MANUAL KEBIJAKAN KEAMANAN INFORMASI ISO 27001:2013

Authored by: ***Malikhah*** *[malikhah@staf.unair.ac.id]*

Pengesahan

Manual Keamanan Informasi disahkan oleh Direktur Direktorat Sistem Informasi, UNIVERSITAS AIRLANGGA

Manual Keamanan Informasi merupakan :

1.Pedoman pelaksanaan kerja di jajaran Direktorat Sistem Informasi - UNIVERSITAS AIRLANGGA, yang mencakup seluruh kebijakan untuk dipahami, dipatuhi, dan dipergunakan oleh setiap seksi kerja dan sebagai acuan dalam pengelolaan keamanan informasinya.

2.Acuan bagi Direktorat Sistem Informasi (DSI) dalam melaksanakan kebijakan Universitas Airlangga (UNAIR), khususnya terkait Keamanan Informasi.

3.Acuan bagi penyedia layanan sistem informasi (service provider) dan rekanan bisnis (business partner atau alliance) dalam mensinergikan standar yang digunakan.

4.Suatu dokumen yang bersifat dinamis dan selalu dikembangkan dan dimutakhirkan secara periodik untuk disesuaikan dengan kebutuhan.

Bagi seluruh Pegawai Pimpinan dijajaran DSI-Universitas Airlangga bertanggung jawab atas tercapainya pelaksanaan implementasi dari manual ini di seksi kerjanya.

Surabaya,

UNIVERSITAS AIRLANGGA

DIREKTORAT SISTEM INFORMASI

Direktur,

Dr.Ir. SOEGIANTO SOELISTIONO, M.Si.

Daftar Distribusi

DAFTAR PEMEGANG MANUAL KEAMANAN INFORMASI

No	Jabatan	Code	No. Ordner	Bahasa
1	Direktur Direktorat Sistem Informasi	DIR	ORG.03.29.01	Indonesia
2	Kepala Sub Bagian	SUB	ORG.03.29.02	Indonesia

CATATAN Mengenai Revisi

Identitas Dokumen		Uraian Perubahan	Disahkan	
Nomor	Tanggal		Tanggal	Oleh

daftar Istilah

Dalam Manual Keamanan Informasi ini yang dimaksud dengan :

No	Istilah	Definisi
1.	*Activity Log*	Catatan yang menerangkan kegiatan pengguna atau sistem dalam periode tertentu untuk suatu proses kegiatan sistem informasi.
2.	Administrator	Pegawai yang bertanggung jawab secara teknis terhadap kelancaran operasional sistem aplikasi atau infrastruktur sistem informasi.
3.	Akuisisi	Suatu proses penyediaan sistem aplikasi atau infrastruktur informasi dengan pengadaan dari pihak ketiga melalui mekanisme pengadaan yang berlaku dalam DSI-Universitas Airlangga .
4.	Akses	Perbuatan memasuki, memberikan instruksi atau melakukan komunikasi dengan fungsi logika, aritmatika, atau memori dari komputer, sistem komputer, atau jaringan computer.
5.	Aplikasi	Perangkat lunak yang dibuat dan disesuaikan terhadap kebutuhan bisnis organisasi sehingga dapat membantu proses bisnis yang dijalankan organisasi.

6.	Aset TI	Sumber daya TI (aplikasi, data/informasi, infrastruktur dan sumber daya manusia) yang mempunyai nilai dukung/manfaat bagi keberhasilan penyelenggaraan proses TI
7.	Area Khusus	Lokasi yang dibatasi oleh keamanan fisik tempat keberadaan aset informasi secara fisik dalam media dan/atau fasilitas pengolah informasi.
8.	Asset Informasi	Sumber daya It yang terdiri atas data/informasi, infrastruktur/phisik, Aplikasi/*Software, Sumber daya manusia, Layanan/service dan Intangible*
9.	*Audit-Trail*	Catatan yang menerangkan transaksi maupun aktifitas sistem informasi yang menyediakan informasi untuk keperluan verifikasi aktifitas sistem.

No	Istilah	Definisi
10.	*Audit Tools*	Perangkat yang digunakan untuk membantu melakukan aktivitas Audit. Dapat berbentuk aplikasi maupun perangkat manajemen seperti kuesioner, dll.
11.	*Backup*	Sebuah proses pembuatan salinan data ke dalam media *backup (tape, harddisk dan CD) sehingga salinan tersebut dapat digunakan untuk mengembalikan data atau konfigurasi ke keadaan sebelumnya.*
12.	*BCP*	Kependekan dari "*Business Continuity Planâ€• yang merupakan satu set dokumentasi sebagai pedoman operasional DSI-Universitas Airlangga ketika terjadi kondisi di luar normal.*
13.	*Business Process Owner*	Suatu unit organisasi DSI-Universitas Airlangga yang memiliki dan bertanggung jawab dalam pengelolaan proses bisnis yang dijalankan melalui suatu aplikasi sesuai dengan lingkup kerjanya.
14.	*Business Continuity*	Merupakan suatu mekanisme manajemen untuk menjaga agar bisnis DSI-Universitas Airlangga dapat tetap berlangsung pada kondisi yang dapat diterima pada saat terjadi kondisi di luar normal.
15.	*Correct Processing*	Penggunaan aplikasi dengan cara yang benar sesuai mekanisme.
16.	*Database*	Sekumpulan data yang disusun dan dikelompokkan sesuai atributnya untuk menyimpan dan memberikan Informasi bagi penggunanya.
17.	*Denial of Service (DoS)*	Kondisi sistem tidak dapat memberikan layanan secara total akibat suatu proses yang tidak terkendali baik dari dalam maupun dari luar sistem.

