KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

Information Security Awareness

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

Pengenalan Keamanan Informasi

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

TUJUAN

Information Security Awareness bertujuan agar semua pegawai Kementerian Keuangan memahami pentingnya keamanan informasi dan tanggung jawab mereka terkait keamanan informasi.

Information Security Awareness bukan hanya tanggung jawab *Top Management*, Tim TIK, maupun Tim Keamanan Informasi saja, namun merupakan tanggung jawab semua pegawai di lingkungan Kementerian Keuangan.

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

Prinsip Keamanan Informasi

Prinsip-prinsip Keamanan informasi terdiri dari:

- ***Confidentiality*** **(Kerahasiaan):** melindungi data dan informasi organisasi dari penyingkapan orang –orang yang tidak berhak
- ***Integrity*** **(Integritas):** melindungi keutuhan data dan informasi organisasi dari modifikasi yang tidak sah
- ***Availability*** **(Ketersediaan):** melindungi ketersediaan data dan informasi organisasi, sehingga data tersedia pada saat dibutuhkan

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

Contoh Penerapan CIA

- Kerahasiaan: data Wajib Pajak harus tertutup untuk umum
- Integritas: data penerimaan negara harus benar, tidak ada modifikasi
- Ketersediaan: data penerimaan negara tersedia saat dibutuhkan

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

Mengapa harus *aware*?

1. **Meningkatnya tren ancaman keamanan informasi di dunia**, misalnya serangan siber semakin canggih dan masif, *ransomware* menyerang setiap 14 detik pada tahun 2019 (sumber: https://techjury.net/)
2. **Tingginya nilai transaksi keuangan pada Kementerian Keuangan** sehingga menjadikan Kemenkeu target serangan siber. Data serangan pada sistem Kemenkeu tahun 2019 adalah sebanyak 2.518.536
3. **Perkembangan teknologi semakin pesat**, menyebabkan peningkatan *cyber crime*. Misalnya *mobile banking*

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

Mengapa harus *aware*?

4. **Tingginya tingkat ketergantungan proses bisnis Kemenkeu terhadap TIK**. Digitalisasi proses bisnis, seperti *Office Automation* Kemenkeu, pelaporan pajak (e-filling), Sistem Perbendaharaan dan Anggaran Negara (SPAN), dan Customs-Excise Information System and Automation (CEISA). Sehingga jika terjadi gangguan terhadap TIK, maka kegiatan bisnis kemenkeu akan terganggu.
5. **IT *literacy* dan *information security awareness* pegawai Kemenkeu masih rendah**, misalnya masih banyak pegawai yang menggunakan *email* non kedinasan, tidak mengganti *password* sejak pertama kali mendapatkan, atau pegawai menggunakan PC yang belum terinstal antivirus.
6. **Masih terdapat sistem informasi yang belum sesuai standar keamanan**, misalkan suatu aplikasi belum lulus uji kerentanan tapi sudah digunakan.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Dampak gangguan keamanan informasi

1. **Terganggunya kegiatan operasional**
   - misalkan aplikasi x terkena serangan *hacking* sehingga *down*, maka proses bisnis yang bergantung pada aplikasi x akan terhenti
   - Perangkat pengguna pada suatu kantor terkena *ransomware* dan menyebabkan kegiatan operasional pada kantor tersebut terganggu
2. **Rusaknya reputasi (*Reputation loss*),**
   - misalkan aplikasi y yang digunakan untuk ekspor impor terganggu sehingga mengganggu proses ekspor impor maka akan menyebabkan rusaknya reputasi penyelenggara aplikasi y
   - Serangan *hacking* pada suatu *website* milik Kemenkeu diketahui oleh masyarakat luas, sehingga merusak reputasi Kemenkeu
3. **Kerugian Finansial (*Financial loss*),**
   - misalnya jika terjadi pencurian sebesar x rupiah untuk setiap transaksi penerimaan negara, maka akan menyebabkan kehilangan financial (penerimaan negara)
   - Layanan Modul Penerimaan Negara terhenti sehingga menyebabkan penerimaan negara tertunda dan kehilangan potensi pendapatan dari bunga penerimaan negara tersebut

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Dampak gangguan keamanan informasi

4. **Kehilangan kekayaan intelektual (*Intellectual property loss*)**
   - Misalnya pencurian hasil penelitian-penelitian
   - Misal *design* sistem informasi dan *source code* aplikasi tersebar kepada pihak lain
5. **Kehilangan kepercayaan dari *stakeholders* (*Loss of stakeholder's confidence*)**
   - Data dan informasi Wajib Pajak tersebar sehingga menyebabkan kepercayaan masyarakat terhadap Kemenkeu hilang
6. ***Opportunity Loss***
   - Misalkan sistem retail SBN *down* maka *opportunity* untuk mendapatkan investasi akan berkurang
   - Layanan Modul Penerimaan Negara terhenti sehingga menyebabkan penerimaan negara tertunda dan kehilangan potensi pendapatan dari bunga penerimaan negara tersebut
7. **Bocornya rahasia negara (*Information Leakage*)**
   - Rancangan RKAKL tersebar ke masyarakat luas
   - Spesifikasi pengadaan tersebar sebelum proses lelang dimulai

