BAB IV
EVALUASI SISTEM KEAMANAN INFORMASI DEPARTEMEN PERTANIAN

4.1 Kebijakan Keamanan Informasi

Hasil evaluasi menunjukkan Deptan belum memiliki kebijakan keamanan informasi yang komprehensif dan formal. Sehingga perencanaan sistem keamanan informasi untuk aspek kebijakan keamanan informasi perlu dibangun dari awal.

Dalam rangka menyediakan arahan bagi pimpinan dan untuk mendukung keamanan informasi sesuai dengan kebutuhan kegiatan unit kerja, tupoksi, dan peraturan perundang-undangan yang berlaku di Departemen Pertanian, pihak pimpinan di Departemen Pertanian selayaknya merancang arah kebijakan secara jelas dan selaras dengan visi, misi, sasaran, dan tujuan Departemen.

Hal ini juga harus ditindaklanjuti dengan memberikan dukungan penuh dan komitmen pada keamanan informasi di seluruh eselon I Deptan. Bentuk dukungan serta komitmen dari pimpinan seyogyanya dituangkan dalam perancangan aturan-aturan atau kebijakan-kebijakan serta merencanakan perbaikan secara berkala terhadap kebijakan tersebut.

4.1.1 Kebijakan Keamanan Informasi

Dokumen Kebijakan Keamanan Informasi seharusnya disetujui oleh pimpinan tertinggi di Departemen Pertanian, dipublikasikan, dan dikomunikasikan kepada seluruh pegawai di lingkungan Departemen Pertanian maupun pihak lain yang relevan.

Dokumen Kebijakan Keamanan Informasi berisikan pernyataan komitmen pimpinan tertinggi di Deptan dan perancangan pendekatan Deptan dalam memanaje keamanan informasi.

Dokumen ini secara umum berisikan :

a. Definisi dari keamanan informasi, tujuan utama dan ruang lingkup, dan pentingnya keamanan informasi sebagai salah satu mekanisme untuk berbagi informasi.
b. Pernyataan dari pimpinan tertinggi di Departmen Pertanian bahwa pihak pimpinan pada prinsipnya setuju bahwa keamanan informasi sejalan dengan visi, misi, sasaran, dan tujuan Deptan.
c. Kerangka kerja dalam merancang tujuan pengendalian termasuk bagaimana pengkajian resiko dan manajemen resiko
d. Penjelasan singkat mengenai kebijakan keamanan, prinsipnya, standar yang digunakan, dan kepentingannya dalam memenuhi peraturan perundang-undangan yang ada.
e. Pengaturan mengenai tanggung jawab untuk manajemen keamanan informasi termasuk pelaporan apabila terjadi gangguan keamanan.
f. Referensi ke dokumen lain yang isinya mungkin berkaitan dengan dokumen kebijakan untuk memudahkan pegawai dalam memahami kebijakan yang ada.

Dokumen kebijakan keamanan informasi ini dibagi menjadi beberapa bagian, diantaranya adalah :

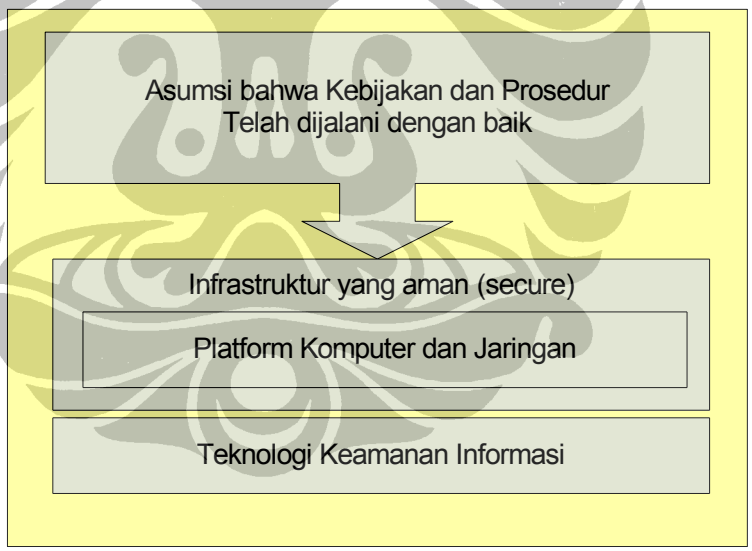
a. Manajemen dan perlindungan password, termasuk aturan dalam penggunaan password dan kewajiban penggantian password secara berkala.
b. Kebijakan lisensi perangkat lunak, yaitu aturan Deptan dalam penggunaan perangkat lunak yang berlisensi maupun yang dibangun sendiri (*inhouse development application*)
c. Kebijakan perlindungan terhadap virus.
d. Kebijakan penggunaan internet
e. Kebijakan penggunaan e-mail
f. Kebijakan dalam pemberian sangsi, peringatan terhadap pihak-pihak yang membahayakan keamanan organisasi
g. Kebijakan dalam akses ke lokasi-lokasi khusus.

4.1.2 Arsitektur dan Model Keamanan Informasi

Arsitektur dan model keamanan informasi Departemen Pertanian merupakan pengejawantahan dari kebijakan keamanan informasi yang ada. Sebagai gambaran arsitektur informasi di Deptan dapat dilihat pada gambar 4.1

Kebutuhan organisasi akan layanan TI dan semakin berkembangnya teknologi TI mengharuskan organisasi untuk memiliki suatu misi tertentu demi fokusnya proses keamanan informasi.

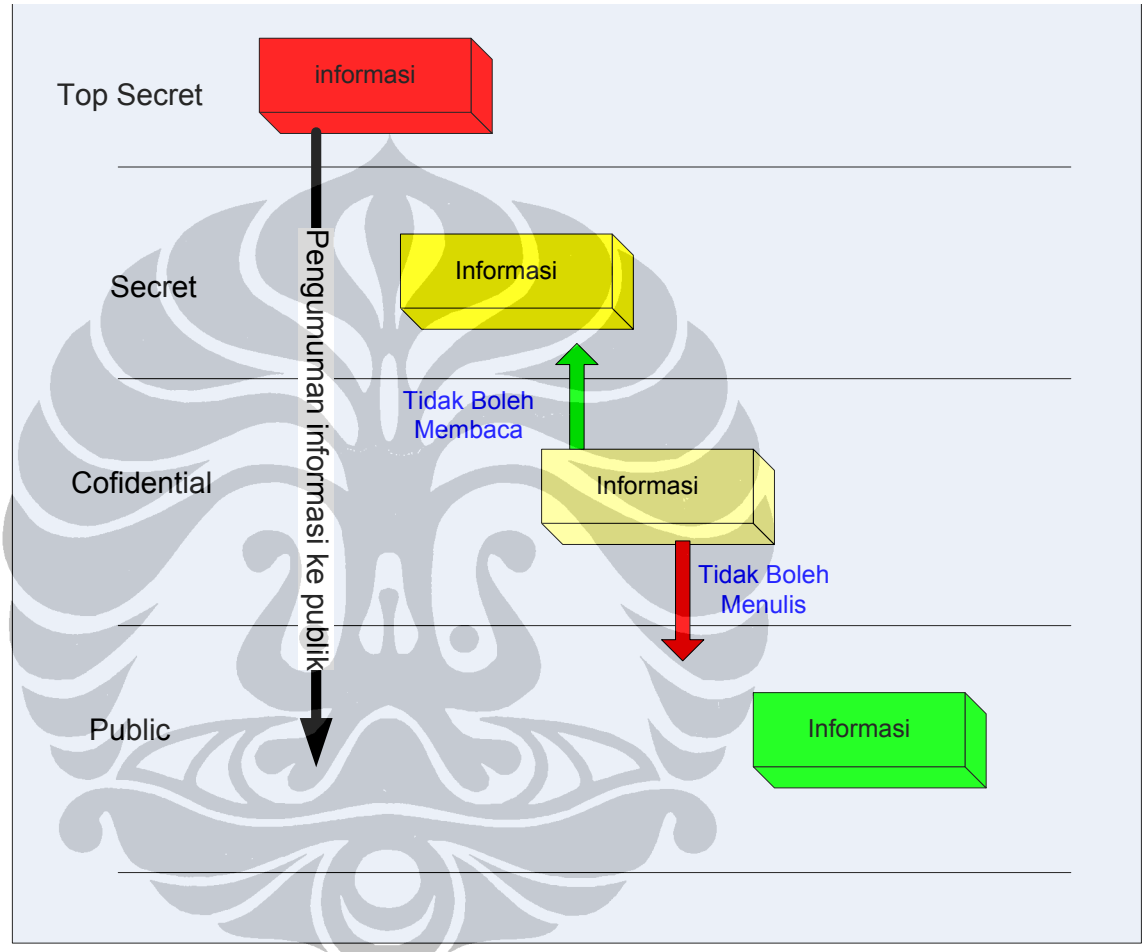
Apabila kebijakan dan prosedur telah dijalankan, misalnya informasi telah diklasifikasikan berdasarkan tingkat keamanan yang dibutuhkan atau hak akses setiap individu terhadap aset telah terdefinisikan maka dapat diasumsikan bahwa masukan atau input untuk infrastruktur dalam kondisi ideal maka kondisi keamanan informasi dapat tercipta. Seperti terlihat pada gambar 4.1 berikut.



