

SISTEM MANAJEMEN KEAMANAN INFORMASI (ISMS)

1

KERAHASIAAN DATA

Informasi sensitif, termasuk data pribadi dan catatan perusahaan, harus dilindungi kerahasiaannya. Informasi rahasia tidak boleh dibagikan, diakses, atau diungkapkan kepada pihak yang tidak berwenang kecuali telah memperoleh persetujuan yang sah dan diperlukan untuk kepentingan pekerjaan.



INTEGRITAS DATA

Keakuratan, kelengkapan, dan konsistensi data harus dijaga setiap saat. Seluruh proses pembaruan, penyimpanan, penggunaan, dan transmisi informasi wajib mengikuti prosedur yang telah ditetapkan guna mencegah perubahan data yang tidak sah atau tidak disengaja.

2

3

PENGENDALIAN AKSES

Gunakan kata sandi yang kuat dan memperbaruinya secara berkala. Kredensial akun, termasuk username dan password, dilarang untuk dibagikan kepada pihak lain. Akses terhadap sistem, aplikasi, dan data hanya diperbolehkan sesuai dengan otorisasi dan kebutuhan pekerjaan masing-masing.



KEAMANAN FISIK

Perangkat kerja harus diamankan ketika tidak digunakan, termasuk dengan mengunci workstation atau perangkat kerja. Setiap akses tidak sah atau aktivitas mencurigakan harus segera dilaporkan kepada pihak yang berwenang.

4

5

PELAPORAN INSIDEN

Seluruh dugaan maupun kejadian insiden keamanan informasi wajib segera dilaporkan kepada tim IT atau pihak yang ditunjuk tanpa penundaan. Pelaporan yang cepat membantu perusahaan dalam melakukan penanganan, mitigasi risiko, dan pencegahan dampak yang lebih luas.



EMAIL & INTERNET

Hindari membuka tautan, lampiran, atau pesan dari sumber tidak dikenal. Jangan mengunduh file atau perangkat lunak yang tidak terverifikasi karena dapat membahayakan keamanan informasi perusahaan.

6