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

KEBIJAKAN KEAMANAN INFORMASI DAN SANKSI PELANGGARAN

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

KEBIJAKAN KI

Melaksanakan Kebijakan KI yang telah ditetapkan organisasi

Kebijakan keamanan informasi adalah serangkaian aturan terkait keamanan informasi dalam rangka melindungi keamanan informasi.

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

REGULASI TERKAIT KEAMANAN INFORMASI

a. **Undang-Undang Nomor 11 Tahun 2008** Tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah melalui **UU Nomor 19 Tahun 2016** tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik;
b. **Peraturan Pemerintah Nomor 71 Tahun 2019** tentang Penyelenggaraan Sistem dan Transaksi Elektronik
c. **Perpres Nomor 95 Tahun 2018** tentang Sistem Pemerintahan Berbasis Elektronik (SPBE)
d. **Peraturan Kepala Arsip Nasional Republik Indonesia Nomor 17 tahun 2011** tentang Pedoman Pembuatan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis
e. **Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016** tentang Sistem Manajemen Pengamanan Informasi
f. **Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2018** tentang Penyelenggaraan Sertifikat Elektronik

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

REGULASI TERKAIT KEAMANAN INFORMASI

g. **PMK Nomor 97/PMK.01/2017** tentang Tata kelola Teknologi Informasi dan Keuangan di Lingkungan Kementerian Keuangan

h. **Surat Edaran Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 137 Tahun 2018** tentang Penyebarluasan Informasi Melalui Media Sosial Bagi Aparatur Sipil Negara

i. **Surat Edaran Menteri Keuangan Nomor SE-16/MK.01/2018** tentang Panduan Aktivitas dan Penggunaan Media Sosial Bagi Pegawai Kementerian Keuangan RI

j. **KMK Nomor 942/KMK.01/2019** tentang Pengelolaan Keamanan Informasi Di Lingkungan Kementerian Keuangan

k. **KCIO Nomor KEP-03/SA.5/2013** Tentang Kebijakan dan Standar Penggunaan dan Pengelolaan *Anti Malicious Code* di Lingkungan Kementerian Keuangan.

l. **KCIO Nomor KEP-03/SA.5/2014** : Tentang Pedoman Pengelolaan Perangkat Lunak *Antivirus* di Lingkungan Kementerian Keuangan.

m. **KCIO Nomor KEP-01/SA.5/2015** : Kebijakan *Baseline* Konfigurasi Keamanan Perangkat Teknologi Informasi dan Komunikasi Kementerian Keuangan.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008

Secara umum, materi UU ITE dibagi menjadi dua bagian besar yang terkait keamanan informasi, yaitu:

1. Pengaturan mengenai informasi dan transaksi elektronik termasuk didalamnya mengenai tanda tangan digital
2. Pengaturan mengenai perbuatan yang dilarang, antara lain:
   a) Penggunaan setiap informasi melalui media elektronik yang menyangkut **data pribadi** seseorang tanpa persetujuan Orang yang bersangkutan
   b) mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun dengan sengaja dan tanpa hak atau melawan hukum

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Lanjutan...

d) melakukan **intersepsi atau penyadapan** atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain dengan sengaja dan tanpa hak atau melawan hukum

e) **mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan** suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun.

f) **melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik** dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya dengan sengaja dan tanpa hak atau melawan hukum

Peraturan Pemerintah Nomor 71 Tahun 2019

Materi dalam PP 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik yang terkait keamanan informasi adalah :

1. Penyelenggaraan Sistem Elektronik, antara lain termasuk Penyelenggara Sistem Elektronik, Penempatan Sistem Elektronik dan Data Elektronik, serta Transaksi Elektronik dan Sertifikasi Elektronik
2. Pengelolaan Nama Domain

Peraturan Presiden No 95 Tahun 2018

1. SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE

2. SPBE dilaksanakan dengan prinsip salah satunya adalah keamanan (kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation))

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Peraturan Kepala Arsip Nasional Republik Indonesia Nomor 17 tahun 2011

1. tentang Pedoman Pembuatan Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis
2. Penentuan kategori klasifikasi keamanan:
   a. Sangat Rahasia
   b. Rahasia
   c. Terbatas
   d. Biasa/Terbuka
3. Pengamanan berdasarkan tingkat klasifikasinya (dalam hal penyimpanan dan penyampaian)

