BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Hasil penelitian menunjukkan bahwa Departemen Pertanian belum memiliki kebijakan keamanan informasi yang komprehensif dan formal, dengan kata lain 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. Kondisi demikian menyebabkan aspek keamanan informasi yang menyangkut kerahasiaan, integritas dan ketersediaan data di lingkungan Deptan sangat rentan mengalami gangguan.

Dari lima macam asset yang ada di Departemen Pertanian, data memiliki resiko keamanan terbesar. Oleh sebab itu perlu ada penanganan khusus terhadap asset yang memiliki resiko terbesar tersebut. Terungkap pula bahwa frekuensi serangan virus terhadap sistem operasi merupakan frekuensi tertinggi serangan terhadap asset. Rusaknya media penyimpan data dan serangan virus terhadap sistem operasi merupakan serangan yang memiliki nilai dampak terbesar terhadap kegiatan pelaporan.

Pimpinan Departemen Pertanian perlu segera merancang dokumen kebijakan keamanan informasi secara jelas dan selaras dengan visi, misi, sasaran, dan tujuan Departemen yang meliputi aspek keamanan fisik, aspek teknis, aspek personil, dan aspek tata kelola sistem informasi untuk menjaga keamanan asset sekaligus menjamin kegiatan pertukaran informasi dapat berjalan dengan aman dan *seamless* (mulus).

Tahap berikutnya sebagai pengejawantahan dari kebijakan keamanan 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.

Ditinjau dari aspek fisik langkah awal yang diperlukan adalah dengan mendefinisikan wilayah aman (secure areas) yang ada di lingkungan Deptan. 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 asset.

Setiap asset (termasuk informasi) harus diklasifikasi untuk menjamin bahwa setiap asset mendapatkan tingkat perlindungan sesuai dengan karakteristiknya dan kebutuhan organisasi. Informasi selayaknya diklasifikasi berdasarkan kebutuhan, prioritas, dan derajat keamanan yang diharapkan oleh pengguna informasi. Klasifikasi informasi selayaknya diimplementasikan dengan pemberian label tiap informasi dalam berbagai bentuk dan format. Hal yang sama perlu juga dilakukan untuk kategori asset lainnya.

Dalam aspek keamaanan personil, diperlukan adanya Standar Prosedur Operasional untuk menjamin bahwa pengguna sistem informasi baik dari pegawai Deptan maupun pihak ketiga memahami tanggungjawabnya dan sesuai dengan perannya, dan untuk mencegah terjadinya pencurian maupun perusakan aset oleh personil. Tanggung jawab keamanan harus di tuangkan ke dalam suatu bentuk deskripsi tugas sesuai dengan tugas dan fungsi, dan kondisi personil. Pengguna fasilitas pemrosesan informasi, baik dari pegawai maupun pihak ketiga, harus menandatangani persetujuan berdasarkan peran dan tanggung jawabnya terhadap keamanan informasi. Peran dan tanggung jawab keamanan setiap personil seharusnya terdefinisi dan terdokumentasi berlandaskan kebijakan keamanan informasi Deptan.

5.2 Saran

Peningkatan kesadaran keamanan informasi, pendidikan, dan pelatihannya menjadi hal yang mendesak dilakukan. Seluruh pegawai di lingkungan Departemen Pertanian tanpa kecuali sebaiknya mendapatkan pelatihan dalam rangka peningkatan kesadaran terhadap keamanan informasi dan sosialisasi terhadap kebijakan dan

prosedur keamanan informasi yang relevan bagi tupoksi masing-masing pegawai. Pelatihan ini sebelumnya harus diawali dengan serangkaian proses sosialisasi terhadap kebijakan keamanan organisasi dan harapan pegawai terhadap jaminan akses pada informasi atau layanan.

Langkah awal dari hal ini dapat dimulai dengan membentuk suatu fungsi baru di lingkungan organisasi TI di Deptan yaitu penanggungjawab keamanan informasi (*information security manager*). Adapun tugas dari fungsi atau jabatan ini adalah untuk mengkoordinir dan memonitor pelaksanaan rencana keamanan informasi di Deptan yang telah disepakati bersama.