Gambar 4.1 Faktor pendukung efektifnya kebijakan keamanan informasi

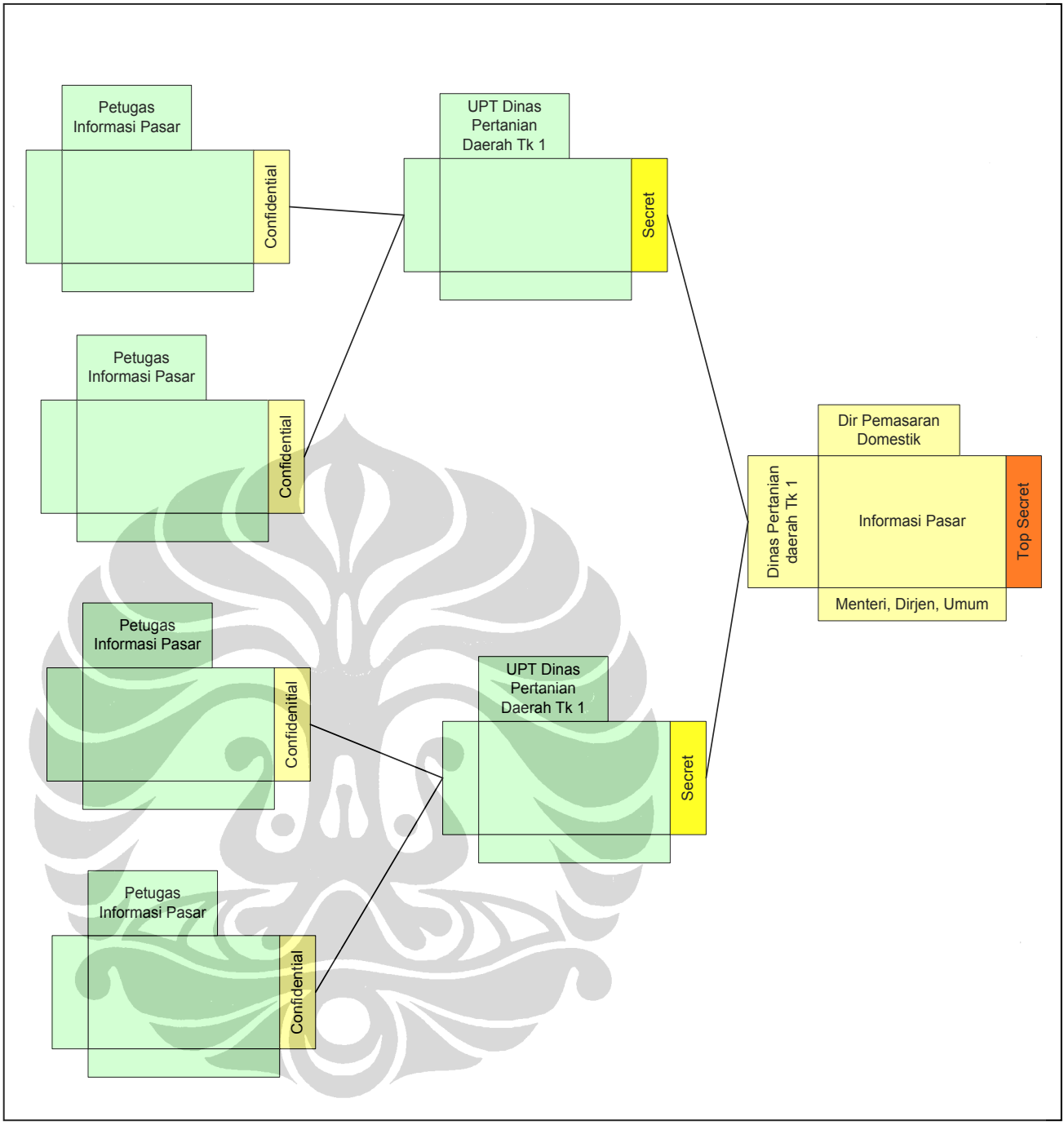
Tahap berikutnya sebagai pengejawantahan dari kebijakan kemanan informasi adalah menentukan model keamanan informasi yang sesuai dengan kebutuhan Departemen Pertanian. Berdasarkan observasi, diperlukan suatu model keamanan informasi yang membagi jenis informasi berdasarkan tingkat kerahasiannya.

Sebagai contoh, informasi harga komoditi pertanian, sebelum di sebarluaskan kepada umum, maka informasi harga yang berasal dari dinas pertanian di daerah harus dijaga kerahasiaannya supaya data tersebut tidak dimanfaatkan oleh spekulan sebelum sampai ke tingkat eselon 1 atau menteri. Model keamanan yang mengakomodasi hal ini adalah model Bell Lapadua, Model ini diperlihatkan pada gambar 4.2



Gambar 4.2 Model Bell Lapadua sebagai model keamanan informasi Deptan

Pengejawantahan dari model ini adalah dengan memperhatikan business dependency diagram Deptan yang tercantum pada Dokumen Proses Bisnis, seperti terlihat pada gambar 4.3



Gambar 4.3 Implementasi model keamanan informasi Deptan

Dari ilustrasi di atas dapat diketahui bahwa petugas informasi pasar di daerah mengirimkan informasi yang seharusnya sudah diberi label *confidential*, informasi ini kemudian diteruskan ke Dinas Pertanian Daerah, yang merekap seluruh informasi yang berasal dari petugas informasi pasar. Data rekapan kemudian diberi label *Secret* untuk menjaga kerahasiaan dan meminimalisir penyalahgunaan informasi oleh pihak lain. Informasi dari masing-masing Dinas

inilah yang kemudian di teruskan ke Direktorat Pemasaran Domestik Ditjen P2HP untuk diteruskan ke menteri. Informasi yang mencakup hasil pemasaran di seluruh daerah di Indonesia inilah yang kemudian dilaporkan ke menteri. Informasi yang sudah diolah di eselon 1 ini kemudian di labelkan sebagai informasi *top secret* karena berkaitan dengan kebijakan yang akan ditempuh oleh menteri dan jajaran eselon 1 di Deptan terutama Ditjen P2HP.

Implementasi dari model atau arsitektur informasi ini dapat berupa perangkat lunak maupun perangkat keras yang mencegah adanya perubahan informasi oleh pihak yang tidak berwenang. Penggunaan firewall server adalah salah satu upaya mereduksi perubahan informasi oleh pihak yang tidak berwenang selain penerapan fitur otentikasi dan verifikasi untuk akses ke sumber informasi.

4.1.3 Prosedur Keamanan Pertukaran Informasi

Harapan dari terpenuhinya aspek ini adalah adanya kebijakan, prosedur, dan kendali-kendali pertukaran informasi yang formal untuk melindungi pertukaran informasi melalui penggunaan semua jenis fasilitas komunikasi.

Prosedur dan kendali yang harus dipatuhi ketika menggunakan fasilitas komunikasi elektronik untuk pertukaran informasi seharusnya meninjau aspek berikut :

1. Prosedur dirancang untuk melindungi informasi yang dipertukarkan dari pemotongan atau penghilangan sebagian, penggandaan, modifikasi, kesalahan alamat, dan perusakan data
2. Prosedur untuk mendeteksi dan melindungi kode-kode berbahaya yang dapat di kirim melalui penggunaan media komunikasi elektronik, seperti email
3. Prosedur untuk melindungi informasi elektronik sensitif yang dikomunikasikan melalui metode attachment
4. Kebijakan atau panduan secara garis besar mengenai penggunaan yang dapat ditoleransi terhadap fasilitas komunikasi elektronik.
5. Prosedur dalam penggunaan komunikasi nirkabel dan beberapa resiko spesifik yang diakibatkannya

6. Pertanggungjawaban pegawai, pihak ketiga, kontraktor, dan setiap pengguna untuk tidak membahayakan organisasi melalui kegiatan yang membahayakan organisasi
7. Menggunakan teknik kriptografi untuk melindungi kerahasiaan, integritas, dan keaslian dari informasi
8. Panduan dalam proses pemberhentian perjanjian kerjasama dengan organisasi lain, termasuk pemusnahan dokumen-dokumen penting yang berkaitan dengan surat perjanjian kerjasama.
9. Tidak meninggalkan informasi yang sensitif atau kritis pada fasilitas percetakan, seperti mesin fotokopi, printer, atau mesin faks karena dapat dimanfaatkan oleh pihak yang tidak berwenang
10. Pengendalian dan pembatasan fasilitas komunikasi seperti pengiriman secara otomatis e-mail ke alamat e-mail di luar Deptan
11. Mengingatkan personil untuk berhati-hati dalam memberikan alamat email atau informasi pribadi lainnya, untuk mencegah koleksi data oleh pihak yang tidak berwenang.

4.2 Ruang Lingkup Sistem Manajemen Keamanan Informasi

4.2.1 Aspek Fisik

Berdasarkan observasi dan wawancara, pengamanan yang sifatnya fisik sampai saat ini belum terdefinisikan di Deptan. Pembangunan sarana dan fasilitas informasi yang ada belum memiliki wawasan keamanan informasi sebagaimana yang telah ditetapkan berbagai standar keamanan. Beberapa diantaranya dapat diobservasi melalui kegiatan kunjungan lapangan yang dilakukan di beberapa unit eselon 1 dan 2 Deptan sebagai berikut :

Tabel 4.4 Hasil Kunjungan Lapangan

Unit	Pengaksesan Ruangan Pengolahan Data		Pengamanan Pintu Ruangan Pengolahan Data		Pengamanan Jendela Ruangan Pengolahan Data		Ketersediaan Pendingin Udara			Ketersediaan Tenaga Listrik			Perlindugan Terhadap Gangguan Tikus		Alat Deteksi Asap dan Pemadam Kebakaran		
	hak akses	ruangan tersendiri	kunci pintu	kebijakan pemegang kunci	jendela	teralis	AC	Kondisi	perawatan berkala	UPS	Generator	kapabilitas	Ancaman	Perlindungan	Detektor	Pemadam kebakaran	Kondisi
Ditjen Hortikultura	tidak ada	tidak	ya	tidak	ya	tidak	2 unit	1 dalam kondisi mati	ya	ya	tidak	kurang memadai	Tidak ada	Tidak ada	tidak ada	ada di koridor ruangan	kurang sosialisasi
Pusdatin	ada, namun belum formal	ya	ya	ada, namun belum formal	ya	tidak	2 unit	baik	ya	ya	ya	cukup memadai	ya	kabel anti tikus	ada, namun tidak pernah di uji coba	ada di koridor ruangan	kurang sosialisasi
Badan SDM Pertanian	tidak ada	ya	ya	petugas security	ya	tidak	AC Central	baik	ya	ya	ya	cukup memadai	ya	sinyal penggang gu, racun tikus, perangkap tikus	ada, namun tidak berfungsi	ada di koridor ruangan	kurang sosialisasi
Pelindungan Varietas Tanaman	ada, namun belum formal	ya	ya	ada, namun belum formal	ya	tidak	I unit	baik	ya	ya	ya	cukup memadai	Tidak ada	Tidak ada	tidak ada	ada di koridor ruangan	kurang sosialisasi

Berdasarkan hasil tinjauan lapangan dapat diketahui bahwa belum ada kebijakan keamanan sistem informasi yang berlaku di Deptan yang berkaitan dengan aspek fisik. Deptan belum memiliki kebijakan ataupun aturan yang diterapkan secara menyeluruh di semua unit kerja di lingkungan Deptan. Beberapa unit sudah memiliki sistem pengamanan secara fisik yang memadai namun lebih banyak unit yang belum memilikinya.

Aspek keamanan fisik bertujuan untuk melindungi aset Deptan dari serangan ataupun ancaman yang dilancarkan melalui kelemahan fisik. Tahapan awal dari perencanaan pengamanan informasi ditinjau dari aspek fisik ini adalah dengan mendefinisikan wilayah aman (secure areas) yang ada di lingkungan Deptan. Kriteria dari wilayah aman ini meliputi suatu gedung atau ruangan yang di dalamnya terdapat media penyimpan data seperti data center atau peralatan pemrosesan data seperti ruang server dan ruang komputer.