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2018

- Permenkominfo No 11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.
- Penyelenggara Sertifikasi Elektronik terdiri atas Penyelenggara Sertifikasi Elektronik Indonesia (Instansi dan Non-instansi) dan Asing.
- Tata Cara Memiliki Sertifikat Elektronik.
- Pengawasan terhadap Penyelenggaraan Sertifikasi Elektronik dilaksanakan oleh Menteri Kominfo.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

PMK Nomor 97/PMK.01/2017

- Pengaturan Tata Kelola TIK di lingkungan Kementerian Keuangan bertujuan untuk memberikan pedoman bagi setiap Unit di Lingkungan Kementerian Keuangan dalam pengelolaan dan pemanfaatan TIK.
- Pengelolaan TIK dimaksud dilaksanakan berdasarkan atas prinsip salah satunya adalah keamanan informasi.
- Prinsip keamanan informasi diterapkan untuk menjami ketersediaan, keutuhan , dan kerahasiaan.
- Dalam mendukung penerapan prinsip keamanan informasi dimaksud maka dibentuk Organisasi Keamanan Informasi.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

KMK Nomor 942/KMK.01/2019

1. Pengelolaan Keamanan Informasi (KI) di lingkungan kemenkeu di terapkan sesuai dengan prinsip KI yaitu menjamin ketersediaan (*availability*), keutuhan (*integrity*), dan kerahasiaan (*confidentiality*).
2. KMK ini mengatur tentang:
   - Sistem Manajemen Keamanan Informasi (SMKI);
   - Penggunaan akun, kata sandi, dan pengelolaan internet dan intranet; dan
   - Penggunaan Sertifikat elektronik.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Sanksi Pelanggaran Keamanan Informasi

Hal : Menjaga informasi dan data Kemeterian Keuangan yang bersifat rahasia

Contoh:

1. Tanpa sengaja menyebar dokumen rahasia kantor saat melakukan foto selfie → merupakan pelanggaran kode etik dengan sanksi moral
2. Sengaja menyebarkan dokumen rahasia kantor → merupakan pelanggaran disiplin dengan Sanksi Hukuman Disiplin berat (dampak negatif pd pemerintah dan/atau negara)

Dasar Hukum:

- PP Nomor 53 Tahun 2010 tentang Disiplin Pegawai Negeri Sipil
- PMK Nomor 29/PMK.01/2007 tentang Pedoman Peningkatan Disiplin Pegawai Negeri Sipil di Lingkungan kementerian Keuangan
- PMK Nomor 190/PMK.01/2018 tentang Kode Etik dan Kode Perilaku
- Pegawai Negeri Sipil di Lingkungan Kemenkeu

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Sanksi Pelanggaran Keamanan Informasi

Pelanggaran terhadap ketentuan pada UU ITE dapat dikenai sanksi pidana sesuai dengan Bab XI KETENTUAN PIDANA.

Contoh:

Pelanggaran terhadap Pasal 33, yaitu “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya” dapat dikenai sanksi pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

PENERAPAN KEAMANAN INFORMASI

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

PENERAPAN KEAMANAN INFORMASI

- Klasifikasi Aset Informasi dan Kerahasiaan Informasi
- Keamanan Fisik
- Keamanan Komputer
- Pengelolaan Kata Sandi (*Password*)
- Penggunaan Intranet dan Internet, Surat Elektronik, WIFI, dan Etika Bersosial Media
- Perangkat Lunak Berlisensi
- Insiden KI dan Kewaspadaan terhadap *Malware* dan *Phising*

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

KLASIFIKASI

- SANGAT RAHASIA
- RAHASIA
- TERBATAS
- PUBLIK

KLASIFIKASI DATA DAN INFORMASI

Mengamankan data dan informasi sesuai dengan tingkat klasifikasinya.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Klasifikasi Data dan Informasi

PMK Nomor 97 Tahun 2017:

Sangat Rahasia: Data Kementerian Keuangan yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian ketahanan ekonomi nasional.

Contoh: Data RAPBN

Rahasia: yaitu Data Kementerian Keuangan yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan Kementerian Keuangan atau mengganggu citra dan reputasi Kementerian Keuangan dan/ atau yang menurut peraturan perundang-undangan dinyatakan rahasia.

Contoh: Data Wajib Pajak; Data Wajib Bayar.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Klasifikasi Data dan Informasi

Terbatas: Data Kementerian Keuangan yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan Kementerian Keuangan tetapi tidak mengganggu citra dan reputasi Kementerian Keuangan.

Contoh: SOP; Laporan Kinerja.

Publik: Data Kementerian Keuangan yang secara sengaja disediakan oleh Kementerian Keuangan untuk dapat diketahui oleh masyarakat umum.

