BSEP

BAHAGIAN SIBER DAN ELEKTROMAGNETIK PERTAHANAN

GARIS PANDUAN KESELAMATAN SIBER

EDISI 1/2021

CONNECT . PROTECT . CONTROL . WIN

#LindungDiriDariJenayahSiber

selsiber.bsep@mod.gov.my

BSEP

GARIS PANDUAN KESELAMATAN SIBER

#LindungDiriDariJenayahSiber

- PENGURUSAN KATA LALUAN
- PENGURUSAN MEDIA SOSIAL & INTERNET
- PENGURUSAN ANTI-VIRUS
- PENGURUSAN SANDARAN MAKLUMAT
- PENGURUSAN PERANTI MUDAH ALIH
- POLISI MEJA DAN SKRIN KOSONG
- PERLINDUNGAN KEJURUTERAAN SOSIAL
- PERLINDUNGAN MAKLUMAT PERIBADI
- PERLINDUNGAN EMEL-PHISHING
- WASPADA JENAYAH SIBER

BAHAGIAN SIBER DAN ELEKTROMAGNETIK PERTAHANAN

PANDUAN KESELAMATAN SIBER

1 PENGURUSAN KATA LALUAN

BSEP

BAHAGIAN SIBER DAN ELEKTROMAGNETIK PERTAHANAN

PENGURUSAN KATA LALUAN

1. Kata laluan perlu kukuh, dilindungi dan dilarang berkongsi dengan orang tidak berkepentingan

2. Tukar kata laluan jika ianya didapati bocor atau dikompromi

3. Gunakan kata laluan sekurang-kurangnya lapan (8) aksara dengan gabungan huruf, nombor dan aksara khas

4. Tukar kata laluan setelah 90 hari atau selepas tempoh masa yang bersesuaian

2 PENGURUSAN INTERNET & MEDIA SOSIAL

BSEP
BAHAGIAN SIBER DAN ELEKTROMAGNETIK PERTAHANAN

1. Pastikan alamat e-mel dan kata laluan rasmi tidak digunakan dalam akaun peribadi media sosial

2. Elakkan berkongsi maklumat peribadi dan maklumat berkaitan tugas rasmi di internet dan media sosial

3. Keluar (*log out*) daripada akaun media sosial jika tidak menggunakannya

4. Elakkan berkongsi maklumat yang tidak diketahui kesahihannya

3 PENGURUSAN PERISIAN ANTI-VIRUS

BSEP