Tinjauan atas aspek fisik dilakukan untuk melindungi akses secara fisik oleh pihak yang tidak berwenang dan terjadinya perusakan aset tersebut. Fasilitas pemrosesan informasi yang kritis dan sensitif harus ditempatkan di wilayah aman dan terlindungi oleh sistem pengamanan yang telah terdefinisi, dengan pembatas keamanan dan kendali keamanan yang sesuai dengan kebutuhan aset.

4.2.1.1 Keamanan Fisik Gedung/Ruangan

Untuk setiap bangunan atau ruangan terdapat tiga tingkat keamanan yang harus diimplementasikan, yaitu :

1. Wilayah Umum

   Wilayah perlindungan tingkat pertama ini memiliki konsekuensi kerugian aset yang paling kecil daripada wilayah lain, meliputi seluruh area umum di lingkungan gedung. Untuk teknik yang dapat digunakan pada wilayah ini sederhananya bisa dalam bentuk pemeriksaan kartu identitas oleh pihak keamanan gedung dan kewajiban dalam menggunakan kartu identitas.

2. Wilayah terbatas (*Limited Areas*)

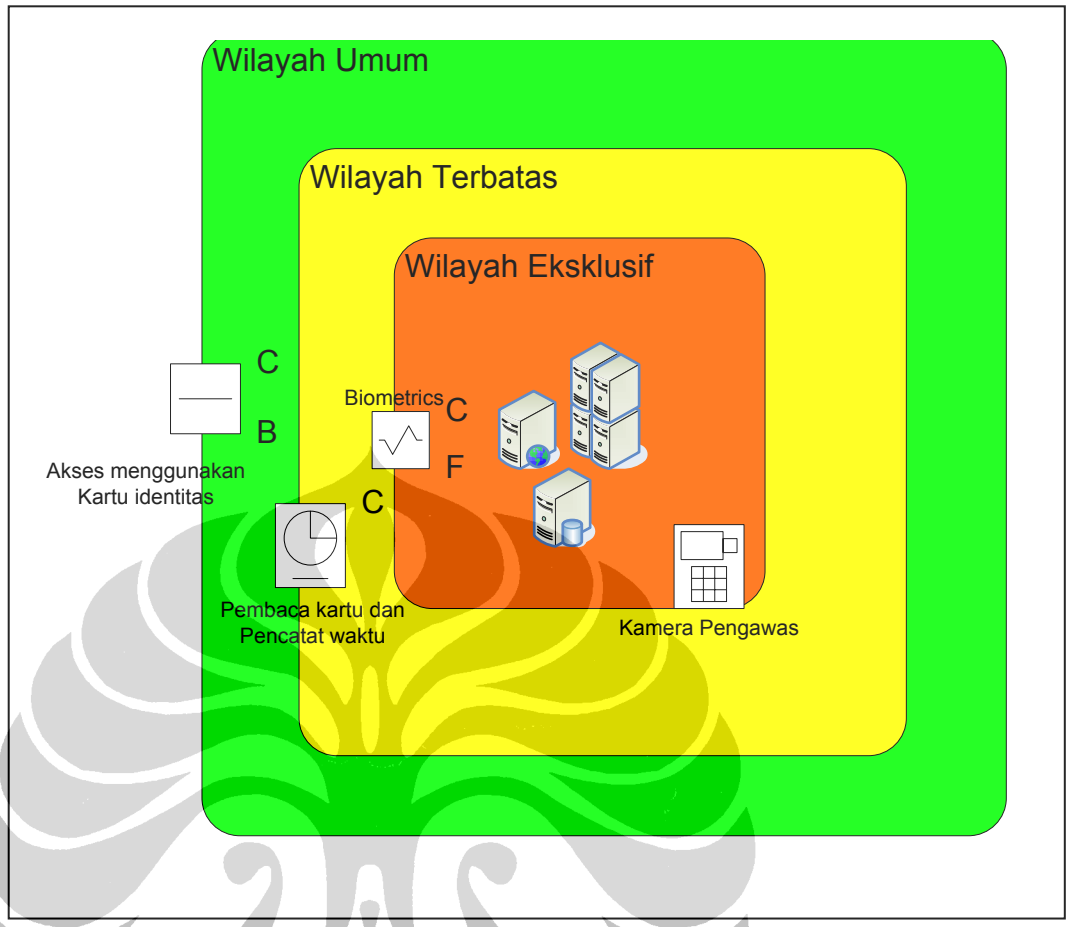
   Wilayah terbatas ini memiliki tingkat konsekuensi kerugian aset yang lebih besar daripada wilayah wilayah perlindungan. Wilayah ini meliputi ruang

administrasi dan ruang staf. Untuk memasuki wilayah ini setiap staf memiliki kartu identitas yang unik yang berfungsi sebagai alat akses masuk dan pencatat waktu masuk dan keluar ruangan.

3. Wilayah Eksklusif (*Exclusion Areas*)

Wilayah eksklusif meliputi ruang data center, ruang server maupun ruang perlengkapan jaringan seperti hub dan switch. Wilayah ini membutuhkan tingkat keamanan yang paling tinggi karena memiliki konsekuensi kerugian paling tinggi apabila terkena serangan dan mengalami gangguan. Akses masuk ke dalam ruangan ini terbatas hanya untuk beberapa orang, yaitu petugas harian seperti administrator dan pimpinan TI pada unit kerja yang bersangkutan. Teknik yang digunakan dapat berupa *biometrics* menggunakan sidik jari dan dilengkapi dengan kamera pengawas.

Gambaran secara logik terhadap perencanaan fisik dapat diamati pada gambar 4.4 Fokus perhatian di dalam pembahasan ini adalah tinjauan terhadap wilayah eksklusif atau ruangan yang dapat berupa ruang server / data center.



Gambar 4.4 Pembagian wilayah berdasarkan tingkat kekritisan aset

Tabel 4.2 Perangkat atau proses yang dibutuhkan untuk setiap wilayah

No	Perangkat /Proses	Area	Penjelasan
1	Pemeriksaan kartu identitas oleh petugas keamanan	Wilayah umum	Kartu identitas harus dengan jelas menyebutkan status dari pihak yang memasuki ruangan dan petugas keamanan wajib mengingatkan untuk selalu menggunakan kartu identitas tersebut
2	Mesin pemeriksa kartu identitas	Wilayah terbatas	Untuk memeriksa keabsahan pegawai, dapat pula disertai pencatat waktu masuk dan keluar pegawai

Tabel 4.2 Perangkat atau proses yang dibutuhkan untuk setiap wilayah (cont.)			
No	**Perangkat /Proses**	**Area**	**Penjelasan**
3	Biometrics	Wilayah Eksklusif	Dapat berupa pemeriksa sidik jari yang dilengkapi dengan password
4	Kunci Pintu Ganda atau terprogram	Wilayah Eksklusif	Berupa kunci tambahan atau gembok dengan pemegang kunci yang dibatasi
5	Kamera Pengawas	Wilayah Eksklusif	Berfungsi memantau kegiatan seseorang yang berada di dalam ruangan atau keluar masuk ruangan
6	Petugas keamanan di luar ruangan wilayah eksklusif	Wilayah Eksklusif	Berfungsi untuk mengontrol keamanan di sekitar wilayah eksklusif.
7	Pemadam kebakaran dalam bentuk Halon	Wilayah Eksklusif dan Terbatas	Untuk menghindari kerusakan peralatan apabila terjadi pemadaman
8	Pengkondisi Udara (AC)	Wilayah Eksklusif dan Terbatas	Kondisi ruangan harus terjaga agar tetap sesuai standar
9	Alat Pengukur Suhu dan Kelembaban	Wilayah Eksklusif	Digunakan untuk menjaga suhu supaya tetap stabil
10	Generator dan Stabilizer	Wilayah Eksklusif dan terbatas	Generator digunakan sebagai cadangan energi listrik sedangkan stablizer digunakan untuk menjamin stabilnya tegangan listrik
11	Pelabelan Kabel	Wilayah Eksklusif dan terbatas	Digunakan untuk memudahkan penelusuran apabila terjadi kerusakan kabel listrik maupun jaringan
12	Pelapis Alas Ruangan	Wilayah Eksklusif	Digunakan untuk mengurangi gejala elektrostatik pada ruangan

Perlindungan secara fisik didapat dengan menciptakan satu atau beberapa batasan fisik di sekeliling fasilitas. Penggunaan lebih dari satu jenis perlindungan akan memberikan kekuatan tambahan yang dapat menjadi back up apabila satu perlindungan berhasil ditembus.

4.2.1.2 Kendali Keluar Masuk Ruangan

Wilayah aman harus terlindungi dengan kendali untuk menjamin bahwa hanya pihak yang berwenang yang memiliki akses.

Panduan berikut harus diterapkan, yaitu :

1. Waktu masuk dan keluarnya pengunjung fasilitas harus senantiasa tercatat, dan semua pengunjung fasilitas harus dikawal walaupun telah memiliki izin akses.
2. Akses ke area-area yang mengolah informasi sensitif harus terkendali dan dibatasi hanya untuk pihak tertentu yang berwenang.
3. Seluruh pegawai maupun pihak ketiga harus diminta untuk menunjukan kartu identitas pegawai maupun kartu identitas pengunjung apabila memasuki fasilitas
4. Hak akses ke fasilitas penting dan sensitif harus secara reguler direvisi atau terupdate.

4.2.1 Aspek Teknis

Secara formal, belum ada kebijakan mengenai pengamanan secara teknis terhadap aset yang di miliki Deptan. Belum adanya klasifikasi terhadap aset juga menjadi kendala tersendiri dalam melakukan kajian resiko pada masing-masing aset. Berdasarkan kuesioner maka di dapatlah gambaran mengenai aset pendukung informasi dan klasifikasinya serta besarnya resiko yang di miliki akibat adanya serangan dari luar atau bahkan akibat kelemahan dari aset itu sendiri berdasarkan studi literatur.