18.	*Diagnostic Port*	*Port pada perangkat yang digunakan sebagai antar muka dalam melakukan proses diagnosa sistem.*
19.	*Digital Signature*	Kode-kode digital yang disertakan pada suatu pesan atau dokumen elektronik yang digunakan dalam proses verifikasi, otentikasi, dan otorisasi suatu transaksi.

No	Istilah	Definisi
20.	DMZ (Demiliterized Zone)/Middle tear	Suatu segmen network yang dibatasi oleh dua perangkat perimeter keamanan, yang menjadi area penyangga bagi lingkungan server dan lingkungan eksternal. DMZ sering digunakan sebagai strategi keamanan TI untuk koneksi ekstranet.
21.	Ekstranet	Jaringan pribadi yang menggunakan protocol internet dan sistem telekomunikasi public untuk membagi sebagian informasi bisnis atau operasi secara aman kepada *supplier, vendor, partner, konsumen, dll.*
22.	Enkripsi	Proses pengacakan informasi dengan menggunakan sandi atau kode tertentu sehingga tidak dapat dibaca oleh orang lain tanpa mengetahui kunci dari sandi atau kode tersebut.
23.	*Fallback Arrangement*	Mekanisme untuk mengembalikan instalasi sistem ke kondisi awal setelah terjadinya kegagalan instalasi atau kerusakan perangkat.
24.	*Firewall*	Perangkat baik *hardware maupun software teknologi informasi yang digunakan dalam konteks komunikasi jaringan data untuk mencegah masuknya paket data yang secara aturan tidak diperbolehkan ke dalam lingkungan internal.*
25.	Integritas informasi (*informationintegrity)*	Keutuhan informasi, yang berarti tidak ada perubahan, penghilangan atau penambahan yang tidak semestinya terjadi. integritas informasi juga menjamin tentang kebenaran dari data dan lengkap dengan atributnya (seperti: *author dan waktu pembuatannya).*
26.	*Information Technology*	Merupakan teknologi yang berfokus kepada alat bantu/otomatisasi dalam pemrosesan informasi.
27.	Internet	Jaringan komputer yang sangat luas yang menghubungkan satu komputer dengan komputer lainnya dimana di dalamnya terdapat berbagai aneka ragam informasi.
28.	Intranet	Jaringan pribadi yang menggunakan protokol komunikasi *internet protocol, dapat terhubung ke internet (tidak selalu), dan hanya dapat digunakan dalam lingkungan terbatas.*
No	Istilah	Definisi

29.	*Intrusion Detection System (IDS)*	Sistem yang melakukan pengamatan trafik masuk (*inbound) dan keluar (outbound) jaringan secara menyeluruh, serta mengenali pola paket tidak dikenal yang mengindikasikan serangan terhadap sistem internal.*
30.	*ISO (International Standard Organization atau International Organization for Standardization)*	Organisasi non pemerintah yang menetapkan standar yang berlaku secara internasional bagi berbagai jenis industry.
31.	*ISO/IEC 27000 Series*	Panduan standar internasional (ISO) tentang pengendalian dan rekomendasi bagi suatu organisasi dalam mengelola Keamanan informasi.
32.	Keamanan	Sesuatu yang dilakukan sebagai upaya untuk menjaga agar tidak terjadi hal-hal yang tidak dikehendaki, misalnya kerusakan, kehilangan maupun gangguan, baik yang disebabkan oleh kejahatan, kelalaian, maupun tindakan-tindakan lain yang dapat mengakibatkan dampak buruk bagi suatu obyek.
33.	Keamanan informasi (*informationsecurity)*	Suatu upaya yang dilakukan untuk mengamankan informasi, agar terhindar dari berbagai ancaman maupun kejadian yang dapat mengganggu pencapaian tujuan, yaitu; ketersediaan, integritas dan kerahasiaan informasi.
34.	Kepatuhan (*compliance)*	Suatu kondisi yang disikapi agar memenuhi persyaratan peraturan dan undang-undang yang berlaku maupun perjanjian atas pemilikan suatu perangkat TI, sehingga bebas dari tuntutan hukum.
35.	Kerahasiaan informasi (*informationconfidentiality)*	Perlindungan informasi agar tidak dapat diakses (dilihat/diketahui) oleh pihak yang tidak berhak.
36.	Ketersediaan informasi *(information availability)*	Tersedianya akses dan pemanfaatan informasi setiap saat diperlukan.

No	Istilah	Definisi
37.	Klasifikasi	Proses penentuan indikator nilai, indikator kepekaan (sensitivitas) dan risiko terhadap suatu informasi yang dibuat oleh *originator atau Custodian untuk menentukan tingkat pengamanan yang diperlukan bagi informasi tersebut.*

38.	Komite Keamanan Sistem Informasi	Suatu organisasi *adhoc dalam DSI-Universitas Airlangga yang bertugas untuk menentukan standar keamanan yang akan diterapkan DSI-Universitas Airlangga dalam suatu periode berdasarkan kebutuhan bisnis dan teknologi serta risk"s apetite DSI-Universitas Airlangga .*
39.	*Logon atau login*	Proses yang disediakan oleh sistem komputer untuk mengidentifikasi dan otentifikasi pengguna pada saat mulai mengakses (berinteraksi dengan) sistem komputer. Biasanya pengguna lebih dahulu memasukkan kode identitas (*user-id) dan kata sandi (password), kemudian sistem melakukan proses validasi (pengesahan).*
40.	*Main Site*	Suatu tenpat atau lokasi utama fasilitas pengolah dan penyimpan data/informasi.
41.	*Malicious Code*	Kode program yang dapat melakukan pemodifikasian program-program komputer dengan tanpa disadari oleh penggunanya, dapat menghancurkan sistem, mencuri atau memodifikasi data, menyisipkan kode lain pada sistem yang dapat menghancurkan sistem aplikasi beberapa waktu kemudian.
42.	*Malware*	Perangkat lunak komputer (program kecil) yang dibuat untuk tujuan mengganggu dan/atau merusak operasi sistem komputer atau melakukan suatu tujuan tertentu yang tidak baik dan diluar kehendak pengguna sistem komputer, seperti ; *virus, worms, spyware, spam, dan lain-lain.*
43.	Mitra Kerja/Pihak ke-3	Individu atau organisasi yang menyediakan jasa atau unit perangkat yang sesuai dengan perjanjian kontrak.

