

TATA KELOLA CYBER SECURITY

pada pemerintahan daerah



PERMASALAHAN

Perkembangan teknologi komunikasi melalui media maya (cyber), harus disertai dengan kesadaran terhadap potensi ancaman kejahatan (cybercrime).

Contoh kegiatan cybercrime:



pencurian data
(sumber daya informasi)



pembajakan akun
(email, social network)



malware/malicious
code, fraud, spionase



cyber warfare
(perang di dunia maya)

Tata kelola cyber security sangat diperlukan oleh pemerintah daerah, terutama jika terkait dengan pengembangan e-government, demi terciptanya pelayanan publik yang baik dan berbasis online.

KEGUNAAN CYBER SECURITY

pada pemerintahan daerah



mengamankan hal
terkait KEPEMILUAN

- penyalahgunaan medsos
- *black campaign*
- *real count* Pilkada
- peningkatan partisipasi
- sosialisasi



mencegah POTENSI
KONFLIK dari medsos

- potensi konflik di facebook
- terbawa ke kehidupan nyata
- konten muatan SARA
- hoax
- *hate speech*



meningkatkan
PELAYANAN PUBLIK

- menjaga otensitas informasi
- menjaga kerahasiaan informasi yang termasuk dalam kategori informasi yang dikecualikan



E-COMMERCE



DIPLOMASI
INTERNASIONAL

REKOMENDASI



Penataan Cyber Security

- menambah SDM berkompeten
- peningkatan anggaran pembangunan keamanan siber
- penyediaan perangkat teknologi modern
- membentuk peraturan terkait sistem keamanan siber skala nasional.



Penguatan Kapasitas Teknologi Informasi

anggota KPU & Bawaslu harus memahami bahwa TI agar dapat terjadi sinkronisasi data kependudukan dengan data pemilih, pengamanan data pemilihan, serta mencegah penyalahgunaan media sosial.



Pengembangan Political Will di Pemerintah Daerah

- pencerdasan masyarakat untuk menangkal hoax
- mencegah provokasi di media
- mengembangkan sistem pemerintahan berbasis online