Contoh: Siaran Pers; PMK

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Tabel Pengamanan Dokumen Konvensional

No	Klasifikasi	Pelabelan	Pengguna	Prasarana & Sarana
1	Biasa/ Terbuka	Tidak ada persyaratan dan prosedur khusus	Pengguna yang berasal dari eksternal dan internal yang mempunyai hak akses	Tidak memerlukan prasarana dan sarana khusus
2	Terbatas	Ada persyaratan dan prosedur dengan memberikan cap "TERBATAS" pada fisik dokumen	Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum	Diperlukan tempat penyimpanan yang aman
3	Rahasia	1. Ada persyaratan dan prosedur rahasia dengan memberikan cap "RAHASIA" pada fisik dokumen 2. Tidak sembarangan meletakkan arsip/ dokumen yang bersifat rahasia	Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum	Lokasi aman dengan akses yang terbatas
4	Sangat Rahasia	Ada persyaratan dan prosedur rahasia dengan memberikan cap "SANGAT RAHASIA" pada fisik dokumen	Dibatasi hanya untuk Penentu Kebijakan, Pengawasan, dan Penegak Hukum	1. Disimpan dalam zona yang sangat aman, dengan penelusuran jejak akses 2. Penerapan kebijakan "Meja harus bersih"

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Tabel Pengamanan Dokumen Elektronik (Part 1)

No	Klasifikasi	Pelabelan	Pengguna	Prasarana & Sarana
1	Biasa/ Terbuka	*Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin keaslian dokumen	Pengguna yang berasal dari eksternal dan internal yang mempunyai hak akses	Tidak memerlukan prasarana dan sarana khusus
2	Terbatas	1. *Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin keaslian dokumen 2. File-file elektronik (termasuk *database*) harus dilindungi terhadap penggunaan internal atau oleh pihak-pihak eksternal	1. Autentikasi pengguna (nama pengguna/ *password* atau ID digital) 2. Penggunaan untuk *log in* pada tingkat individual	1. Autentikasi server 2. Langkah-langkah keamanan dengan *Operating System* khusus atau aplikasi khusus 3. *Firewall* dan sistem-sistem serta prosedur-prosedur deteksi terhadap intrusi

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Tabel Pengamanan Dokumen Elektronik (Part 2)

No	Klasifikasi	Pelabelan	Pengguna	Prasarana & Sarana
3	Rahasia	1. *Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin keaslian dokumen 2. File-file elektronik (termasuk *database*) harus dilindungi terhadap penggunaan internal atau oleh pihak-pihak eksternal	1. Hanya staf yang ditunjuk oleh kementerian atau organisasi dan tingkat di atasnya yang dapat mengakses arsip tersebut 2. Autentikasi pengguna (nama pengguna/ *password* atau ID digital) 3. Penggunaan untuk *log in* pada tingkat individual	1. Langkah-langkah keamanan dengan *Operating System* khusus atau aplikasi khusus 2. *Firewall* serta sistem-sistem dan prosedur-prosedur deteksi terhadap intrusi. *Firewall* adalah sistem untuk melindungi komputer atau jaringan dari akses komputer lain yang tidak memiliki hak untuk mengakses komputer atau jaringan kita
4	Sangat Rahasia	1. *Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin keaslian dokumen 2. File-file elektronik (termasuk *database*) harus dilindungi terhadap penggunaan internal atau oleh pihak-pihak eksternal	1. Autentikasi pengguna (nama pengguna/*password* atau ID digital) 2. Penggunaan untuk *log in* pada tingkat individual	1. Autentikasi server 2. Langkah-langkah keamanan dengan *Operating System* khusus atau aplikasi khusus 3. *Firewall* dan sistem-sistem dan prosedur-prosedur deteksi terhadap intrusi.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Prosedur Pengiriman Informasi

No	Klasifikasi	Konvensional	Elektronik
1	Biasa/ Terbuka	Tidak ada persyaratan prosedur khusus.	Tidak ada prosedur khusus.
2	Terbatas	Amplop segel.	Apabila pesan elektronik atau email berisi data tentang informasi personal, harus menggunakan enkripsi, email yang dikirim dengan alamat khusus, password, dan lain-lain
3	Rahasia	1. Menggunakan warna kertas yang berbeda 2. Diberi kode rahasia 3. Menggunakan amplop dobel 4. Amplop segel, stempel rahasia 5. Konfirmasi tanda terima 6. Harus dikirim melalui orang yang sudah diberi wewenang dan tanggung jawab terhadap pengendalian arsip/ dokumen rahasia.	1. Harus ada konfirmasi dari penerima pesan elektronik atau email 2. Menggunakan perangkat yang dikhususkan bagi pesan elektronik atau email rahasia. 3. Menggunakan persandian atau kriptografi.
4	Sangat Rahasia	1. Menggunakan warna kertas yang berbeda 2. Menggunakan amplop dobel bersegel 3. Audit jejak untuk setiap titik akses (misal: tandatangan) 4. Harus dikirim melalui orang yang sudah diberi wewenang dan tanggung jawab terhadap pengendalian arsip/dokumen rahasia.	1. Harus ada konfirmasi dari penerima pesan elektronik atau email 2. Menggunakan perangkat yang dikhususkan bagi pesan elektronik atau email rahasia 3. Menggunakan persandian atau kriptografi 4. Harus ada pelacakan akses informasi untuk suatu pesan elektronik atau email.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