No	**Istilah**	**Definisi**
44.	*MKI*	Merupakan kependekan dari "Manual Keamanan Informasiâ€• yang merupakan satu set dokumen yang terdiri dari manual kualitas keamanan informasi, standar keamanan informasi, prosedur keamanan informasi, instruksi kerja keamanan informasi dan formulir keamanan informasi.
45.	*Mobile Code*	Kode program yang ditransfer dari satu komputer ke komputer lain untuk kemudian dieksekusi secara otomatis dengan menjalankan suatu fungsi tertentu tanpa atau dengan campur tangan pengguna.
46.	*Mobile Computing*	Penggunaan peralatan komunikasi dan/atau komputer (misal: laptop,PDA, telepon selular) secara *mobile tanpa keterbatasan tempat dan waktu.*

47.	*Notebook*	Istilah untuk menyatakan komputer pribadi (personal computer) yang pemakaiannya dapat berpindah-pindah *(mobile) dan bentuknya relatif kecil menyerupai sebuah buku.*
48.	Organisasi Keamanan Informasi	Suatu organisasi *adhoc yang memiliki tugas utama dalam hal mengkoordinasikan implementasi Sistem Manajemen Keamanan Informasi*
49.	*Password*	Kata sandi yang digunakan bersamaan dengan *username (sign on/sign in/log-on/log-in) oleh pemilik yang sah sebelum melakukan koneksi/akses ke sistem computer.*
50.	*Patches*	Rutin program atau sekumpulan kecil instruksi yang biasanya dibuat sebagai solusi sementara untuk mengatasi atau memperbaiki permasalahan *(bugs) pada program komputer dan sering dibuat dalam bentuk "objectcode" yang disisipkan ke dalam program yang akan dieksekusi.*
51.	Pegawai	Setiap Pria atau Wanita yang mempunyai hubungan kerja untuk waktu tidak tertentu dengan DSI-Universitas Airlangga yang telah melampaui masa percobaan (di luar Direktur) dan diangkat oleh DSI-Universitas Airlangga dengan Surat Keputusan.

No	**Istilah**	**Definisi**
52.	Pekerja Kontrak	Individu yang menjadi pegawai berbatas waktu yang diikat dalam suatu perjanjian kontrak.
53.	Pembuat Informasi (*Originator)*	Pegawai DSI-Universitas Airlangga yang menyiapkan naskah asli dari suatu dokumen atau *file.*
54.	Pemelihara Informasi (*Custodian)*	Pejabat DSI-Universitas Airlangga yang bertanggung jawab atas pengelolaan suatu kumpulan informasi.
55.	Pemilik Data	Suatu unit organisasi DSI-Universitas Airlangga yang memiliki data/informasi yang dikelola melalui suatu sistem database sesuai dengan lingkup kerjanya
56.	Penetration test	Salah satu bentuk pengujian keamananan jaringan dimana pelaksana pengujian mencoba menerobos sistem keamanan jaringan yang sedang diuji.
57.	Pengelola Infrastruktur Teknologi Informasi	Kelompok atau unit organisasi yang diberi tanggung jawab mengelola operasi infrastruktur teknologi informasi sehingga terjaga ketersediaannya.
58.	Pengelola Layanan Sistem Informasi	Kelompok atau unit organisasi yang diberi tanggung jawab untuk mengelola layanan Sistem Informasi.

59.	Pengelola Sumber daya manusia (SDM)	Kelompok atau unit organisasi DSI-Universitas Airlangga yang diberi tanggung jawab untuk mengelola sumber daya manusia yang digunakan oleh DSI-Universitas Airlangga , baik pegawai maupun pekerja kontrak.
60.	Pengguna	Individu akhir yang *authorized dalam suatu organisasi DSI-Universitas Airlangga yang menggunakan layanan sistem informasi.*
61.	Penyebaran Informasi (*Disclosure)*	Memberikan atau menunjukkan atau memberitahukan informasi kepada orang, organisasi atau sistem secara lisan melalui presentasi dengan menggunakan transparansi, *slide atau gambar, secara tertulis, dan memberikan akses ke dalam komputer atau menunjukkan data dari komputer melalui display.*
62.	DSI-Universitas Airlangga	Direktorat Sistem Informasi salah satu Direktorat dalam Struktur Organisasi Universitas Airlangga

No	**Istilah**	**Definisi**
63.	Prosedur	Suatu rangkaian aktivitas, tugas-tugas, tahapan, keputusan, perhitungan dan proses yang bila dilakukan dengan seksama akan memberikan hasil atau tujuan sesuai dengan yang direncanakan.
64.	Proses	Suatu aktivitas yang terstruktur.
65.	*Remote Sit*	Suatu tempat atau lokasi sistem cadangan fasilitas pengolah dan penyimpan data/informasi, yang lokasinya terpisah dalam area geografis tertentu dari sistem utama (*main site).*
66.	*Removable media*	Media yang mengandung informasi dan secara fisik dapat dipindahkan dengan mudah.
67.	*Restore*	Proses mengembalikan data atau konfigurasi dari hasil *backup.*
68.	*Resumption*	Pengembalian sistem ke kondisi normal setelah terjadi bencana.
69.	Risiko	Segala kejadian dalam setiap aktivitas DSI-Universitas Airlangga yang timbul karena faktor eksternal maupun internal, yang mengandung potensi menghambat pencapaian tujuan DSI-Universitas Airlangga .
70.	*Routing*	Penetapan jalur lintasan komunikasi data dari suatu jaringan sumber ke suatu jaringan tujuan.
71.	Segmentasi jaringan	Pembagian jaringan dalam bentuk ruas-ruas.
72.	Segregasi jaringan	Pemilahan/pemisahan jaringan dari jaringan lainnya.
73.	*Segregation of Duties*	Satu konsep pengaturan terhadap lebih dari satu pegawai yang dibutuhkan untuk menyelesaikan suatu tugas.

