HEBAHAN KESEDARAN
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
ISO/IEC 27001:2022

CLEAR SCREEN & CLEAR DESK POLICY

SIMPAN DOKUMEN SENSITIF

Pastikan semua dokumen rasmi atau maklumat sensitif disimpan dalam laci atau kabinet yang boleh dikunci apabila tidak digunakan.

PASTIKAN TIADA BAHAN TERTINGGAL

Jangan tinggalkan dokumen sensitif, fail, atau bahan bercetak di atas meja, terutamanya berhampiran pencetak, pengimbas atau mesin faks.

LUPUSKAN DENGAN SELAMAT

Buang dokumen yang tidak lagi diperlukan secara selamat, seperti dengan menggunakan mesin pencarik (*shredder*).

KUNCI SKRIN

Kunci skrin komputer anda setiap kali anda meninggalkan meja, walaupun hanya untuk seketika.

LOG KELUAR

Log keluar daripada akaun anda jika anda akan meninggalkan komputer untuk tempoh yang lama.

GUNAKAN SKRIN KUNCI AUTOMATIK

Manfaatkan *feature* skrin kunci automatik atau *screensover* yang memerlukan kata laluan untuk membuka semula.

HEBAHAN KESEDARAN

SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) ISO/IEC 27001:2022

TIPS

KENALPASTI E-MEL PALSU

TIP 1

E-mel tidak mengandungi ucapan salam atau maklumat untuk penerima hubungi.

TIP 2

E-mel tersebut mengandungi kesalahan ejaan atau tatabahasa yang jelas.

TIP 3

E-mel meminta penerima untuk klink pautan log masuk atau kongsi maklumat peribadi seperti kad kredit atau kata laluan.

TIP 4

E-mel tersebut boleh menimbulkan rasa cemas atau rasa terancam kepada penerima sekiranya penerima tidak bertindak.

TIP 5

Maklumat pengirim tidak sesuai dengan maklumat organisasi yang dinyatakan di dalam e-mel.

ASAS KESELAMATAN

SelGDX
Selangor Government Data Exchange
SELAMAT . CEPAT . TEPAT

Menjamin KESELAMATAN perkongsian data dengan infrastruktur yang SELAMAT

- SUMBER DATA
- REKOD TRANSAKSI
- KAWALAN DATA
- PEMBAHARUAN KUNCI
- SETUJU KONGSI DATA
- KERAHSIAAN DATA

SelGDX dilancarkan sebagai langkah strategik untuk menyokong agenda **Transformasi Digital Negeri yang memacu inovasi digital dan menyokong usaha Kerajaan Negeri Selangor ke arah membina sebuah kerajaan pintar yang inklusif, responsif dan berasaskan data.**

SelGDX berteraskan prinsip data perlu dilindungi dan dipelihara kerahsiaan/privasi bagi menjamin keselamatan data. Amalan perkongsian dan perlindungan data yang efisien dapat menangani ancaman dan risiko keselamatan siber seperti penggodaman, pencerobohan sistem, ketirisan data dan serangan virus.

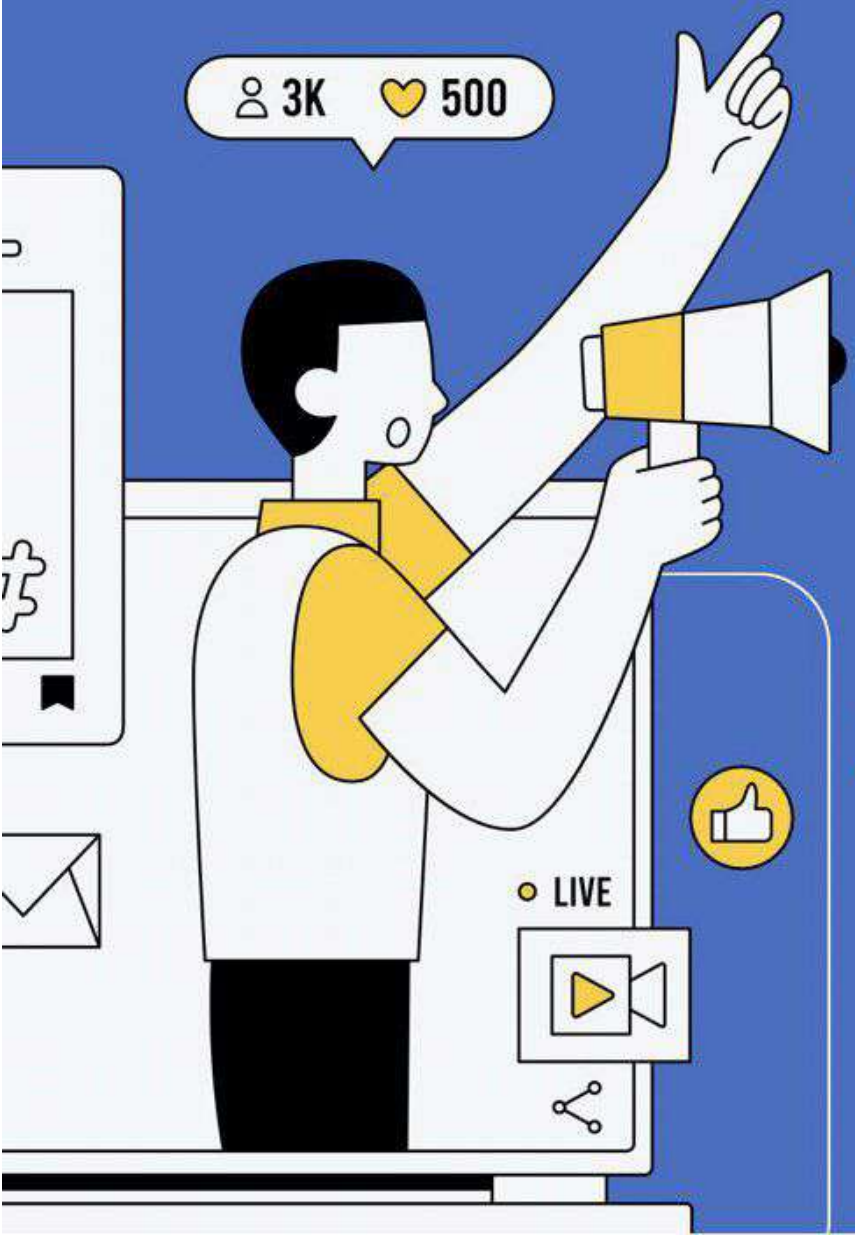
PEJABAT SETIAUSAHA
KERAJAAN NEGERI SELANGOR

3 Langkah Penting

Memantau Keselamatan SIBER

1 Pendidikan Ancaman Semasa

Tingkatkan pengetahuan pekerja anda tentang ancaman siber semasa seperti phishing, malware, dan serangan penipuan. Berikan latihan berkala untuk mengenal pasti isyarat bahaya dan langkah pencegahan yang tepat



2 Penyemakan Berkala Data

Laksanakan audit keselamatan data secara berkala untuk mengesan dan menilai potensi kerentanan atau celah dalam sistem.

3 Pemantauan Aktiviti Rangkaian

Pantau secara aktif aktiviti rangkaian untuk mengesan aktiviti yang mencurigakan atau tidak dibenarkan.