PANDUAN UMUM PENGAMANAN DOKUMEN

Jangan membiarkan dokumen sensitif terbuka

Jangan mencetak dokumen sensitif di printer yang diluar jangkauan

Jangan berbagi informasi sensitif

Jangan melihat informasi sensitif yang bukan kewenangannya

Jangan menyimpan informasi sensitif di luar fasilitas kedinasan

Jangan membuat *sharing folder* dengan akses "*everyone*"

Jangan membuang laporan/informasi tanpa dihancurkan terlebih dahulu

Jangan memberikan aset informasi kepada pihak lain untuk kepentingan di luar kedinasan

Memberikan label/kode kerahasiaan pada amplop pembungkus dokumen sensitif

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Pengamanan Area Kerja

- Gunakan sistem akses keamanan lingkungan seperti *access card, finger print*, dll
- Jangan berbagi akses masuk area kerja
- Area kerja harus terlindungi dari bahaya lingkungan dan akses pihak tidak berwenang
- Jalur keluar masuk area kerja harus dijaga dan dipantau
- Area kerja harus terlindungi dari benda berbahaya dan benda mudah terbakar
- Menerapkan *clear desk* dan *clear screen* pada saat meninggalkan area kerja

  Contoh *clear desk*: Menyimpan dokumen rahasia pada tempat terkunci

  Contoh *clear screen*: Menghapus papan tulis, mematikan atau mengunci (*lock*) komputer.
- Hati-hati terhadap orang asing, misalnya menanyakan ID terhadap orang tak dikenal yang berada di lingkungan kerja
- Membawa pengunjung hanya diruang resepsionis/ ruang tamu
- Waspada terhadap "*tailgating*"

  Tailgating adalah tindakan *bypass access* fisik yang dilakukan dengan cara mengikuti individu yang berwenang untuk memasuki area aman.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

PENGAMANAN PERANGKAT (KOMPUTER)

- Perangkat Pengguna wajib *Join Domain* resmi Kementerian Keuangan
- Pengguna login pada perangkat dengan Akun Domain resmi Kementerian Keuangan
- Pastikan sistem operasi selalu *update* dengan *patch* sistem operasi terbaru
- Perangkat Pengguna menggunakan antivirus dan *signature* versi terbaru

- Aktifkan fitur *lock* pada komputer saat ditinggalkan
- *Backup* berkala untuk data penting

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

PENGAMANAN PERANGKAT (KOMPUTER)

- Matikan komputer ketika meninggalkan kantor
- Waspada terhadap *shoulder surfing,* yaitu metode observasi langsung dengan cara mengintip untuk mendapatkan informasi.
- Hati-hati menyimpan data penting di komputer seperti nomor kartu kredit, atau tanggal ulang tahun dan jangan mengirimkan data penting tersebut melalui pesan instan/*email*

- Konfigurasi komputer yang tidak digunakan dalam 15 menit dibuat mati (*hibernate*/*sleep*) secara otomatis
- Jangan menggunakan *Removable Media* (misal, DVD , HDD external atau USB) yang tidak diketahui pemiliknya ke perangkat pengguna

Perangkat Pengguna termasuk perangkat pribadi yang digunakan untuk kepentingan kedinasan dan mengakses jaringan kemenkeu

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

PENGGUNAAN KATA SANDI (*PASSWORD*)

1. Gunakan kata sandi dengan kriteria:
   - Minimal 8 karakter
   - Kombinasi: huruf kapital, huruf kecil dan angka (0 – 9)
   - Contoh: Kbr7MizU
2. Ganti kata sandi secara berkala, maksimal dalam waktu **180** hari atau dalam hal kata sandi diketahui orang lain
3. Menjaga kerahasiaan Kata Sandi
4. Ubah kata sandi yang telah diberikan oleh Unit TIK Eselon I pada saat pertama kali diberikan

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

PENGGUNAAN KATA SANDI (*PASSWORD*)

Hal-hal yang dilarang dalam penggunaan kata sandi, antara lain:

1. Menggunakan kata sandi yang mengandung:
   - Nama diri/kerabat
   - Tanggal lahir
   - Jabatan kerja
   - Lokasi kerja
   - Alamat rumah
   - Hal pribadi lainnya
   - baik sebagian atau seutuhnya nama akun
2. Menggunakan kata sandi yang mudah ditebak, misalnya Jakarta, Kemenkeu, P@ssw0rd
3. Berbagi kata sandi
4. Menggunakan Akun dan Kata Sandi milik Pengguna lain;

