**NIM : 512121230007**

**NAMA : TEGUH AGUNG PRABOWO**

**JURUSAN : SISTEM INFORMASI**

**MATAKULIAH : MANAJEMEN TEKNOLOGI INFORMASI**

**Sebutkan dan jelaskan secara prinsip tujuan utama organisasi atau perusahaan dalam menerapkan kebijakan keamanan informasi ?**

**Jawab :**

Manajemen Keamanan Informasi Di Perusahaan. Banyak organisasi yang memanfaatkan perangkat teknologi informasi berbasis jaringan baik local maupun global untuk mendukung tujuan pengembangan organisasinya. Namun banyak yang tanpa disadari mengimplementasikan sistem jaringan computer tersebut tanpa dibarengi dan diimbangi dengan sistem keamanan yang memadai sesuai dengan standar keamanan yang berlaku. Hal itu dikarenakan karena banyak yang tidak menggunakan prinsip­-prinsip pengamanan sesuai standar, dan dalam mengimplementasikan tidak melalui tahap siklus hidup keamanan informasi.

Keamanan informasi dimaksudkan untuk mencapai kerahasiaan, ketersediaan, dan integritas di dalam sumber daya informasi perusahaan. Manajemen keamanan informasi terdiri dari:

1. Perlindungan Sehari-hari disebut Manajemen Keamanan Informasi (information security management/ ISM)
2. Persiapan untuk menghadapi operasi setelah bencana disebut Manajemen Kesinambungan Bisnis (business continuity management /BCM)

**Tujuan Keamanan Informasi**

Keamanan informasi dimaksudkan untuk mencapai tiga sasaran utama, yaitu:

* Kerahasiaan: melindungi data dan informasi perusahaan dari penyingkapan orang –orang yang tidak berhak
* Ketersediaan: meyakinkan bahwa data dan informasi perusahaan hanya dapat digunakan oleh orang yang berhak menggunakannya.
* Integritas: sistem informasi perlu menyediakan representasi yang akurat dari sistem fisik yang direpresentasikan

**Manajemen Keamanan Informasi**

Manajemen keamanan informasi menjadi penting diterapkan agar informasi yang beredar di perusahaan dapat dikelola dengan benar sehingga perusahaan dapat mengambil keputusan berdasarkan informasi yang ada dengan benar pula dalam rangka memberikan layanan yang terbaik kepada pelanggan. ISM terdiri dari empat langkah:

* Identifikasi threats (ancaman) yang dapat menyerang sumber daya informasi perusahaan
* Mendefinisikan resiko dari ancaman yang dapat memaksakan
* Penetapan kebijakan keamanan informasi
* Menerapkan controls yang tertuju pada resiko

**Ancaman**

* Ancaman keamanan informasi adalah seseorang, organisasi, mekanisme, atau peristiwa yang dapat berpotensi menimbulkan kejahatan pada sumber daya informasi perusahaan
* Ancaman dapat berupa internal atau external, disengaja atau tidak disengaja

**Resiko**

Tindakan tidak sah yang menyebabkan resiko dapat digolongkan ke dalam empat jenis :

* Pencurian dan Penyingkapan tidak sah
* Penggunaan Tidak Sah
* Pembinasaan dan Pengingkaran Layanan yang tidak sah
* Modifikasi yang tidak sah

**Kebijakan Keamanan Informasi**

Sebuah  kebijakan keamanan infomasi bisa diimplementasikan menggunakan 5 pendekatan dibawah ini:

* Tahap 1: Pengenalan project.
* Tahap 2 Pengembangan kebijakan
* Tahap 3: Konsultasi dan penyetujuan
* Tahap 4: Kesadaran dan pendidikan
* Tahap 5: Penyebaran kebijakan

**Kontrol**  
Kontrol adalah mekanisme yang diimplementasikan untuk melindungi perusahaan dari resiko-resiko dan meminimalisir dampak dari resiko yang terjadi:

* Technical control teknis dibangun didalam sistem oleh sistem pengembang sementara proses pengembangan berjalan.
* Access control adalah dasar keamanan melawan ancaman oleh orang-orang yan tidak berkepentingan langsung/terkait.
* Intrusion detection systems akan mencoba mencari tahu satu percobaan yang dilakukan ntuk menerobos keamanan sebelum menimbulkan kerusakan