74.	*Server*	Sebuah sistem computer yang menyediakan jenis layanan tertentu dalam sebuah jaringan computer.
75.	Sistem Aplikasi	Sistem dan mekanisme yang diotomatisasikan untuk memproses informasi.

No	Istilah	Definisi
76.	Sistem Informasi	Suatu sistem terpadu yang terdiri dari perangkat keras (*hardware), sistem aplikasi (software / application), jaringan komunikasi, sumber-sumber data, sumber daya manusia (brainware), serta mekanisme yang mengumpulkan, mentransformasikan dan menyebarkan informasi dalam suatu organisasi.*
77.	*Smartphone*	Sebuah peralatan mini yang dapat dikantongi (seperti *P ocket PC), yang pada awalnya dirancang sebagai alat organizer pribadi. Namun, sekarang kemampuannya telah berkembang sehingga dapat juga digunakan sebagai alat penunjuk waktu dan kalender, bermain game komputer, mengakses internet, mengirim dan menerima e-mail, sebagai radio atau stereo, merekam gambar, menyimpan catatan, daftar alamat, spreadsheet dan bahkan sebagai telepon mobile, web browser atau media players.*
78.	SMKI	Kependekan dari "Sistem Manajemen Keamanan Informasiâ€• yang merupakan serangkaian kegiatan perencanaan, implementasi, pemantauan dan peningkatan Keamanan Informasi dengan pendekatan manajemen.
79.	*Tamper-Evident Packaging*	Proses pengemasan media informasi yang menjamin keamanan isi/media dari kerusakan dan akses yang tidak sah.
80.	*Teleworking*	Pelaksanaan pekerjaan dalam sistem informasi yang dilaksanakan secara jarak jauh dengan menggunakan fasilitas jaringan (*Wide Area Network/WAN).*
81.	TimAudit Sistem Informasi	Tim yang dibentuk olehDSI-Universitas Airlangga yang bertugas melakukan kegiatan *assessment dan audit sistem informasi untuk seluruh sistem informasi kritikal DSI-Universitas Airlangga .*

No	Istilah	Definisi

82.	Sub Direktorat Operasional SIstem Informasi	Unit organisasi Direktorat Sistem Informasi - Universitas Airlangga yang diberi tanggung jawab untuk mengelola teknologi informasi dan komunikasi, menyusun, memonitor, dan memutahirkan kebijakan teknologi informasi dan komunikasi dalam lingkungan DSI-Universitas Airlangga
83.	Seksi Keamanan Data	Unit organisasi Direktorat Sistem Informasi - Universitas Airlangga yang bertanggung jawab untuk mengelola keamanan data dan asset informasi DSI-Universitas Airlangga .
84.	*User Account Management*	Pengelolaan identitas pengguna dalam sistem informasi, mulai dari tahapan: pembuatan identitas, pengaturan hak akses, perubahan, dan penghapusan pengguna; untuk keperluan pengguanaan sumber daya teknologi informasi, keamanan dan aktivitas pencatatan *log.*
85.	*Virtual Private Network (VPN)*	Jaringan komunikasi khusus yang digunakan untuk kepentingan internal DSI-Universitas Airlangga dengan memanfaatkan infrastruktur jaringan publik.
86.	*Vulnerability*	Kelemahan yang disebabkan oleh adanya titik rawan yang memungkinkan masuknya serangan yang mengakibatkan kerusakan sistem atau aplikasi.
87.	*Workstation*	Komputer yang terhubung dengan sebuah *local-area network (LAN)*

MKI.0. KEBIJAKAN KEAMANAN INFORMASI

A. PENDAHULUAN

Nilai suatu Informasibisa berbentuk nomor, tulisan, gambar, pengetahuan, konsep, ide, dan merekyang merupakan contoh dari asset tidak berwujud. Saat ini proses pertukaran informasi dapat terjadi melalui system, jaringan, orang yang terlibat dalam proses tersebut. Mengelola dan menjaga asset terutama asset bisnis sangatlah penting dari ancaman yang disengaja maupun tidak disengaja baik itu dari dalam organisasi maupun dari luar organisasi. Organisasi juga harus memperkirakan dampak yang terjadi ketika ada perubahan bisnis di dalam organisasi atau ketika adanya perubahan dari luar organisasi seperti perubahan peraturan perundang undangan.

Tujuan

Manual Keamanan Informasi ini merupakan pedoman umum penerapan keamanan sistem informasi yang selaras dengan kebutuhan DSI-Universitas Airlangga dan dapat dilaksanakan secara berkesinambungan. Manual ini juga merupakan acuan setiap unit yang terkait dengan penyelenggaraan teknologi informasi DSI-Universitas Airlangga dalam penyusunan dan penetapan petunjuk pelaksanaan dan operasional di

lingkungan organisasi unit terkait.