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

PENGELOLAAN KATA SANDI (*PASSWORD*)

6. Menuliskan Kata Sandi dimanapun dan/atau menyimpan Kata Sandi dalam berkas elektronik pada setiap sistem komputer (termasuk perangkat *mobile computing* atau sejenisnya);
7. Membuat Kata Sandi yang sama pada Sistem TIK di lingkungan Kementerian Keuangan dengan Kata Sandi yang digunakan dalam Akun di luar Sistem TIK milik Kementerian Keuangan
8. Mengaktifkan fitur "***remember password***" pada *browser* internet

PENGGUNAAN INTRANET DAN INTERNET

- Menggunakan fasilitas akses Intranet dan Internet secara bijak sesuai dengan tugas, fungsi, dan wewenang;
- Menggunakan fasilitas akses Intranet dan Internet sesuai norma hukum dan etika yang berlaku;

- Menyampaikan pendapat yang bermuatan ujaran kebencian terhadap Pancasila, Undang-Undang Dasar Republik Indonesia Tahun 1945, Bhinneka Tunggal Ika, Negara Kesatuan Republik Indonesia (NKRI), Pemerintah, dan Suku, Agama, Ras, dan Antar Golongan (SARA)
- Mengirimkan dan/atau mempublikasikan konten yang berisi perjudian, pornografi, keasusilaan, ancaman, penghinaan, pemerasan, dan/atau pencemaran nama baik orang lain atau digunakan untuk mengemukan pandangan dan pendapat pribadi (positif maupun negatif) terhadap sesama pegawai, pimpinan, mitra, dan pihak lain yang terkait dengan Kementerian Keuangan
- Melewati ketentuan pembatasan hak akses internet
- Memberikan pendapat pribadi mengatasnamakan Kemenkeu

PENGGUNAAN INTRANET DAN INTERNET

- Menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian bagi individu maupun Kementerian Keuangan
- Menggunakan perangkat lunak yang dapat mengelabui sistem pengendalian/pembatasan akses Internet
- Melakukan kegiatan yang dapat menimbulkan gangguan terhadap Sistem TIK Unit di lingkungan Kementerian Keuangan antara lain menggunakan *tunneling tools*, mengakses laman yang berpotensi mengandung virus, mengakses *video streaming* yang membutuhkan *bandwidth* besar
- Mengunggah, mengunduh, menjalankan *software* berlisensi milik Kemenkeu atau Pihak Ketiga manapun untuk keperluan di luar kedinasan
- Mengungkapkan/menyebarkan informasi milik Kemenkeu yang bersifat sensitif (**terbatas, rahasia, dan sangat rahasia**)

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

PENGGUNAAN INTRANET DAN INTERNET

- Menggunakan **HAKI** pihak lain tanpa persetujuan melalui fasilitas internet Kemenkeu
- Mengakses, mengunggah, mengunduh, dan/atau mempublikasikan situs-situs yang tidak menunjang kedinasan;
- Melakukan kegiatan yang dapat merusak/mencoreng nama baik individu maupun Kementerian Keuangan melalui fasilitas akses Intranet atau Internet;

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

Data penggunaan akses internet Kemenkeu (per minggu)

Top Applications by Bandwidth

#	Application	Bandwidth	Sent	Received
1	YouTube			11.03 TB
2	HTTPS.BROWSER			3.98 TB
3	Google.Accounts			1.46 TB
4	WhatsApp			1.24 TB
5	MS.Windows.Update			1.04 TB
6	Google.Services			993.20 GB
7	Facebook			762.59 GB
8	Instagram			616.71 GB
9	Netflix			309.26 GB
10	HTTP.BROWSER			295.29 GB

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

Data penggunaan akses internet Kemenkeu (per minggu)

Top Applications by Sessions

#	Application	Sessions
1	HTTPS.BROWSER	38,170,456
2	Google.Services	16,152,352
3	QUIC	10,964,518
4	YouTube	9,387,195
5	Google.Accounts	6,285,517
6	Microsoft.Portal	5,465,236
7	HTTP.BROWSER	4,218,518
8	Google.Ads	3,976,701
9	MS.Windows.Update	3,755,418
10	udp/161	3,484,584

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

PENGGUNAAN *EMAIL*

- Menjaga kerahasiaan dan keamanan email miliknya
- Menggunakan email Kemenkeu hanya untuk kepentingan kedinasan secara bijak sesuai dengan tugas, fungsi, dan wewenang;
- Waspada *attachment* dan *email* dari orang asing
- Verifikasi *email* kepada pengirimnya
- Hapus *email spam/junk*
- Waspada terhadap virus
- Pastikan identitas individu dan organisasi penerima email sebelum mengirimkan informasi kedinasan
- Gunakan *e-dropbox* kemenkeu untuk pengiriman file dengan ukuran besar
- Hubungi Service Desk Pusintek / PIC TIK masing-masing unit jika ada hal yang mencurigakan, seperti email spam, pishing, dll