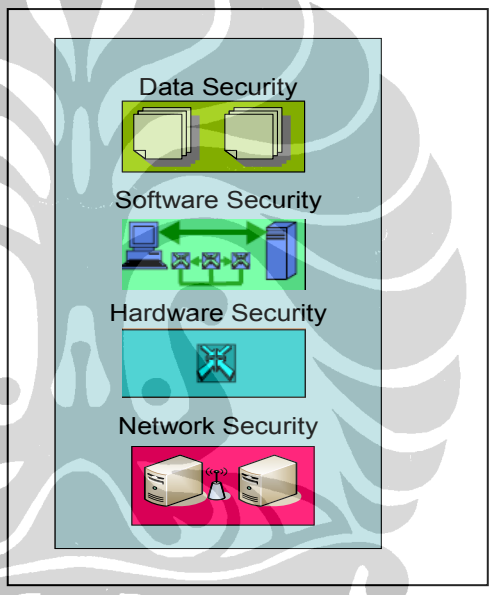
4.2.2.1 Klasifikasi Aset

Untuk memudahkan pengkajian (*assessment*) maka ditinjau berdasarkan fungsinya terhadap informasi, aset di Departemen Pertanian dapat dibagi menjadi

empat jenis, yaitu data, perangkat lunak, perangkat keras, dan perangkat jaringan komunikasi. Hal ini diilustrasikan pada gambar 4.5

Pengklasifikasian aset berdasarkan fungsi juga memudahkan dalam membentuk lapisan keamanan informasi. Adanya lapisan keamanan sistem informasi ini mempermudah dalam memanaje resiko, mitigasi apabila ada bencana, dan meningkatkan aspek penatakelolaan keamanan TI yang baik di Deptan.

Secara garis besar, lapisan keamanan sistem informasi di Deptan dapat di bagi atas empat lapisan, yaitu data atau informasi, perangkat lunak, perangkat keras, dan jaringan komunikasi.



Gambar 4.5 Klasifikasi aset untuk membentuk lapisan keamanan sistem informasi

Berikut ini adalah uraian masing-masing asset :

1. **Data/informasi**

Data berperan sangat strategis dalam kegiatan operasional maupun pembuatan kebijakan oleh pimpinan. Data yang berkualitas yaitu akurat dan cepat tentunya harus dilengkapi dengan pemenuhan aspek keamanan seperti kerahasiaan, integritas, dan ketersediaan. Berkurangnya aspek kerahasiaan,

integritas, dan ketersedaiaan tentunya akan menghambat kegiatan operasional dan pembuatan kebijakan di lingkungan Departemen Pertanian.

Tujuan dari klasifikasi data/informasi pada dasarnya adalah untuk menjamin bahwa data/informasi mendapatkan tingkat perlindungan sesuai dengan karakteristiknya dan kebutuhan organisasi. Informasi selayaknya diklasifikasi berdasarkan kebutuhan, prioritas, dan derajat keamanan yang diharapkan oleh pengguna informasi. Informasi memiliki derajat atau tingkat sensitivitas dan kekritisan yang berbeda. Beberapa informasi mungkin membutuhkan perlakuan keamanan khusus. Skema atau alur dari klasifikasi informasi seharusnya digunakan untuk mendefinisikan tingkat perlindungan dan mengkomunikasikan kebutuhan akan perlindungan khusus. Klasifikasi informasi dalam hal ini dapat terdiri antara lain :

a. Tingkat Kerahasiaan

Tingkat Kerahasiaan	
Level	Deskripsi
1	Apabila data diketahui oleh orang yang tidak berhak tidak mengganggu kegiatan operasional
2	Apabila data diketahui orang yang tidak berhak maka dapat mengganggu kegiatan operasional
3	Apabila data diketahui orang yang tidak berhak maka dapat menghentikan kegiatan operasional

b. Tingkat Ketersediaan

Tingkat Ketersediaan	
Level	Deskripsi
1	Ketiadaan data tidak akan menghambat kegiatan operasional
2	Ketiadaan data akan menghambat kegiatan operasional
3	Ketiadaan data akan menghentikan kegiatan operasional

c. Tingkat Integritas

Tingkat Integritas		
Level	Deskripsi	
1	Perubahan data dari orang yang tidak berhak tidak akan mengganggu kegiatan operasional	Inkonsistensi data tidak berpengaruh terhadap pengambilan keputusan
2	Perubahan data dari orang yang tidak berhak akan mengganggu kegiatan operasional	Inkonsistensi data mengurangi tingkat akurasi dalam pengambilan keputusan oleh Menteri
3	Perubahan data oleh orang yang tidak berhak akan menghentikan kegiatan operasional	Inkonsistensi data menjadi perhatian publik dan mengurangi citra baik institusi

d. Tingkat Kepentingan untuk menteri

Tingkat Kepentingan untuk menteri	
Level	Deskripsi
1	Data sama sekali tidak dibutuhkan oleh menteri
2	Data dibutuhkan secara tidak langsung oleh menteri, artinya data harus melalui proses lebih lanjut untuk dapat dimanfaatkan oleh menteri
3	Data dibutuhkan secara langsung oleh menteri

e. Tingkat Kepentingan untuk Dirjen

Tingkat Kepentingan untuk Dirjen	
Level	Deskripsi
1	Data sama sekali tidak dibutuhkan oleh Dirjen
2	Data dibutuhkan secara tidak langsung oleh Dirjen artinya data harus melalui proses lebih lanjut untuk dapat dimanfaatkan oleh Dirjen
3	Data dibutuhkan secara langsung oleh Dirjen

Klasifikasi Informasi selayaknya diimplementasikan dengan pemberian label tiap informasi dalam berbagai bentuk dan format. Langkah pertama bagi Deptan adalah pelabelan informasi yang dapat di implementasikan di bagian depan atau sampul informasi dengan berbagai keterangan tentang informasi.

Label ini lengkap dengan keterangan tingkat kerahasiaan, tingkat integritas, dan tingkat ketersediaan dan harus dicantumkan pula dari mana sumber informasi, dan ke mana informasi akan diserahkan. Untuk data yang memiliki

format elektronik penamaan informasi juga harus terstandarisasi, memiliki password untuk menjamin bahwa data tidak dibaca oleh pihak yang tidak berwenang, dan harus jelas mencantumkan nama institusi yang menciptakannya

2. Perangkat Lunak

Difokuskan pada keamanan sistem operasi, aplikasi yang di gunakan untuk memasukan (input) informasi, aplikasi pemrosesan informasi, serta aplikasi penyebaran informasi (diseminasi). Lapisan ini juga memperhatikan aplikasi jaringan dan aplikasi basis data.

Aspek keamanan terhadap perangkat lunak sebagai media dihasilkannya informasi merupakan tantangan tersendiri di Deptan, karena jumlah eselon 1 yang relatif banyak dan kebutuhan masing-masing eselon 1 yang sangat spesifik dalam menjalankan tupoksinya. Dalam mengantisipasi hal itu, Departemen Pertanian belum memiliki standar baku pengamanan yang berlaku bagi seluruh eselon 1 mengenai perangkat lunak, termasuk aspek pengembangan, implementasi, sampai review terhadap implementasi.

Tidak semua pegawai dapat melakukan instalasi perangkat lunak. Kebutuhan pengamanan terhadap perangkat lunak pun diharapkan berlapis. Sebagaimana terlihat dari hasil survey bahwa sistem operasi memiliki nilai resiko tertinggi setelah data, maka perlu diimplementasikan sistem otentikasi dan otorisasi sebelum seseorang dapat memasuki sistem operasi. Aplikasi anti virus juga harus diperhatikan sehubungan dengan fakta bahwa virus merupakan ancaman yang paling sering menyerang aset. Aplikasi anti virus harus selalu di-update untuk menjamin kehandalan aplikasi.

3. Perangkat Keras

Berbagai kegiatan operasional maupun pembuatan kebijakan membutuhkan perlakuan khusus terhadap sarana atau fasilitas di hasilkan, disimpan, dan di sebarkannya informasi. Departemen Pertanian dalam hal ini belum memiliki standar yang baku mengenai pengamanan secara khusus terhadap aset perangkat keras yang berlaku secara luas di seluruh eselon 1.

Serupa dengan aset data, maka aset perangkat keras juga selayaknya terklasifikasi untuk mengoptimalkan strategi keamanan bagi masing-masing perangkat yang sesuai dengan kekritisan perangkat tersebut bagi kegiatan pelaporan di Deptan. Berbagai hal lainnya seperti harga perangkat atau tingkat kesulitan perawatan juga dapat menjadi variabel tambahan dalam proses klasifikasi perangkat keras ini.

Setelah dilakukan klasifikasi, hal yang sangat penting dilakukan adalah melakukan pelabelan. Setiap aset perangkat keras harus memiliki label yang mencerminkan tingkat kaamanan yang dibutuhkan bagi aset tersebut. Di dalam label juga terdapat nomor identifikasi setiap aset yang unik sehingga memudahkan pencatatan dan pengarsipan secara elektronik. Pelabelan juga mempercepat penanganan dan meningkatkan keakuratan apabila aset mengalami gangguan.

Jenis ancaman yang mungkin ada tentunya berbeda antara satu perangkat dengan perangkat lainnya. Identifikasi ancaman harus diperbaharui secara periodik untuk mengantisipasi kemungkinan ancaman yang berubah secara cepat. Untuk itu perlu adanya berbagi pengetahuan antar unit kerja yang ada di Deptan mengenai ancaman dan kelemahan yang mungkin mengganggu kegiatan. Deptan juga diharapkan memiliki semacam tabel akses tentang personil siapa saja yang berhak menggunakan aset. Penanggungjawab aset juga berkewajiban mereview tabel ini secara berkala.

4. Perangkat Jaringan Komunikasi

Pemanfaatan media komunikasi data sebagai sarana untuk mempercepat pelaporan maupun dalam memperoleh data sudah sangat luas implementasinya di Deptan. Bervariasinya kebutuhan kecepatan maupun kapasitas media komunikasi data merupakan tantangan tersendiri dalam merancang keamanan jaringan yang ideal diterapkan di lingkungan Departemen Pertanian, namun hal ini belum diantisipasi dengan tiadanya dokumen mengenai keamanan jaringan secara khusus.

Aset jaringan komunikasi di Deptan selayaknya merupakan integrasi dari beberapa prinsip keamanan jaringan.

Diantaranya adalah :

- Otentikasi

  Untuk melindungi Network Deptan dari ancaman penyamaran atau ancaman dari pintu belakang. Mekanisme yang digunakan dapat berupa Digital Signature, Enkripsi, Timestamp dan Password

- Integritas Pesan

  Melindungi header protokol, informasi routing, dan modifikasi isi pesan. Mekanisme yang digunakan berupa otentikasi dan enkripsi pesan

- Non Repudiation

  Menjamin bahwa pengirim pesan tidak dapat menyangkal bahwa dirinya telah mengirim pesan. Mekanisme yang digunakan berupa enkripsi, digital signature, dan pencegahan terhadap Denial of Service.