Risiko

Penilaian resiko menjadi proses awal yang sangat penting bagi organisasi. Resiko keamanan informasi selalu ada, keamanan informasi yang efektif adalah dengan mengurangi resiko dengan menjaga organisasi dari ancaman dan kerentanan, dankemudian mengurangi dampak terhadap aset.

B. KEBIJAKANKEAMANAN INFORMASI

MKI.0.1. SISTEM MANAJEMEN KEAMANAN INFORMASI

Kebutuhan keamanan informasi dalam organisasi dapat dibagi menjadi tiga bagian :

a.penilaian resiko pada organisasi, yang meliputi seluruh stategi dan tujuan bisnis. meliputi penilaian resiko, identifikasi ancaman terhadap aset, kerentanan, likelihood, dan impact

b.hukum, undang-undang, peraturan dan kontrak persyaratan bahwa suatu organisasi, mitra dagang, kontraktor, dan penyedia layanan harus patuh, dan lingkungan sosial budaya.

c.sejumlah prinsip, tujuan dan kebutuhan bisnis untuk penanganan informasi, pengolahan, penyimpanan, komunikasi bahwa organisasi dikembangkan untuk mendukung secara operasional.

A. Kebijakan

Dalam menetapkan SMKI, DSI-Universitas Airlangga harus melakukan hal-hal sebagai berikut:

1.Manajemen harus menetapkan permasalahan internal dan eksternal yang relevan dengantujuan dan yang mempengaruhi kemampuannya untuk mencapai hasil yang dimaksudkan dalam SMKI

2.Manajemen harus menetapkan pihak yang berkepentingan dengan SMKI dan kebutuhan mereka terhadap SMKI termasuk kebutuhan hukum dan peraturan serta kewajiban kontaktual

3.Menetapkan ruang lingkup dan batasan SMKI dengan mempertimbangkan permasalahan internal dan external organisasi, kebutuhan organisasi, karakteristik bisnis, organisasi, lokasi, aset dan teknologi, dan termasuk rincian dari setiap pengecualian.

4.Menetapkan kebijakan SMKI dengan mempertimbangkan permasalahan internal dan external organisasi, karakteristik bisnis, organisasi, lokasi, aset dan teknologinya.

5.Menetapkan Peraturan perundang undangan yang akan diadopsi dalam melaksanakan SMKI

6.Menetapkan standart yang digunakan dalam melaksanakan SMKI

B. DOKUMEN TERKAIT

1. Kontrak Kinerja Direktur Sistem Informasi

2. Menetapkan SOA

MKI.0.2.TANGGUNG JAWAB MANAJEMEN

Dalam mendukung terselenggaranya Keamanan Informasi yang berlaku di seluruh DSI-Universitas Airlangga , manajemen memberikan komitmen sebagai tanda dukungan terhadap pelaksanaan Keamanan Informasi. Komitmen manajemen tersebut didokumentasikan, ditandatangani oleh manajemen puncak dan disebarluaskan ke seluruh unit yang ada di DSI-Universitas Airlangga .

Manajemen harus membuat kebijakan tentang keamanan informasi, dan harus dapat mendefinisikan peran, tanggungjawab, dan otoritas dalam manajemen keamanan informasi.

A. KEBIJAKAN

Top manajemen harus menyusun kebijakan keamanan informasi bahwa :

1. Kebijakan dan tujuan keamanan informasi harus sesuai dengan tujuan organisasi

2. komitmen untuk memenuhi persyaratan yang berlaku terkait dengan keamanan informasi

3. komitment untuk selalu melakukan perbaikan terus menerus pada SMKI

4. menempatkan SDM sesuai dengan skill

B. DOKUMEN TERKAIT

1. Manual keamanan informasi

2. DSI.UA/IK-MR.04 Tinjauan Manajemen

3. Laporan training awareness.

4. Job description untuk masing masing pagawai

5. Training sesuai skill yang dibutuhkan

MKI.0.3.PERENCANAAN DAN PENGELOLAAN KEAMANAN INFORMASI

DSI Universitas Airlangga harus membuat perencanaan dan menerapkan keamanan informasi berdasarkan pada penilaian resiko.

A. KEBIJAKAN

1. Seksi keamanan data harus melakukan penilaian resiko terhadap asset yang dimiliki oleh DSI berdasarkan

confidentiality, integrity, availability, likelihood dan level resiko.

2. Menetapkan kriteria resiko yang dapat diterima oleh manajemen, rencana risk treatment, dan residual risk yang dapat diterima manajemen.

3. Penilaian resiko harus direview minimal satu tahun sekali.

B. DOKUMEN TERKAIT

1. DSI.UA/P.IK.11 Information Risk Manajement (IRM)

2. Laporan hasil penilaian resiko

MKI.0.4.Evaluasi dan improvement keamanan informasi

A. KEBIJAKAN

1. Semua metode SMKI harus dimonitor, diukur, dianalisis, dievaluasi, diterapkan, dan dipastikan memberikan hasil yang valid

2. Direktorat system informasi harus melakukan internal audit minimal satu tahun sekali.

3. Direktorat system informasi harus menetapkan instruksi kerja untuk internal audit

4. Manajemen harus melakukan review terhadap SMKI minimal satu tahun sekali

5. dalam manajemen review juga harus menetapkan perbaikan terus menerus berdasarkan kebutuhan dalam perubahan SMKI

6. melakukan tindaklajut perbaikan dan mereview tindakan perbaikan terhadap temuan ketidaksesuaian dalam internal audit.