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

PENGGUNAAN *EMAIL*

- Mengirim email yang berisi ancaman, penghinaan , pencemaran nama baik
- Menyampaikan pendapat ke pihak lain dengan mengatasnamakan Kementerian Keuangan melalui email
- Menggunakan email Kemenkeu untuk mailing list, forum diskusi atau sosial media untuk kepentingan pribadi.
- Membuka *email*/*attachment* dari orang asing yang terindikasi dapat mengancam keamanan informasi
- Mengirim informasi pribadi kepada pihak yang tidak dikenal
- Mengirim informasi kedinasan kepada pihak yang tidak berkepentingan
- Mengirim *email* berantai atau *email hoax*
- Mengirim email atas nama pengguna lain.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

PENGGUNAAN WI-FI

- Memperhatikan ketentuan penggunaan intranet dan internet di lingkungan kementerian Keuangan
- Pastikan menggunakan **SSID** yang di sediakan oleh Kementerian Keuangan jika berada di area Kementerian Keuangan
- Tidak memancarkan SSID lain dari perangkat Stand alone Wifi, Handphone, hal ini dapat mengurangi kualitas sinyal yang dipancarkan oleh SSID yang di kelola Unit TIK.
- Jangan terhubung dengan SSID yang tidak dikenal. Jika dalam keadaaan mendesak, hal-hal yang perlu diperhatikan saat menggunakan ***free*** wifi anatara lain:
  - Tidak mengakses aplikasi sensitif misalnya aplikasi kedinasan atau *mobile banking*
  - Jangan menginput data rahasia (*password*, pin akun bank, *login administrator*, dll) pada sembarang situs
  - Gunakan layanan keamanan dasar seperti antivirus

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Etika Bermedia Sosial

Berikut ini himbauan penyebarluasan informasi melalui media sosial khususnya terkait keamanan informasi:

1. Menjaga kerahasiaan yang menyangkut kebijakan negara, memberikan informasi secara benar dan tidak menyesatkan kepada pihak lain yang memerlukan informasi terkait kepentingan kedinasan.
2. Tidak menyalahgunakan informasi intern negara untuk mendapat atau mencari keuntungan atau manfaat bagi diri sendiri atau untuk orang lain.
3. Memastikan bahwa informasi yang disebarluaskan jelas sumbernya, dapat dipastikan kebenarannya dan tidak mengandung unsur kebohongan.

Sesuai dengan SE MenPAN-RB Nomor 137 Tahun 2018

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Etika Bermedia Sosial

Berikut ini himbauan etika bermedia sosial terkait Keamanan Informasi:

1. Melakukan pengaturan privasi (identitas dan unggahan) di berbagai *platform* media sosial untuk menjaga keamanan informasi
2. Membuka media sosial secara berkala untuk memastikan akun media sosial tidak disalahgunakan
3. Hindari membagi identitas pribadi seperti alamat lengkap, no telepon , *email* pribadi/kantor, atau tanggal lahir. Jika diperlukan lakukan komunikasi privat dalam saluran terpercaya
4. Tidak menggunakan alamat *email* kantor untuk mendaftar media sosial kecuali untuk keperluan resmi kantor
5. Segera komunikasikan ke tim terkait sambil berupaya mengamankan kembali akses ke akun media sosial anda jika kehilangan akses ke akun media sosial

Sesuai dengan SE MenKeu No 16 Tahun 2018

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

PERANGKAT LUNAK BERLISENSI

- Gunakan *software* yang direkomendasikan oleh Unit TIK
- Gunakan *software* milik Kemenkeu untuk kedinasan
- Pastikan membaca dan memahami *End User License Agreement* untuk pemasangan *software*
- Menghubungi PIC TIK untuk instalasi *software*

- Menginstal dan menggunakan *software* yang tidak direkomendasikan
- Menggunakan *software* Kemenkeu untuk kepentingan pribadi

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Software yang tidak direkomendasikan pada perangkat pengguna

