SILABUS

Mata Kuliah : **Keamanan Sistem Informasi**
Kode/bobot/Semester : **ISH3G4 / 4 sks / Semester 6**

Capaian Pembelajaran Matakuliah (CP-MK):

Setelah mengikuti matakuliah ini mahasiswa:

1. Mampu berkomunikasi antar personal baik dalam bentuk diskusi dan presentasi yang efektif (KH.3);
2. Mampu berpikir analitis, kritis, dan kreatif dalam menyelesaikan permasalahan di bidang Sistem Informasi (KH.1);
3. Mampu melakukan proses evaluasi diri terhadap kelompok kerja yang berada dibawah tanggung jawabnya, dan mampu mengelola pembelajaran secara mandiri; (KU.8);
4. Mampu bertanggungjawab atas pencapaian hasil kerja kelompok dan melakukan supervisi dan evaluasi terhadap penyelesaian pekerjaan yang ditugaskan kepada individu yang berada di bawah tanggungjawabnya; (KU.7)
5. Menyusun deskripsi saintifik hasil kajian dalam bentuk laporan tugas akhir, dan mengunggahnya dalam laman perguruan tinggi;(KU.4)
6. Mampu menunjukkan kinerja mandiri, bermutu, dan terukur; (KU.2)
7. Mampu menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi IPTEK yang memperhatikan dan menerapkan nilai humaniora yang sesuai dengan bidang keahlian Sistem Informasi; (KU.1)
8. Menguasai konsep dasar keamanan sistem informasiuntuk mendukung strategi pemanfaatan sistem informasi dan untuk memenuhi kebutuhan bisnis organisasi. (P.6)
9. Mempunyai keahlian dalam melakukan evaluasi terhadap kepatuhan perusahaan terhadap standar keamanan informasi dan memberikan rekomendasi terhadap pemanfaatan keamanan informasi sesuai dengan kebutuhan bisnis untuk bersaing secara global.(K.4)

Kemampuan yang direncanakan tiap tahapan belajar (Sub-CP-MK):

Setelah mengikuti matakuliah ini mahasiswa:

1. mampu menjelaskan pengertian, latar belakang, fungsi keamanan sistem informasi;
2. mampu menjelaskan konsepvulnerabilities dan ancaman keamanan;
3. mampu menjelaskan konsep resiko dan kendali keamanan;
4. mampu menjelaskan konsep kriptografi dan contoh implementasinya;
5. mampu menjelaskan dan mengimplementasikan berbagai kendali akses dan manajemen identitas;
6. mampu menjelaskan dan menggunakan strategi keamanan jaringan, implementasi dan sistem keamanan jaringan;
7. mampu menjelaskan konsep keamanan host;
8. mampu menjelaskan konsep keamanan data;
9. mampu menjelaskan konsep dan berbagai aspek keamanan aplikasi berbasis web dan cloud;
10. mampu menjelaskan keamanan operasional;
11. mampu menjelaskan pengelolaan keamanan dan kepatuhan pengelolaan;
12. mampu menjelaskan manajemen resiko keamanan dan kontinuitas bisnis (pemulihan dari bencana)
13. mampu menjelaskan pengelolaan respon insiden dan forensik;
14. mampu menjelaskan kebijakan keamanan dan program pelatihan keamanan;

Pokok Bahasan (*Subject Matter*):

Pengertian dan fungsi kemanan informasi, yang mencakup pengertian dan fungsi ancaman dan kontrol keamanan, kriptografi dan kendali akses, keamanan jaringan, keamanan host, data dan aplikasi. Juga membahas pengelolaan keamanan yang mencakup keamanan operasional. Implementasi keamanan informasi menggunakan berbagai studi kasus pada berbagai platform. Implementasi ini berupa praktikum pada laboratorium yang memungkinkan pengujian berbaga kasus, misalnya eksekusi malware, atau skenario penyerangan. Sedangkan dari sisi obyek, kelemahan dan ancaman diarahkan untuk menerapkan kontrol keamanan yang tepat.

Pustaka Utama:

1. GTS Learning,"CompTIA Security+ SY0-041 : Official Study Guide", 2015

KomponenNilaiAkhir:

UAS 25%, Praktikum 30%, Tugas 25%, UTS 20%