BAHAGIAN SIBER DAN ELEKTROMAGNETIK PERTAHANAN

PENGURUSAN PERISIAN ANTI-VIRUS

1. Peranti perlu dilengkapi dengan perisian anti-virus dan dikemaskini

2. Pastikan konfigurasi perisian anti-virus sentiasa beroperasi dan laksanakan imbasan pada masa yang ditetapkan

3. Pastikan perisian anti-virus sentiasa beroperasi untuk mengesan dan menghapuskan kod berniat jahat

4. Pastikan perisian anti-virus yang digunakan mengikut kesesuaian prestasi peranti

PANDUAN KESELAMATAN SIBER

4 PENGURUSAN SANDARAN MAKLUMAT

BSEP

BAHAGIAN SIBER DAN ELEKTROMAGNETIK PERTAHANAN

1. Membuat sandaran keselamatan ke atas semua sistem perisian dan aplikasi sekurang kurangnya sekali

2. Sandaran hendaklah dilaksanakan mengikut jadual yang dirancang sama ada secara harian, mingguan, bulanan atau tahunan

3. Membuat sandaran ke atas semua data dan maklumat mengikut keperluan operasi

4. Menguji sistem sandaran sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna

PANDUAN KESELAMATAN SIBER

5 PENGURUSAN PERANTI MUDAH ALIH

BSEP

BAHAGIAN SIBER DAN ELEKTROMAGNETIK PERTAHANAN

1. Melabelkan semua peranti mengikut tahap sensitiviti sesuatu maklumat

2. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja

3. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja

4. Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan

6 POLISI MEJA & SKRIN KOSONG

BSEP

BAHAGIAN SIBER DAN ELEKTROMAGNETIK PERTAHANAN

1. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer

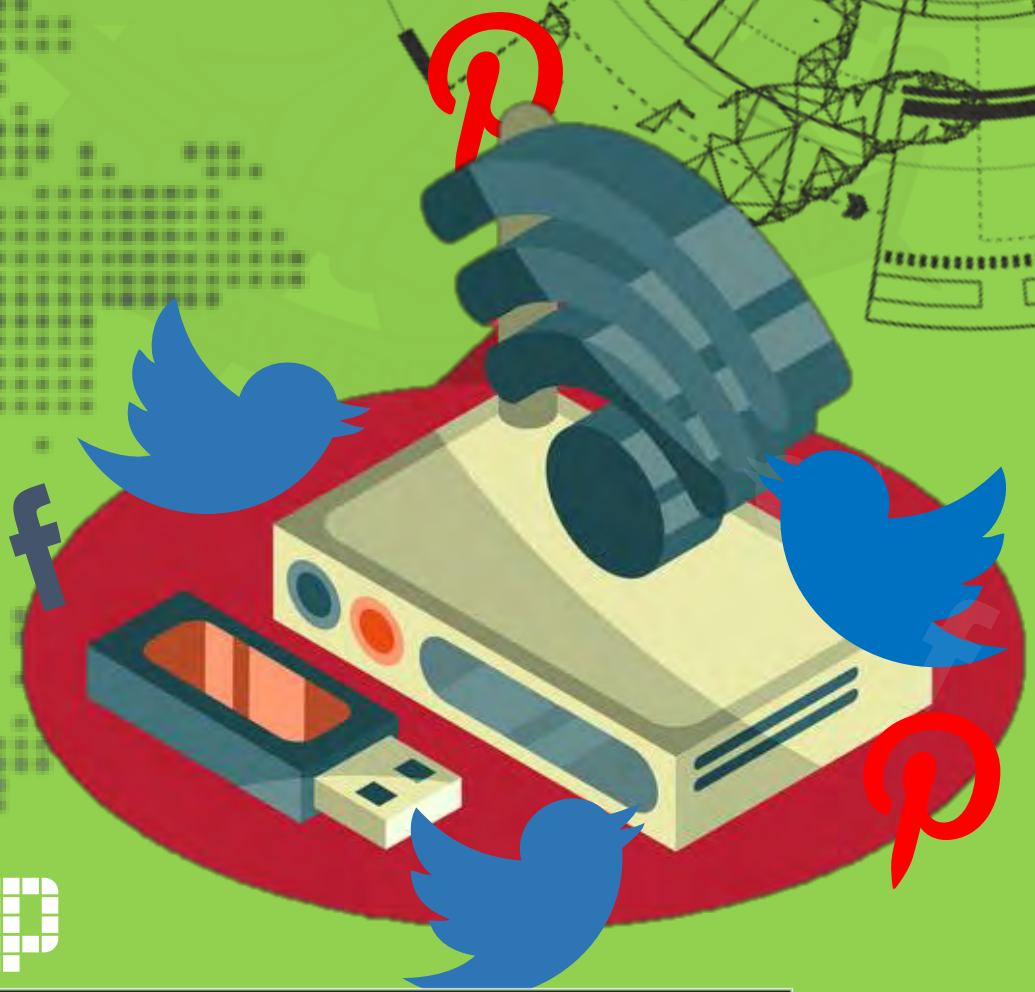
2. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci

3. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat

4. Matikan komputer sekiranya tidak digunakan dalam tempoh yang lama

PANDUAN KESELAMATAN SIBER

7 PELINDUNGAN KEJURUTERAAN SOSIAL



BSEP

BAHAGIAN SIBER DAN ELEKTROMAGNETIK PERTAHANAN

1. Elakkan terima panggilan perkhidmatan pelanggan atau permintaan sokongan e-mel

2. Dilarang melayan panggilan daripada wakil bank yang meminta CCV/PIN/OTP

3. Dilarang mempercayai tawaran hadiah yang ditawarkan oleh orang yang tidak dikenali

4. Dilarang mendedahkan maklumat peribadi melalui panggilan telefon dan di media sosial

PANDUAN KESELAMATAN SIBER

8 PERLINDUNGAN MAKLUMAT PERIBADI

BSEP

BAHAGIAN SIBER DAN ELEKTROMAGNETIK PERTAHANAN

1. Elakkan daripada memuat naik dokumen rasmi Kerajaan dalam *public cloud*

2. Sentiasa sediakan salinan pendua (back up) maklumat digital secara berkala

3. Putuskan sambungan Internet atau wi-fi sekiranya tidak menggunakannya lagi

4. Pastikan perisian anti-virus yang digunakan mengikut kesesuaian prestasi peranti

PANDUAN KESELAMATAN SIBER

9 PERLINDUNGAN EMEL PHISHING

BSEP

BAHAGIAN SIBER DAN ELEKTROMAGNETIK PERTAHANAN

1. Tidak berkongsi *username* dan kata laluan emel rasmi dengan pihak-pihak lain.

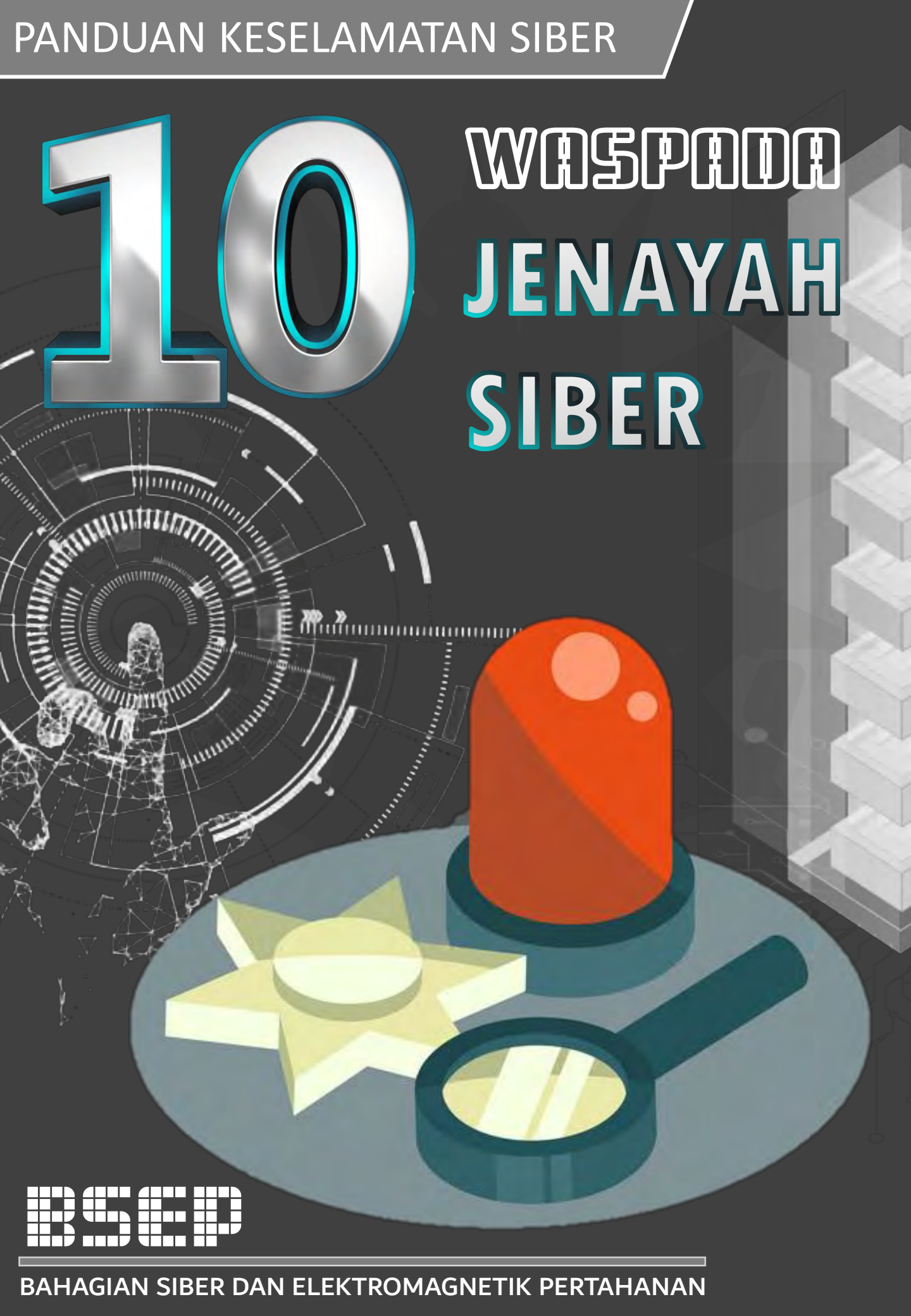
2. Menggunakan emel untuk tujuan kerja-kerja rasmi dan bukan bagi tujuan peribadi

3. Sentiasa melakukan *housekeeping* dengan menghapus emel-emel bersifat spam dan tidak releven

4. Menggunakan kaedah enkripsi dan kata laluan semasa menghantar lampiran maklumat sulit secara emel

PANDUAN KESELAMATAN SIBER

10 WASPADA JENAYAH SIBER



BSEP

BAHAGIAN SIBER DAN ELEKTROMAGNETIK PERTAHANAN

1. Dilarang membenarkan individu lain menggunakan identiti dan kata laluan akaun e-mel dan media sosial

2. Elakkan melayari laman web dan blog yang berunsurkan lucah

3. Dilarang menyebarkan kandungan yang berunsur negatif dan berkongsi maklumat yang tidak diketahui kesahihannya

4. Dilarang mempercayai tawaran atau maklumat daripada individu yang tidak dikenali