- Keberlangsungan Operasional

  Memastikan bahwa jaringan tetap beroperasi walaupun terjadi serangan. Mekanisme untuk aspek ini meliputi redundansi sistem dan kemampuan untuk melakukan konfigurasi ulang parameter network ketika terjadi serangan

- Manajemen Jaringan

  Memantau kinerja jaringan dan mengidentifikasi serangan dan gangguan. Mekanisme yang dapat digunakan adalah menggunakan komponen jaringan yang memungkinkan administrator jaringan melakukan pemantauan dan membatasi akses.

- Kerahasiaan Data

  Melindungi data terakses oleh pihak yang tidak berwenang selama proses transmisi. Mekanisme yang digunakan berupa kontrol akses, enkripsi, dan proteksi secara fisik terhadap kabel jaringan.

- Kerahasiaan Aliran Lalu Lintas Data

  Menjamin bahwa rute informasi atau frekuensi tidak diketahui oleh pihak yang tidak berwenang melalui analisa lalu lintas aliran data.

- *Selective Routing*

  Memanaje rute pesan sehingga mampu menghindari serangan. Mekanisme yang digunakan meliputi konfigurasi jaringan dan implementasi tabel-tabel routing.

Berdasarkan delapan aspek keamanan jaringan yang di rekomendasikan oleh standar BS 17799, maka beberapa mekanisme yang krusial untuk diterapkan adalah :

1. Melakukan enkripsi terhadap data yang akan dikirim melalui jaringan untuk menjamin kerahasiaan dan integritas data
2. Redundansi sistem jaringan seperti server maupun router untuk menjamin ketersediaan layanan jaringan walaupun terjadi serangan.
3. Memastikan bahwa komponen sistem jaringan yang ada dapat dipantau kinerjanya dan admin jaringan mampu melakukan pembatasan akses.
4. Mengimplementasi perangkat lunak untuk memanaje lalu lintas data pada jaringan dan tabel-tabel routing untuk mengetahui aliran data pada jaringan Deptan
5. Manajemen terhadap aset jaringan, seperti memberikan lapisan pelindung bagi kabel jaringan dan melakukan pelabelan terhadap setiap aset termasuk kabel jaringan.

Jaringan di Deptan seharusnya termanaje dan terkendali untuk melindunginya dari serangan pihak luar, dan untuk memelihara keamanan sistem informasi ataupun aplikasi yang menggunakan jaringan.

Kepala Bidang Jaringan komunikasi di Deptan harus menerapkan kendali-kendali untuk menjamin keamanan informasi di dalam jaringan dan perlindungan dari layanan yang ada terkoneksi melalui akses pihak yang tidak berwenang. Secara khusus, hal-hal di bawah ini harus dipertimbangkan

a. Penanggungjawab operasional untuk jaringan (*network admin*) seharusnya dipisahkan dengan penanggungjawab operasional komputer (*system admin*).
b. Penanggungjawab dan prosedur untuk peralatan remote termasuk yang berada di area pengguna harus diimplementasikan

c. Kendali khusus harus di rancang untuk melindungi kerahasiaan dan integritas data yang melalui jaringan publik atau melalui jaringan nirkabel, dan untuk melindungi sistem-sistem informasi ataupun aplikasi. Kendali khusus juga dibutuhkan untuk memelihara ketersediaan layanan jaringan dan komputer-komputer yang tersambung dengan jaringan.
d. Daftar log dan riwayat monitoring jaringan harus diterapkan untuk memungkinkan pembuatan rencana atau tindakan keamanan yang relevan.
e. Aktivitas manajemen seharusnya dikoordinasikan dengan intens, selain untuk mengoptimalkan layanan kepada organisasi juga untuk menjamin bahwa kendali-kendali secara konsisten telah diterapkan pada seluruh infrastruktur pemrosesan informasi.

Departemen Pertanian, yang dalam hal ini bertindak sebagai konsumen terhadap layanan komunikasi harus mengimplementasi *Service Level Agreement* (SLA) dengan penyedia layanan dan memeliharanya dalam suatu konsep *Service Level Management* (SLM).

Sebelum memanfaatkan layanan, maka harus diteliti terlebih dahulu kelengkapan-kelengkapan keamanan, tingkat-tingkat layanan, dan kebutuhan manajemen terhadap seluruh layanan jaringan harus diidentifikasi dan termasuk setiap persetujuan layanan jaringan, baik layanan yang disediakan oleh Deptan sendiri dalam hal ini Pusdatin maupun yang disediakan oleh penyedia layanan.

Kemampuan dari penyedia layanan jaringan (*network service provider*) untuk memanaje layanan yang telah disepakati bersama dengan mempertimbangkan aspek keamanan harus ditentukan dan secara berkala dimonitor, serta harus disepakati juga hak untuk mengauditnya.

Pengaturan-pengaturan keamanan yang penting untuk layanan-layanan khusus seperti fitur-fitur keamanan, tingkat-tingkat layanan, dan kebutuhan-kebutuhan manajemen harus teridentifikasi. Departemen Pertanian harus memastikan bahwa *network service provider* mengimplementasikan hal-hal tersebut.

Yang di maksud dengan fitur-fitur keamanan adalah :

a. Teknologi yang digunakan untuk keamanan layanan jaringan, seperti autentikasi, enkripsi, dan kendali-kendali koneksi jaringan.
b. Parameter teknis yang dibutuhkan untuk berkoneksi secara aman dengan layanan jaringan berdasarkan aturan keamanan dan koneksi jaringan.
c. Prosedur-prosedur untuk penggunaan layanan jaringan untuk membatasi akses kepada layanan jaringan atau aplikasi yaitu hanya ketika dibutuhkan saja.

4.3 Penilaian Resiko-resiko Terhadap Aset

Resiko dalam sistem informasi adalah segala kemungkinan (*likelihood*) yang dapat dimanfaatkan oleh serangan (*threat*). Resiko terkadang juga tidak dapat terhindari, jadi organisasi seyogyanya mampu menerima tingkatan tertentu dari resiko. Resiko dalam berbagai konteks adalah gabungan dari beberapa faktor diantaranya serangan (segala sesuatu yang membahayakan), kelemahan (keterbukaan terhadap serangan), dan nilai aset itu sendiri (seberapa besar dampak apabila asset tersebut tidak ada). Peningkatan terhadap salah satu faktor akan meningkatkan faktor resiko secara umum (Finne 1998).

4.3.1 Identifikasi Ancaman (*Threat*)

Ancaman, menurut *National Institute of Standards and Technology* (NIST) Amerika Serikat, adalah segala sesuatu yang berasal dari sumber ancaman dan dapat memanfaatkan kelemahan. Pada dasarnya ancaman dapat di bagi menjadi 3 jenis berdasarkan sumbernya, diantaranya adalah :

1. Ancaman yang berasal dari bencana alam

   Contohnya adalah banjir, gempa bumi, badai.

2. Ancaman yang berasal dari manusia

   Dapat berupa hal yang disengaja ataupun tidak dari manusia dan dapat bersumber dari dalam maupun luar lingkungan organisasi. Contohnya adalah kesalahan dalam melakukan konfigurasi sistem operasi, kesalahan dalam memasukkan data, serangan melalui jaringan, akses pihak yang

tidak berwenang terhadap informasi yang sifatnya rahasia, dan lain sebagainya.

3. Ancaman Lingkungan

Disebabkan oleh kondisi lingkungan, seperti matinya aliran listrik, polusi, bahan kimia berbahaya, dan lain sebagainya.

Berdasarkan hasil survey yang di lakukan oleh NIST USA, maka dapat diketahui bahwa ancaman yang bersumber dari manusia adalah sumber ancaman yang paling berbahaya terhadap keamanan informasi organisasi. Berdasarkan observasi lapangan maka di dapat beberapa sumber ancaman yang ada di Departemen Pertanian.

4.3.2 Identifikasi Kelemahan

Kelemahan (*vulnerability*) adalah cacatnya atau lemahnya prosedur keamanan, rancangan, atau implementasi sistem informasi di organisasi.

Berdasarkan observasi dan studi literatur maka pada Departemen Pertanian terdapat beberapa kelemahan. Kelemahan dan ancaman yang ada pada tiap aset disajikan pada lampiran B dokumen.

Berdasarkan tabel klasifikasi aset yang sudah dibahas pada subbab sebelumnya, maka perlu diketahui frekuensi kejadian serangan atau ancaman terhadap aset dalam setahun dan perkiraan besarnya dampak yang dialami Deptan apabila aset tidak dapat digunakan akibat adanya kelemahan yang di manfaatkan oleh serangan atau ancaman.

Tabel 4.3 memberi gambaran definisi pengaruh suatu dampak terhadap kegiatan pelaporan di Deptan.

Tabel 4.3 Pengkategorian nilai dampak

Kategori Nilai Dampak	Penjelasan
Kecil	Tidak menghambat kegiatan pelaporan ke menteri
Sedang	Keterlambatan dalam dihasilkannya data
Besar	Data tidak bisa dihasilkan dalam jangka waktu panjang