7. organisasi harus terus meningkatkan kesesuaian, kecukupan dan efektivitas sistem manajemenkeamanan informasi

8. Tata cara tindakan perbaikan dan pencegahan akan dibahas lebih lanjut dalam DSI-UA/P-IK.10 Tindakan perbaikan dan tindakan pencegahan

B. DOKUMEN TERKAIT

1. DSI-UA/P-IK.10 Tindakan perbaikan dan tindakan pencegahan

2. DSI-UA/IK-MR.03 Internal Audit SMKI

MKI.0.5.KEBIJAKAN KEAMANAN INFORMASI

A. KEBIJAKAN

1. Kebijakan keamanan informasi harus berisi :

a. definisi keamanan informasi, tujuan, dan prinsip-prinsip untuk memandu semua kegiatan yang berkaitan dengan keamanan informasi

b. mendefinisikan peran dan tanggungjawab keamanan informasi

c. proses penanganan informasi dan pengecualian

3. Kebijakan keamanan informasi harus di review minimal satu tahun sekali dan dikomunikasikan ke pegawai di DSI dan pihak di luar DSI yang relevan.

B. DOKUMEN TERKAIT

1. Panduan instruksi kerja klasifikasi keamanan informasi

MKI.0.6.ORGANISASI KEAMANAN INFORMASI

5.1.Internal Organisasi

A. KEBIJAKAN

1. Setiap seksi di Direktorat Sistem Informasi harus mengidentifikasi asset yang dimiliki sesuai dengan prosedur yang tertulis di Pedoman Instruksi Kerja

2. Setiap Seksi di DSI harus melakukan analisa resiko setiap asset sesuai dengan prosedur yang tertulis di Pedoman Instruksi Kerja

3. Setiap perubahan dokumen daftar asset dan analisa resiko harus di tandatangani oleh kepala seksi , kasubdit dan Direktur

4. Direktorat Sistem Informasi harus memiliki daftar kontak orang/unit yang harus dihubungi ketika terjadi insiden

5. Setiap pembuatan/penambahan fitur aplikasi IT, penambahan infrastruktur IT, penambahan pegawai, pemberian fasilitas IT kepada pegawai, setiap kepala seksi harus memperhatikan resiko information security.

6. Setiap pegawai yang diberikan fasilitas mobile device harus mengikuti peraturan yang telah ditulis di panduan IK tentang mobile device and teleworking

7. Setiap pegawai yang melakukan Teleworking harus melalui VPN akses yang telah disetujui oleh kepala seksi network dan diketahui oleh Direktur.

B. DOKUMEN TERKAIT

1. Daftar asset

2. Dokumen penilaian resiko

3. Daftar kontak orang/unit yang harus dihubungi ketika terjadi insiden

4. Peraturan tentang mobile device dan teleworking (DSI.UA/P.IK.09)

MKI.0.7.KEAMANAN SUMBER DAYA MANUSIA

A. KEBIJAKAN

1. Setiap pegawai baru di DSI harus melalui background check, untuk copy ijazah, dan identitas lainnya merupakan tanggungjawab dari direktorat Sumberdaya, untuk copy surat keterangan tidak pernah terlibat tindak kriminal dari pihak kepolisian harus diberikan ke DSI.

2. Setiap pegawai di DSI harus menandatangani dokumen NDA (non disclosure agreement)

3. Setiap pihak ketiga yang akan mengakses informasi rahasia di DSI harus menyerahkan copy identitas dan menandatangani dokumen NDA (non Disclosure Agreement)

4. Setiap pegawai harus diberikan pelatihan awareness keamanan informasi yang dilakukan sekali dalam setahun, dan di review

5. Direktur Sistem Informasi berhak untuk melakukan rotasi pegawai yang dinilai tidak relevan lagi pada jabatan tersebut dengan persetujuan Direktorat Sumberdaya

6. Penghentian pegawai merupakan tanggungjawab dari Direktorat Sumber Daya.

7. Setiap Pegawai di DSI akan dilakukan evaluasi kinerja secara berkala pada tiap akhir bulan oleh kepala seksi

8. Setiap pegawai DSI yang mengalami perubahan tanggungjawab baik itu karena rotasi atau pensiun atau mengundurkan diri atau pemutusan hubungan kerja harus menyerahkan tanggungjawab tersebut kepada kepala seksi masing masing.

B. DOKUMEN TERKAIT

1. Surat keterangan tidak pernah terlibat tindak kriminal dari kepolisian

2. Dokumen NDA pegawai dan pihak ketiga

3. Pelatihan awareness dan evaluasi

4. DSI.UA/KT-SDI.01 Induksi & Awareness Keamanan Informasi

5. DSI.UA/KT-SDI-03 Pemenuhan Kebutuhan & Verifikasi Latar Belakang

6. Aplikasi penilaian kinerja

MKI.0.8.MANAJEMEN ASET

A. KEBIJAKAN

1. Setiap asset harus dicatat (pengelola, tempat penyimpanan, penggunaan, kerusakan, penghapusan asset, penghancuran asset, pengembalian asset) dan di review oleh masing masing seksi.

2. Seksi keamanan data harus membuat pedoman IK tentang klasifikasi keamanan informasi, tata keloka informasi, penghancuran informasi.

3. Untuk penggunaan asset telah diatur dalam panduan IK penggunaan asset yang sesuai.

4. Untuk penggunaan removable media di ruang data center harus melalui ijin kasie network

5. Apabila ada perpindahan asset dari data center keruang lain dapat dilakukan dengan seijin kasie network

6. Apabila pemindahan hardware tersebut ditujukan kepada pihak ketiga (missal : untuk maintenance) maka seksi network harus memastikan sudah tidak ada data rahasia yang ada dalam hardware tersebut.

