Yasinta Desty Natalia (20230801033)
**UTS KJ002- KEAMANAN INFORMASI**
**20 Mei 2025- Take Home**

---

1. Apa itu keamanan informasi
   Keamanan informasi adalah Tindakan nyata yang terstruktur dengan baik untuk melindugi suatu informasi atau data yang bersifat privasi dan sensitive dari penyalahgunaan dan gangguan yang berasal dari luar dan tidak memiliki ijin resmi.

2. Apa itu confidentiality, integrity, dan availability
   - Confidentiality (kerahasiaan)
     Adalah Tindakan aksi melindungkan informasi dan data penting yang bersifat privasi dan rahasia agar pihak luar tidak memiliki akses dan peluang untuk masuk secara ilegal
   - Integrity adalah Tindakan untuk menjaga agar data atau informasi tidak dapat dimanipulasi, diubah atau diedit oleh pihak yang tidak punya wewenang. Pada kasus ini, penyeludup bukan hanya bisa masuk saja, melainkan sudah bisa memainkan data rahasia jika tidak dilakukan Tindakan penjagaan.
   - Availability (ketersediaan) adalah upaya untuk memastikan sistem dan data tetap bisa digunakan oleh pihak yang memiliki akses dan kewenangan. Dari Tindakan ini diharapkan pihak berwenang dapat mengakses tanpa gangguan saat digunakan dalam waktu genting maupun tidak

3. Jenis-jenis kerentanan
   Kerentanan dapat muncul dari banyak pihak, baik fisik hingga non-fisik.
   - Kerentanan software bersifat virus yang menyerang system informasi maupun aplikasi itu sendiri yang mempengaruhi system dan data rahasia. Virus ini dapat berasal dari kontak fisik antar perangkat atau melalui pesan dan situs.
   - Kerentanan system informasi yang menyerang system bekerja sehingga aka nada penolakan dalam layanan system
   - Kerentanan jaringan dengan Tindakan mencuri dan mengakses data secara illegal melalui jaringan yang menjadi transportasi data saling bertukar
   - Kerentanan manusia dalam menerima link illegal ataupun memberikan password atau akses rahasia kepada orang yang tidak berwenang secara sadar maupun tidak sadar
   - Kerentanan fisik melalui akses fisik yang tidak sah ke perangkat keras atau infrastruktur IT
   - Kelalaian dalam konfigurasi seperti ijin file yang tidak sesuai yang menyebabkan pengaturan perangkat lunak dan keras mempunyai celah untuk penyusup
   - Serangan membajiri traffic agar system dan jaringan bermasalah dan bug

4. Apa itu hash and encryption
   - **Hashing** adalah Tindakan permanen yang satu arah untuk mengubah data menjadi kode unik, hal itu untuk memastikan pengintegrasian data. Pengaplikasiannya seperti dalam password yang bersifat random dan Panjang yang berisi rangkuman data
   - enkripsi adalah proses mengubah data menjadi format yang tidak terbaca (ciphertext) dengan pengacakan data menjadi kode yang dapat dikembalikan ke bentuk aslinya dengan kunci dekripsi yang unik

5. Apa itu session dan authentication
   - Authentication adalah proses dimana seorang user diverifikasi identitasnya untuk memastikan suatu pihak memiiki akses dan wewenang. Contoh sederhana seperti verifikasi email dan password Ketika mau login
   - **Session** adalah periode waktu jangka pendek (tidak permanen) dalam menyimpan data pengguna sedari berhasil login, sampai logout atau session-nya expired.

6. Apa itu privacy dan ISO
   - Privacy (Privasi) adalah hak seseorang atau sekumpulan orang untuk mengendalikan dan mengamankan informasi pribadi pribadinya agar tidak meserang secara fisik ataupun nonfisik oleh pihak yang tidak berwenang. Privasi dapat mengatur bagaimana data tersebut dikumpulkan, disimpan, digunakan, dan dibagikan.
   - ISO (International Organization for Standardization) adalah lembaga internasional yang mengatur standar-standar internasional di berbagai bidang agar sesuai dengan peraturan yang ada dan tidak ada penyimpangan, hal ini termasuk untuk keamanan informasi. ISO 27001 merupakan standar untuk Information Security Management System. ISO 27001 berisi standar pengelolaan siklus peningkatan kapabilitas keamanan informasi.