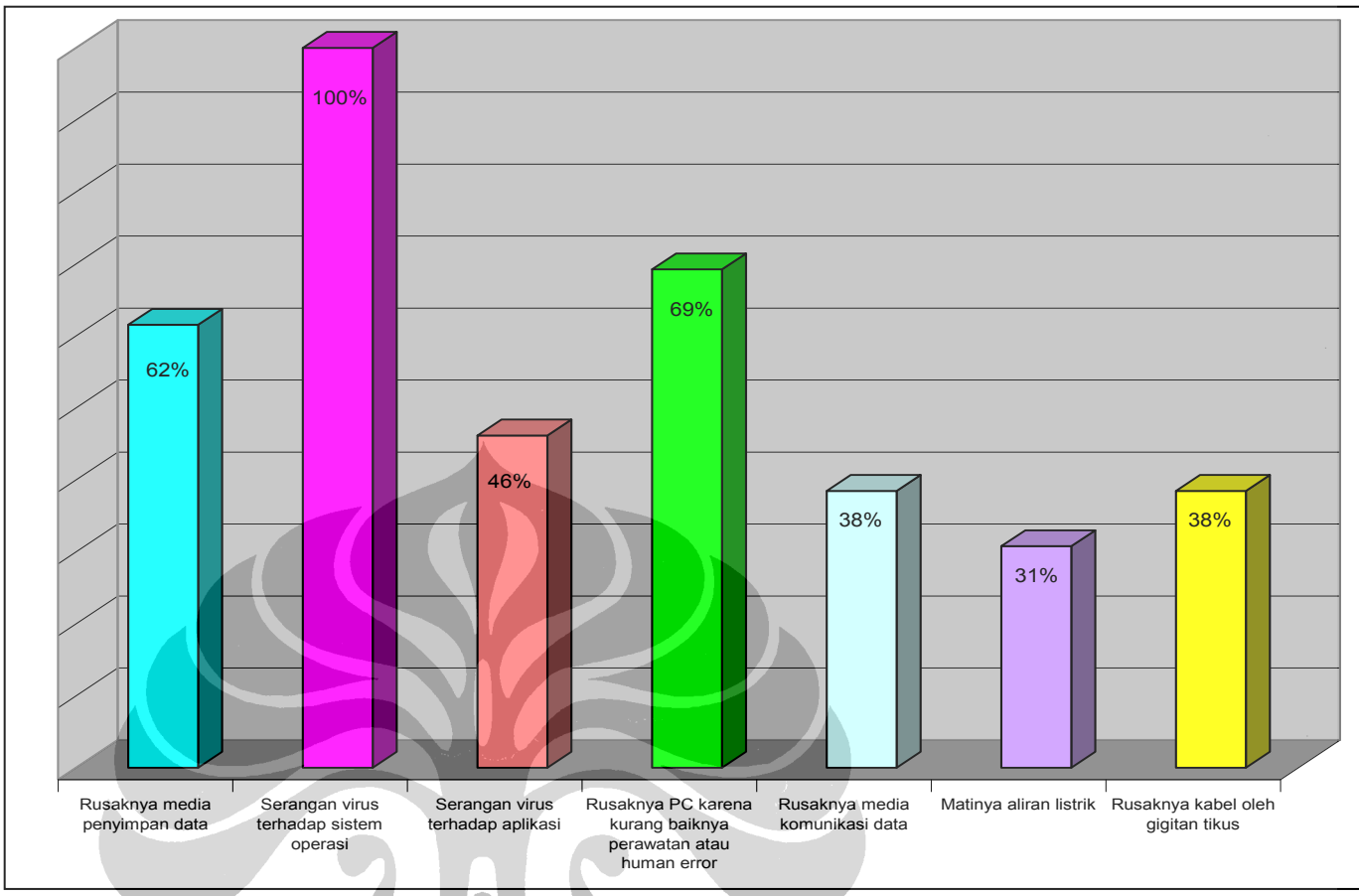
Tabel 4.4 Nilai resiko oleh kemungkinan terjadi serangan dan nilai dampak

Kemungkinan Terjadi		Nilai Dampak		Resiko	
1	Tidak pernah	1	Kecil	1-24	Diterima
2	Kadang-kadang	2	Sedang	25-49	Dikurangi
3	Sering	3	Besar	50-100	Tidak Diterima

Berdasarkan pengkajian resiko yang di dapat dari kuisioner, maka didapat profil keamanan di 12 Eselon 1 dan 2 Departemen Pertanian yang ditampilkan pada Lampiran C

4.3.3 Analisa Hasil Kuisioner

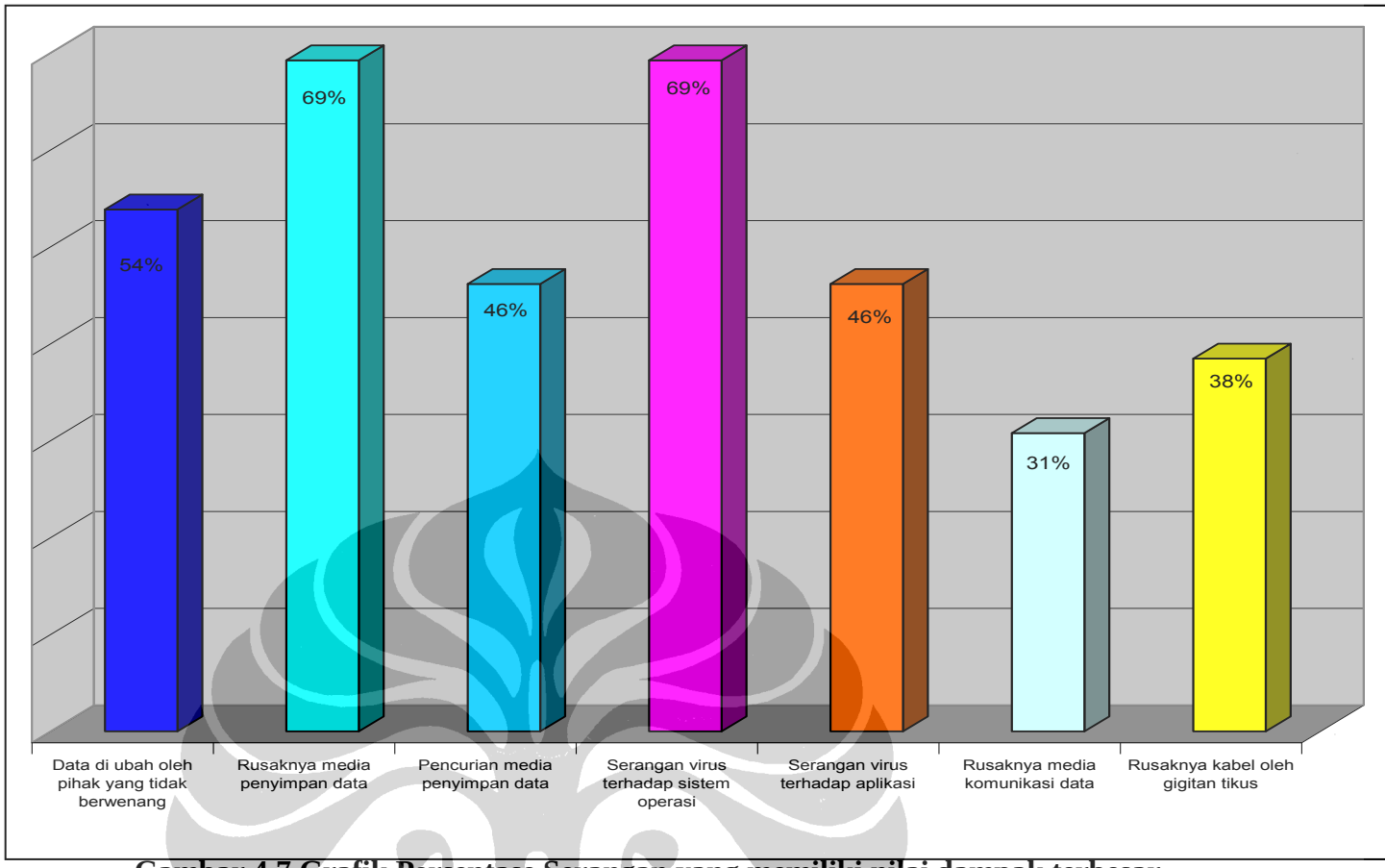
Berdasarkan analisis hasil kuisioner maka dapat di ketahui bahwa serangan virus terhadap sistem operasi merupakan serangan (*threat*) yang paling sering terjadi. Hal ini dapat dilihat pada gambar 4.6



Gambar 4.6 Grafik Persentase Frekuensi Serangan terhadap aset di Deptan

Berdasarkan tabel dari 12 Eselon 1 dan 2 yang ada di Deptan, seluruhnya (100%) mengungkapkan bahwa frekuensi serangan virus terhadap sistem operasi merupakan frekuensi tertinggi serangan terhadap aset.

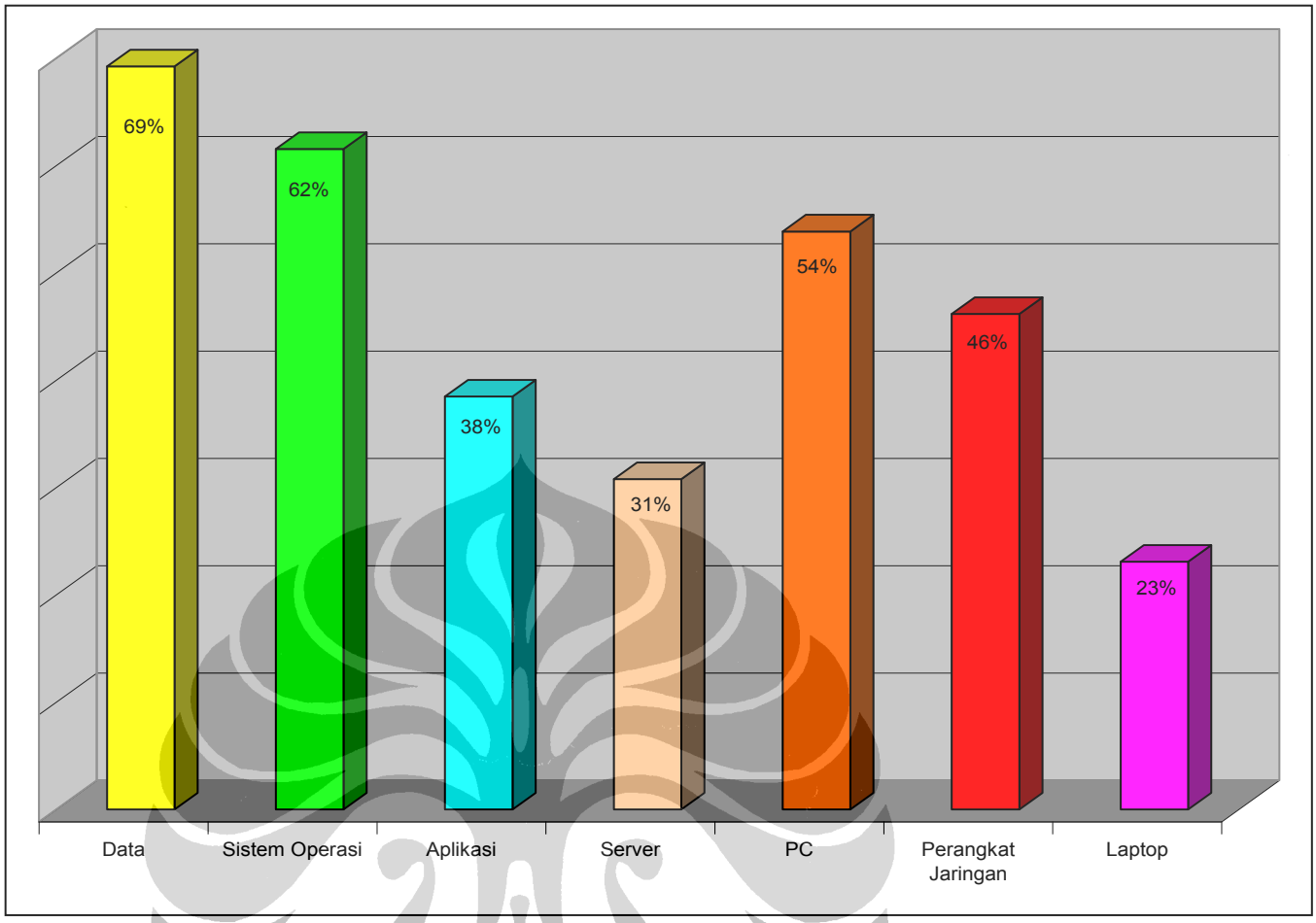
Sementara grafik yang berkaitan dengan nilai dampak dapat di lihat dari gambar 4.7



Gambar 4.7 Grafik Persentase Serangan yang memiliki nilai dampak terbesar di Deptan

Berdasarkan gambar 4.7 dapat diamati bahwa rusaknya media penyimpan data dan serangan virus terhadap sistem operasi merupakan serangan yang memiliki nilai dampak terbesar terhadap kegiatan pelaporan.