B. DOKUMEN TERKAIT

1. Peraturan tentang penggunaan asset ICT yang sesuai (DSI.UA/P-IK.02)

2. Dokumen daftar asset

3. Panduan IK tentang klasifikasi dan penanganan informasi (DSI.UA/P-IK.01)

4. Pemusnahan informasi dan penghancuran media (DSI.UA/IK-Sec.02)

MKI.0.9.AKSES KONTROL

A. KEBIJAKAN

1. Setiap aplikasi, dan manajemen jaringan yang ada di DSI harus memiliki role hak akses baik kedalam aplikasi atau database yang harus disetujui oleh minimal kepala seksi masing masing, dan direview oleh kepala seksi secara berkala

2. Seksi network harus memiliki policy tentang hak akses ke dalam network dan network services yang mencakup hak otorisasi user, area network dan network services yang diijinkan untuk diakses melalui VPN / wireless, monitoring penggunaan network dan network services, dan harus direview secara berkala

3. Harus terdapat matrik hak akses untuk network, network services, aplikasi, dan database

4. Untuk akses laptop atau komputer personal, pegawai diperbolehkan menggunakan jenis akun administrator, tetapi pegawai harus bisa mempertanggung jawabkan pilihan jenis akunnya. Jika terjadi suatu pelanggaran keamanan informasi dikarenakan karena hal tersebut, maka pegawai akan mendapatkan sanksi sesuai dengan yang telah ditentukan.

5. Ketentuan lebih lanjut tentang hak akses diatur dalam pedoman instruksi kerja tata kelola hak akses, dan instruksi kerja manajemen password untuk Administrator.

B. DOKUMEN TERKAIT

1. Matrik hak akses

2. Pedoman instruksi kerja tata kelola hak akses,

3. Role Hak Akses

MKI.0.10.CRYPTOGRAPHY

A. KEBIJAKAN

1. Untuk semua hak akses yang terhubung dengan aplikasi cyber campus dan aplikasi penunjang di DSI, semua password akan terenkripsi secara otomatis melalui system

2. Metode enkripsi harus direview secara berkala sesuai dengan perkembangan teknologi

B. DOKUMEN TERKAIT

1. Enkripsi pada password di aplikasi cyber dan aplikasi penunjang lainnya

MKI.0.11.KEAMANAN FISIK DAN LINGKUNGAN

A. KEBIJAKAN

1. Seksi Keamanan Data harus menetapkan physical security area dan harus disetujui oleh Direktur.

2. Bagian Helpdesk dan receptionist harus melakukan control terhadap tamu yang akan masuk ke DSI

3. Kebersihan dan kerapihan meja kerja dan kerapihan kabel pada meja kerja adalah tanggungjawab staf yang duduk dimeja tersebut

4. Kebersihan area data center dan kerapihan kabel di data center adalah tanggungjawab dari seksi Network

5. Ketentuan lain diatur dalam P-IK standarisasi area data center, Ketentuan Operasional Penerimaan Tamu, dan ketentuan operasional Clean desk dan clear Desk

B. DOKUMEN TERKAIT

1. Peta physical security area

2. Buku tamu

3. DSI.UA/P-IK.04 - Standarisasi Area Data Center

4. DSI.UA/KT-SDI-02 - Penerimaan Tamu

5. DSI.UA/KT-SDI.08 Clear Desk dan clear screen

MKI.0.12.OPERATION SECURITY

A. KEBIJAKAN

1. Setiap seksi di Direktorat Sistem Informasi harus memiliki pedoman prosedur dan instruksi kerja untuk

setiap pekerjaan

2. Setiap ada perubahan atau penambahan infrastruktur jaringan atau konfigurasi jaringan seksi network harus melakukan uji coba terlebih dahulu, dan ujicoba harus sepengetahuan Direktur dan Kepala subdirektorat operasional SI.

3. Seksi Network harus memiliki capacity manajement plan tentang storage, infrastruktur, dan bandwidth.

4. Setiap ada perubahan atau penambahan pada database dan aplikasi Seksi System Integration and Aplication Development harus melakukan ujicoba terlebih dahulu, dan ujicoba harus sepengetahuan Direktur dan Kepala subdirektorat pengembangan system.

5. Setiap ujicoba yang dilakukan harus direncanakan dan didokumentasikan

6. Development, testing, dan operasional aplikasi dan database harus dipisahkan minimal secara logic

7. Untuk melakukan proteksi terhadap malware dan virus pada personal computer pegawai, DSI menyediakan antivirus untuk computer dan laptop yang menjadi asset Universitas Airlangga dananti virus ini akan diperbaharui setiap tahunnya.

8. Untuk melakukan proteksi terhadap malware pada server , DSI menggunakan firewall dengan proteksi terkini

9. Untuk back up dan recovery diatur lebih lanjut pada P-IK pelaksanaan Backup dan recovery

10. Untuk pengelolaan dan monitoring log pada network dan network services merupakan tanggungjawab seksi network, sedangkan log database dan aplikasi merupakan tanggungjawab seksi system integration and application development.

11. Untuk manajemen log dikelola dengan software yang telah ditentukan oleh seksi network

12. Seksi network harus selalu melakukan synchronisasi waktu yang ada di setiap server di Data Center.

13. DSI Unair menyediakan lisensi software Microsoft bagi computer dan laptop yang merupakan asset Universitas, dengan mekanisme yang telah diatur dalam PP-Unair-Mun-04-07 pencitraan internal

14. Instalasi software pada computer atau laptop menjadi tanggungjawab pegawai yang memegang computer atau laptop tersebut

15. Seksi keamanan data memiliki tanggungjawab untuk melakukan pengecekan keamanan pada setiap website yang dimiliki oleh DSI Unair, setiap vulnerability yang ditemukan akan dicatat dan dianalisa untuk meminimalisir resiko keamanan

16. Seksi keamanan data melakukan verifikasi terhadap bisnis proses dalam pelaksanaan pembuatan system network diseksi network dan application development di seksi system integration and application development

