www.jwp.gov.my

**LAMPIRAN C(II)**

## AKUAN PEMATUHAN

## POLISI KAWALAN KESELAMATAN MAKLUMAT (PKKM)
## JABATAN WILAYAH PERSEKUTUAN

**Nama (Huruf Besar)** : ..........................................

**No. Kad Pengenalan** : ..........................................

**Nama Syarikat** : ..........................................

**No. Pendaftaran Syarikat** : ..........................................

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam PKKM; dan

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

Tandatangan : ..................................................

Tarikh : ..................................................

---

Pengesahan Pegawai Keselamatan ICT

................................................

(Tandatangan & Cop Jawatan)

Jabatan Wilayah Persekutuan

Tarikh: .........................

* PKKM boleh dicapai menerusi http://www.jwp.gov.my