Berdasarkan kuesioner juga dapat diketahui bahwa aset yang memiliki resiko terbesar adalah data, seperti terlihat pada gambar 4.8



Gambar 4.8 Grafik persentase aset yang memiliki nilai resiko terbesar di Deptan

Data memiliki resiko keamanan terbesar di Departemen Pertanian. Oleh sebab itu perlu ada penanganan khusus terhadap aset yang memiliki resiko tersebut. Untuk itu perlu dirancang suatu perencanaan yang komprehensif terhadap keamanan informasi ditinjau dari beberapa aset. Pembahasan mengenai hal ini akan diuraikan pada bab Perencanaan Keamanan Sistem Informasi Deptan.

4.4 Manajemen Resiko

Berdasarkan analisa resiko, maka dapat ditentukan beberapa kendali resiko (*risk control*) yang dapat digunakan untuk mengurangi resiko, seperti terlihat pada tabel 5.2. Jenis kendali resiko dipilih berdasarkan aset yang paling sering terkena ancaman seperti telah diuraikan pada fase pertama tahapan pembahasan aspek keamanan teknis.

Tabel 4.5 Pengendali terhadap resiko serangan atau ancaman terhadap aset

No	Aset	Ancaman	Risk Control
1	Sistem Operasi dan Aplikasi	Serangan Virus	Kebijakan dalam penggunaan dan update antivirus. Install antivirus dengan kemampuan terbaik berdasarkan studi komparatif di seluruh PC/Laptop di lingkungan Deptan
2	PC	Rusaknya PC karena human error	Kebijakan dalam hak konfigurasi PC Kebijakan penggunaan password user dan admin Pelatihan dalam penggunaan PC secara aman
3	Data	Rusaknya media penyimpan data	Kebijakan back up data Kebijakan dalam perawatan penyimpan data (clean up, defragmen, dsb)

4.4.1 Manajemen Aset

Untuk mendapatkan perlindungan yang tepat bagi aset-aset di Departemen Pertanian, maka aset-aset tersebut harus memiliki penanggung jawab atau pemilik. Penanggung jawab telah teridentifikasi untuk semua aset yang ada dan telah ada penugasan resmi dari pimpinan eselon 1 tentang pihak yang menjadi pemilik dan penanggung jawab dari setiap aset. Pemilik bertanggung jawab terhadap implementasi perlindungan keamanan semua aset yang ada.

1. Penyimpanan Aset

Seluruh aset teridentifikasi dengan jelas dan penyimpanan dari semua aset penting telah dipersiapkan. Seluruh eselon 1 dan 2 di Deptan mengidentifikasi semua aset dan mendokumentasikan faktor penting dari aset. Penyimpanan aset juga disertai dengan semua informasi penting untuk metode melindungi aset dari

bencana, termasuk tipe aset, format, lokasi, informasi back up, dan informasi lisensi.

Berbagai tipe aset yang ada di Deptan pada masa depan diharapkan untuk dibagi menjadi beberapa jenis :

a. Data dan Informasi
b. Aset Perangkat Lunak
c. Aset Perangkat Keras
d. Aset Perangkat Jaringan

Penyimpanan aset menjamin perlindungan aset secara efektif dapat terlaksana dan proses dalam manajemen penyimpanan aset merupakan syarat utama bagi terselenggaranya manajemen resiko

2. Kepemilikan Aset

Seluruh informasi dan aset yang merupakan fasilitas proses informasi memiliki penanggung jawab yang di tunjuk langsung oleh pimpinan eselon 1. Pemilik/penanggung jawab aset tersebut berkewajiban untuk :

a. Menjamin bahwa informasi dan aset-aset yang berhubungan dengan informasi telah terklasifikasi.
b. Secara periodik melakukan review tentang pembatasan akses dan klasifikasi-klasifikasi termasuk meninjau kebijakan dalam kendali akses yang sudah diterapkan.

Pekerjaan rutin dalam pengawasan aset memang dapat ditugaskan kepada penjaga keamanan semisal satpam, namun pertanggungjawaban secara mutlak tetap berada pada pemilik aset.

3. Penggunaan Aset

Aturan untuk penggunaan informasi dan aset yang berhubungan dengan proses informasi harus teridentifikasi, terdokumentasi, dan diimplementasikan.

Seluruh pegawai, dan pihak-pihak lain di lingkungan Deptan harus mematuhi aturan dalam penggunaan informasi dan aset yang berhubungan dengan proses informasi, seperti sosialisasi aturan dalam penggunaan internet di lingkungan Deptan.

Aturan khusus atau panduan seharusnya disediakan oleh pihak manajemen bagi pihak ketiga yang bekerja di lingkungan Deptan seperti siswa PKL, konsultan, dan pihak ketiga lainnya. Pihak ketiga yang memiliki hak akses ke lingkungan Deptan seharusnya juga memahami batasan penggunaan informasi dan aset organisasi yang diberikan. Mereka harus bertanggungjawab dalam penggunaan setiap sumber informasi, dan fasilitas-fasilitas lain yang mereka gunakan.

4.4.2 Perlindungan Aset Terhadap Ancaman Lingkungan

Perlindungan secara fisik terhadap kerusakan yang disebabkan oleh kebakaran, banjir, bencana alam lainnya, juga kerusakan yang diakibatkan oleh ulah manusia harus dirancang dan diterapkan.

Panduan di bawah ini harus ditinjau untuk mencegah bencana-bencana yang ada, diantaranya adalah :

- Bahan-bahan berbahaya dan mudah terbakar harus disimpan pada jarak yang aman dari wilayah aman yang telah ditentukan.
- Pemadam kebakaran yang memadai harus ditempatkan pada tempat yang tepat. Pemadam kebakaran sebaiknya dalam bentuk bubuk atau gas, dan tidak dalam bentuk cairan. Penggunaan cairan sebagai pemadam memungkinkan terjadinya kerusakan fasilitas apabila terjadi kejadian.
- Perhatian kepada sumber tegangan listrik juga perlu diperhatikan terutama dari tingkat kestabilan tegangan. Kondisi perlengkapan back up juga harus disesuaikan dengan tingkat kebutuhan akan kontinuitas kegiatan. Penanggung jawab terhadap hal ini juga harus memeriksa secara rutin kondisi masing-masing perlengkapan back up.

4.5 Penentuan Sasaran Kontrol Manajemen Keamanan Informasi

Penentuan sasaran kontrol di lakukan dengan menentukan kebutuhan organisasi akan aspek-aspek tertentu yang dinilai masih rentan. Hasil evaluasi mengidentifikasi sepuluh sasaran kontrol yang dapat dilihat secara lengkap pada tabel 4.3 berikut ini :

Tabel 4.6 Sasaran kontrol Manajemen Berdasarkan Kebutuhan Deptan

No	Kebutuhan Organisasi	Kebutuhan Rencana Keamanan Informasi	Yang saat ini dimiliki	Keputusan	Keterangan
1	Mencegah terjadinya resiko yang membahayakan Deptan akibat tiadanya kebijakan dan prosedur keamanan informasi	Peningkatan keamanan ditinjau dari aspek prosedural	Belum ada	(new system) Integrasi sistem manajemen keamanan informasi berdasarkan ISO 17799	
2	Menghindari duplikasi kegiatan operasional dalam manajemen keamanan informasi	Peningkatan keamanan ditinjau dari aspek personil	Dalam Proses	(Upgrade) Melengkapi SOP yang ada dan lebih berorientasi ke aspek keamanan informasi.	
3	Menjamin terjaganya kerahasiaan informasi dan integritasnya	Peningkatan keamanan ditinjau dari aspek teknis	Belum ada	(new system) Melakukan klasifikasi dan pelabelan informasi atau data-data yang ada berdasarkan tingkat kerahasiaan atau tingkat urgensinya bagi dirjen maupun menteri	Dapat berupa routing slip
4	Menjamin tersedianya informasi kapanpun dan dimanapun di butuhkan	Peningkatan keamanan ditinjau dari aspek Teknis		(upgrade) Melakukan identifikasi aset informasi maupun sarana penunjangnya secara berkala dan menentukan potensi serangan dan kelemahan yang di miliki	Meningkatkan faktor avaliabilitas (ketersediaan)
5	Menjamin keberadaan aset terlindungi secara fisik	Peningkatan keamanan ditinjau dari aspek fisik	Belum ada	(Replace) Melakukan perbaikan sarana fisik dengan berorientasi kepada standar keamanan fisik tertentu seperti ISO 17799 atau ISO 27001	Dilakukan secara bertahap, seperti implementasi kamera pengawas dan biometrics. Pusdatin dapat dijadikan pilot project
6	Mengantisipasi pengetahuan pegawai yang minim mengenai keamanan informasi	Peningkatan keamanan ditinjau dari aspek personil	Belum ada	(Upgrade) Mengadakan pelatihan-pelatihan tentang pentingnya keamanan informasi	Termasuk mengikutsertakan pegawai ke pelatihan-pelatihan bersertifikat keamanan informasi

Tabel 4.6 Sasaran kontrol Manajemen Berdasarkan Kebutuhan Deptan (cont.)

No	Kebutuhan Organisasi	Kebutuhan Rencana Keamanan Informasi	Yang saat ini dimiliki	Keputusan	Keterangan
7	Mengantisipasi tumpang tindihnya tugas dan tanggung jawab yang berkaitan dengan keamanan informasi	Peningkatan aspek tata kelola keamanan informasi	Belum ada	(New System) Membentuk jabatan fungsional keamanan informasi sebagai penanggungjawab terselenggaranya sistem manajemen keamanan informasi yang handal di Deptan	
8	Mencegah terhentinya kegiatan operasional atau pelaporan apabila terjadi bencana	Peningkatan aspek teknis yaitu ketersediaan (availability)	Belum ada	(new system) Pembuatan dokumen *Business Impact Analysis* (BIA), *Business Continuity Plan* (BCP) dan *Dissaster Recovery Plan* (DRP).	
9	Mengantisipasi penyebaran virus melalui jaringan atau media penyimpan data	Peningkatan keamanan ditinjau dari aspek Teknis	Sudah ada	(upgrade) Implementasi piranti lunak anti virus dengan layanan update otomatis pada sistem yang kritikal	
10	Mencegah adanya serangan pihak lain melalui jaringan atau penyalahgunaan jaringan komputer di Deptan	Peningkatan keamanan ditinjau dari aspek Teknis	Belum ada	(upgrade) Implementasi piranti lunak *network management system* dan implementasi routing table	Selayaknya dilengkapi juga dengan *Intrusion Detection System*.

4.6 Rekomendasi Kegiatan

Berdasarkan poin-poin sasaran yang akan dikontrol dan dengan memperhatikan kondisi sistem manajemen keamanan informasi di Deptan maka penulis merekomendasikan kegiatan/inisiatif terkait peningkatan tiap aspek keamanan informasi. Rekomendasi kegiatan tersebut secara lengkap disajikan dalam tabel-tabel berikut ini :

Tabel 4.7 Kegiatan Terkait Peningkatan Aspek Kebijakan/Prosedural

1.	Nama kegiatan/inisiatif	Penyusunan Sistem Manajemen Keamanan Informasi
	Penjelasan singkat	Penyusunan Sistem Manajemen Keamanan Informasi berdasarkan standar keamanan ISO 17799
	Tujuan teknis inisiatif/kegiatan	Tersedianya panduan secara komprehensif dan terpadu untuk keamanan sistem informasi Deptan
	Manfaat yang diharapkan	Terciptanya sistem keamanan informasi di Departemen Pertanian yang baik
	Ruang lingkup	1. Risk Analysis 2. Information Security Organization 3. Asset Management 4. Human Resource Security 5. Physical & Environmental Security 6. Communications & Operations Management 7. Access Control 8. IS Acquisition, Development & Maintenance 9. Compliance
	Kebutuhan kompetensi utama utk inisiatif/kegiatan	Keamanan Informasi

Tabel 4.8 Kegiatan Terkait Peningkatan Aspek Fisik

1.	Nama kegiatan/inisiatif	Melakukan perbaikan manajemen sarana fisik dengan berorientasi kepada standar keamanan fisik tertentu seperti ISO 17799 atau ISO 27001
	Penjelasan singkat	Dapat diterapkan dengan langkah awal berupa membagi dan mendefinisikan wilayah berdasarkan tingkat keamanan di masing-masing lingkungan eselon 1 dan 2 Deptan.
	Tujuan teknis inisiatif/kegiatan	Sebagai panduan dalam peningkatan keamanan fisik
	Manfaat yang diharapkan	Mengurangi kelemahan dalam keamanan informasi Deptan ditinjau dari aspek fisik
	Ruang lingkup	Diproritaskan untuk ruangan yang berkaitan dengan pemrosesan dan penyimpanan data seperti Datacenter dan Ruang Server Langkah awal dapat diterapkan di lingkungan Pusdatin terlebih dahulu
	Kebutuhan kompetensi utama utk inisiatif/kegiatan	Pelatihan Keamanan Informasi

T*abel 4.9 Kegiatan Terkait Peningkatan Aspek Teknis*

1.	Nama kegiatan/inisiatif	Melakukan klasifikasi dan pelabelan informasi atau data-data yang ada berdasarkan tingkat kerahasiaan atau tingkat urgensinya bagi dirjen maupun menteri
	Penjelasan singkat	Dapat diimplementasikan dalam bentuk routing slip dan pelabelan informasi
	Tujuan teknis inisiatif/kegiatan	Informasi dan aset lainnya dapat diklasifikasikan berdasarkan tingkat kekritisannya.
	Manfaat yang diharapkan	Penanganan keamanan informasi maupun aset lainnya dapat dilaksanakan secara lebih efektif dan efisien berdasarkan tingkat kekritisannya bagi Deptan.
	Ruang lingkup	Pusdatin dan beberapa Ditjen
	Kebutuhan kompetensi utama utk inisiatif/kegiatan	Keamanan Informasi

2.	Nama kegiatan/inisiatif	Melakukan identifikasi aset informasi maupun sarana penunjangnya secara berkala dan menentukan potensi serangan dan kelemahan yang di miliki
	Penjelasan singkat	Potensi serangan dan ancaman bersifat dinamis, sehingga dibutuhkan implementasi inisiatif ini secara berkala
	Tujuan teknis inisiatif/kegiatan	Mengantisipasi kemungkinan adanya serangan dengan sumber maupun varian yang lebih baru atau kelemahan yang terdapat pada sistem informasi di Deptan secara aktual
	Manfaat yang diharapkan	Mengurangi dampak serangan ataupun kelemahan terhadap kegiatan operasional maupun manajerial di lingkungan Deptan
	Ruang lingkup	Meliputi seluruh aset yang berkaitan dengan pemrosesan informasi baik data itu sendiri, perangkat keras, perangkat lunak dan perangkat jaringan.
	Kebutuhan kompetensi utama utk inisiatif/kegiatan	Up grade pengetahuan mengenai serangan terbaru terhadap sistem informasi

T*abel 4.9 Kegiatan Terkait Peningkatan Aspek Teknis(cont.)*

3.	Nama kegiatan/inisiatif	Pembuatan dokumen Business Impact Analysis (BIA), Business Continuity Plan (BCP) dan Dissaster Recovery Plan (DRP).
	Penjelasan singkat	Business Impact Analysis wajib dikaji terlebih dahulu sebelum merancang BCP dan DRP
	Tujuan teknis inisiatif/kegiatan	Sebagai upaya antisipasi Deptan dalam menghadapi bencana, mendokumentasikannya, dan mensosialisasikannya ke seluruh pegawai Deptan
	Manfaat yang diharapkan	Menjamin keberlangsungan kegiatan operasional dan manajerial di Deptan
	Ruang lingkup	Di lingkup Pusdatin terlebih dahulu
	Kebutuhan kompetensi utama utk inisiatif/kegiatan	Pengetahuan mengenai proses bisnis-proses bisnis utama dan kritikal di Deptan

4.	Nama kegiatan/inisiatif	Implementasi piranti lunak anti virus dengan layanan update otomatis pada sistem yang kritikal
	Penjelasan singkat	Studi komparatif perlu dilakukan untuk menentukan jenis atau tipe antivirus yang sesuai untuk Deptan
	Tujuan teknis inisiatif/kegiatan	Antisipasi serangan virus yang menyerang aset data dan perangkat lainnya
	Manfaat yang diharapkan	Mengurangi dampak terhambatnya aliran informasi dan berkurangnya nilai aset akibat serangan virus dan sejenisnya (spam, worm, trojan)
	Ruang lingkup	Seluruh PC maupun Server di lingkungan Deptan
	Kebutuhan kompetensi utama utk inisiatif/kegiatan	Pengetahuan mengenai jenis-jenis virus dan anti virus yang ada

T*abel 4.9 Kegiatan Terkait Peningkatan Aspek Teknis (cont.)*

5.	Nama kegiatan/inisiatif	Implementasi piranti lunak *network management system* dan implementasi routing table
	Penjelasan singkat	Sebagai langkah awal dari terciptanya keamanan jaringan informasi yang komprehensif di Deptan
	Tujuan teknis inisiatif/kegiatan	Mengantisipasi penggunaan layanan jaringan komunikasi yang tidak sebagaimana mestinya serta serangan terhadap keamanan aset melalui jaringan
	Manfaat yang diharapkan	Meningkatkan aspek ketersediaan (availabilitas) terhadap layanan jaringan
	Ruang lingkup	Diprioritaskan terlebih dahulu di lingkup Pusdatin
	Kebutuhan kompetensi utama utk inisiatif/kegiatan	Pengetahuan mengenai keamanan jaringan komunikasi

Tabel 4.10 Kegiatan Terkait Peningkatan Aspek Personil

1.	Nama kegiatan/inisiatif	Melengkapi SOP yang ada untuk lebih berorientasi ke aspek keamanan informasi.
	Penjelasan singkat	Perlu bersinergi dengan kegiatan penyusunan SOP yang dilakukan bersamaan dengan penyusunan dokumen ini
	Tujuan teknis inisiatif/kegiatan	Tersedianya panduan bagi para pegawai dan juga pihak ketiga dalam melaksanakan tugas dan fungsinya yang memenuhi standar keamanan informasi
	Manfaat yang diharapkan	Mengurangi dampak terhambatnya kegiatan operasional dan manajerial ditinjau dari aspek personil
	Ruang lingkup	Pusdatin dan beberapa Ditjen
	Kebutuhan kompetensi utama utk inisiatif/kegiatan	Pengetahuan mengenai prosedur keamanan informasi berdasarkan standar keamanan informasi yang ada

2.	Nama kegiatan/inisiatif	Mengadakan pelatihan-pelatihan peningkatan kesadaran pentingnya keamanan informasi
	Penjelasan singkat	Pelatihan dilakukan beberapa gelombang untuk seluruh pegawai di Pusdatin dan Datin
	Tujuan teknis inisiatif/kegiatan	Meningkatkan kesadaran pegawai akan pentingnya keamanan informasi
	Manfaat yang diharapkan	Mengurangi faktor kesalahan (human error) yang diakibatkan oleh pengetahuan SDM yang minim terhadap aspek keamanan informasi
	Ruang lingkup	Prioritas terlebih dahulu di lingkungan Pusdatin dan beberapa Datin.
	Kebutuhan kompetensi utama utk inisiatif/kegiatan	Pengetahuan dasar komputer

Tabel 4.11 Kegiatan Terkait Peningkatan Aspek Tatakelola

1.	Nama kegiatan/inisiatif	Membentuk jabatan fungsional keamanan informasi sebagai penanggungjawab terselenggaranya sistem manajemen keamanan informasi yang handal di Deptan
	Penjelasan singkat	
	Tujuan teknis inisiatif/kegiatan	Deptan memiliki penanggungjawab untuk mengkoordinasi keamanan informasi di lingkungan Deptan
	Manfaat yang diharapkan	Meningkatkan aspek tata kelola keamanan informasi yang merupakan bagian tak terpisahkan dari tata kelola teknologi/sistem informasi di lingkungan Deptan
	Ruang lingkup	Pusdatin dan Datin-datin
	Kebutuhan kompetensi utama utk inisiatif/kegiatan	Pengetahuan mengenai standar keamanan informasi dan arsitektur informasi