B. DOKUMEN TERKAIT

1. Laporan hasil uji coba

2. Dokumen capacity management plan

3. Pemantauan penggunaan anti virus di Universitas Airlangga

4. Laporan penetration tester

MKI.0.13.COMMUNICATION SECURITY

A. KEBIJAKAN

1. Pada prinsipnya keamanan jaringan merupakan tanggungjawab dari seksi network

2. Tata kelola keamanan jaringan telah diatur dalam panduan IK tata kelola keamanan jaringan

3. Setiap pihak ketiga yang akan melakukan akses kedalam internal jaringan DSI Unair harus menandatangani NDA, dan harus mendapatkan persetujuan dari kepala seksi Network dan diketahui oleh Direktur

4. Pemberian informasi rahasia kepada pihak ketiga harus sesuai dengan aturan panduan IK tentang klasifikasi dan penanganan Informasi.

B. DOKUMEN TERKAIT

1. NDA untuk pihak ketiga

2. Panduan IK tentang klasifikasi keamanan informasi

MKI.0.14.SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE

A. KEBIJAKAN

1. Setiap pembuatan aplikasi, baik itu baru atau penambahan modul maka harus ada tahap testing

2. Untuk proses pembayaran mahasiswa, menggunakan prosedur yang berlaku di Universitas Airlangga, sedangkan dalam aplikasi harus menggunakan teknologi terkini ketika Database Unair berkomunikasi dengan database pihak lain (pihak bank)

3. Untuk Proses pengelolaan keuangan dan e-procurement DSI bertanggungjawab dalam pengelolaan jaringan sedangkan secara proses dan penanganan aplikasi merupakan tanggungjawab Direktorat masing masing.

4. Untuk security development live cycle akan dibahas lebih lanjut dalam pedoman instruksi kerja security development live cycle

5. Seksi Keamanan Data bertugas untuk membuat dokumen analisa kebutuhan dan spesifikasi keamanan aplikasi

B. DOKUMEN TERKAIT

1. pedoman instruksi kerja security development live cycle

MKI.0.15.SUPPLIER RELATIONSHIPS

A. KEBIJAKAN

1. Proses Pengadaan barang dan jasa di DSI mengacu pada peraturan perundang-undangan yang berlaku

2. Proses pemilihan supplier untuk pengadaan barang dan jasa di DSI mengacu pada peraturan perundang-undangan yang berlaku

3. DSI berlanggungjawab untuk mempersiapkan spesifikasi kebutuhan barang dan jasa.

4. Seksi Keamanan data bertanggungjawab melakukan analisis penilaian resiko supplier barang dan jasa di DSI Unair

5. Pengelolaan perubahan jasa supplier diatur sesuai dengan peraturan perundang undangan yang berlaku

B. DOKUMEN TERKAIT

1. Risk assessment

MKI.0.16. INFORMATION SECURITY INCIDENT MANAGEMENT

A. KEBIJAKAN

1. Setiap seksi harus mencatat setiap terjadi insiden keamanan informasi yang berkaitan dengan tupoksi seksi tersebut

2. Prosedur penanganan even dan weakness sesuai dengan DSI.UA/IK-Sec.01 Penanganan Event dan Weakness Keamanan Informasi.

3. Setiap seksi harus melakukan analisa penyebab dan dampak untuk setiap insiden/trouble yang terjadi dan didokumentasikan.

B. DOKUMEN TERKAIT

1. DSI.UA/IK-Sec.01 Penanganan Event dan Weakness Keamanan Informasi.

MKI.0.17. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

A. KEBIJAKAN

1.DSI Unair bertanggungjawab untuk tetap bisa menyediakan layanan system informasi setelah terjadinya kondisi diluar normal seperti yang dijelaskan diatas

2.DSI Unair bertanggungjawab melakukan pemulihan kondisi layanan system informasi setelah terjadi

kondisi diluar normal baik itu infrastruktur jaringan, aplikasi, dan database

3. Nilai RTO dan MTPD telah ditetapkan di IK Keberlangsungan layanan Sistem Informasi (DSI.UA/IK.SDI.02)

4. Ujicoba layanan di DSI dilakukan sesuai dengan jadwal yang ditetapkan dan minimal dilaksanakan satu tahun sekali.

5. Prosedur pelaksanaan respon tanggap darurat dan pemulihan kegiatan untuk setiap kondisi diluar normal sesuai dengan IK-Unair-Mun-04-09-03 pelimpahan penanganan trouble helpdesk

6. Redundancies infrastruktur dan aplikasi disediakan sesuai dengan kekuatan anggaran DSI Unair.

B. DOKUMEN TERKAIT

1. IK Keberlangsungan layanan Sistem Informasi (DSI.UA/IK.SDI.02)

2. Laporan Hasil Ujicoba Backup Recovery database dan aplikasi

MKI.0.18. COMPLIANCE

A. KEBIJAKAN

1. Kepatuhan terhadap Undang-Undang diatur dalam Instruksi Kerja Identifikasi dan evaluasi terhadap peraturan perundang-undangan.

2. DSI bertanggungjawab menyediakan kebutuhan licency software legal sesuai dengan kekuatan anggaran yang dimiliki

3. Setiap seksi di DSI harus mematuhi pedoman prosedur dan instruksi kerja masing masing

4. Setiap seksi harus melakukan evaluasi pedoman prosedur dan instruksi kerja masing masing minimal satu tahun sekali.

5. Evaluasi pelaksanaan pedoman prosedur dan instruksi kerja bisa dilakukan melalui internal audit maupun eksternal audit.

B. DOKUMEN TERKAIT

1. IK identifikasi dan evaluasi terhadap peraturan perundang-undangan.