No	Klasifikasi	Contoh
1	Perangkat lunak yang melanggar hak cipta (bajakan dan cracking)	Bajakan: Nitro Pro, Corel, Photosop (tidak berlisensi) Cracking: KMSpico, IDM crack
2	Perangkat lunak yang tidak mendukung kedinasan	Game, Chat (Snapchat, Discord)
3	Perangkat lunak yang digunakan untuk aktifitas hacking/ exploit celah keamanan	network scan, Angry IP, Advanced IP Scanner, nexpose, wireshark, Nmap, metasploit, dll
4	Perangkat lunak yang sudah tidak disupport	Windows XP, Windows Server 2003, Windows Server 2008, Windows 7, dll
5	Perangkat lunak yg digunakan untuk remote access	Ultra VNC, Teamviewer, RemotePC, Hotspot Shield, VNC viewer, VNC server, TightVNC, dll
6	Perangkat lunak yang digunakan untuk upload dan download secara ilegal	uTorrent, dll
7	Perangkat lunak yang digunakan untuk mendukung koneksi privat yang tidak sah	FlyVPN, Profixier, SoftetherVPN Client, Open VPN, Tor, Proxifier, dll

professional · responsive · innovative · modern · enthusiastic

Sumber: Hasil Audit ITJEN

INSIDEN KEAMANAN INFORMASI

- Mencatat semua rincian penting gangguan dengan segera, seperti jenis pelanggaran, jenis kerusakan, pesan pada layar, atau anomali sistem
- Segera melaporkan gangguan ke Service Desk, PIC TIK masing-masing unit, atau Petugas Keamanan Informasi (KI) masing-masing unit
- Petugas KI berkoordinasi dengan Gov-CSIRT Indonesia (BSSN) dalam menangani gangguan keamanan informasi

- Membicarakan insiden keamanan dengan siapa pun di luar organisasi maupun di tempat umum
- Menghambat atau mencegah pegawai lain melaporkan insiden keamanan informasi

Contoh usaha penerobosan yang perlu diwaspadai Pengguna, antara lain:

- *Ransomware*
- *Phising*
- *Social Engineering*

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

RANSOMWARE

Ransomware adalah salah satu bentuk *malware* dengan metodologi *cryptovirology*, yang mengancam untuk menyebarkan data atau memblok semua akses ke dalam data tersebut jika pemilik data tidak memberikan sejumlah uang tebusan.

Langkah-langkah Pencegahan & Penanganan:

- Jangan menginstall *software* tidak berlisensi/*software* dari sumber yang tidak terpercaya.
- Jangan mengunduh *attachment* dari pengirim yang tidak dikenal.
- Pembatasan akses *sharing folder*
- Lakukan *backup* secara berkala
- Putuskan jaringan perangkat yang terindikasi *ransomware*
- Laporkan kepada Service Desk dan PIC TIK masing-masing unit

PHISING

Phising adalah suatu metode yang di gunakan *hacker* untuk mencuri *password* dengan cara mengelabui target menggunakan *fake form login* pada situs palsu yang menyerupai situs aslinya.

Berikut adalah contoh phising dengan menggunakan fake form login dengan situs yang menyerupai situs asli:
Situs internet *banking* BCA, **http://www.klikbca.com**, seperti:
– kilkbca.com
– clikbca.com
– klickbca.com
– klikbac.com
– wwwklikbca.com

Contoh *phising* melalui *link* yang dikirimkan melalui *email*

From: Kementerian Keuangan Admin Helpdesk <134014001@iitb.ac.in>
Sent: Thursday, March 7, 2019 10:29 AM
Subject: Pembaruan Akun

Attn: Pemilik Akun Email Kementerian Keuangan yang terhormat
Diamati bahwa akun email Anda baru-baru ini masuk dengan alamat IP yang tidak dikenal: 72.240.180.228 dan akan ditutup karena melanggar syarat dan ketentuan. Anda tidak akan dapat mengirim dan menerima email dan akun email Anda akan dihapus dari server.

silakan KLIK DI SINI untuk memvalidasi dan memverifikasi akun email Anda

Kegagalan untuk mematuhi akan mengakibatkan penghentian akun email Anda.

Salam,
Kementerian Keuangan admin helpdesk

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Pencegahan dan Penanganan *Phising*

1. Pastikan mengakses halaman *website* yang benar. Periksa tanda keamanan (gambar Gembok terkunci) untuk memastikan *website* yang diakses adalah benar. Tanda tersebut akan memberikan informasi pemilik *website* yang sebenarnya.
2. Jangan pernah membuka halaman dari *link* yang dikirimkan melalui surat, *email*, sms atau media lain yang sumbernya tidak jelas.
3. Jaga selalu kerahasiaan *user id*, *password*, serta data pribadi lain. Jangan pernah memberikan atau memasukkan data tersebut ke program aplikasi yang tidak terpercaya.
4. Pastikan menggunakan media komputer yang aman, tidak dari tempat publik atau media lain yang keamanan transaksinya tidak terjamin.
5. Laporkan kepada Unit TIK atau *Service Desk* Kementerian Keuangan jika menemukan halaman *website* yang terindikasi pishing.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA

Social Engineering

- *Social engineering* adalah kegiatan untuk mendapatkan informasi rahasia/penting dengan cara menipu pemilik informasi tersebut
- *Social engineering* mengkonsentrasikan diri pada rantai terlemah sistem jaringan komputer, yaitu MANUSIA.

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA