BAB IV

HASIL DAN PEMBAHASAN

4.1. PENDEFINISIAN RUANG LINGKUP KEBIJAKAN KEAMANAN INFORMASI

Dalam penelitian dan penulisan tesis ini, penulis mencoba untuk memfokuskan pengembangan kebijakan keamanan informasi pada PT. NCS dengan mengadopsi sejumlah domain yang terdapat dalam standard ISO/IEC 27002 yang merupakan penomoran ulang dari standar ISO 17799:2005. Beberapa domain yang dimaksud adalah sebagai berikut:

- *Security Policy*, dan
- *Organization of Information Security*.

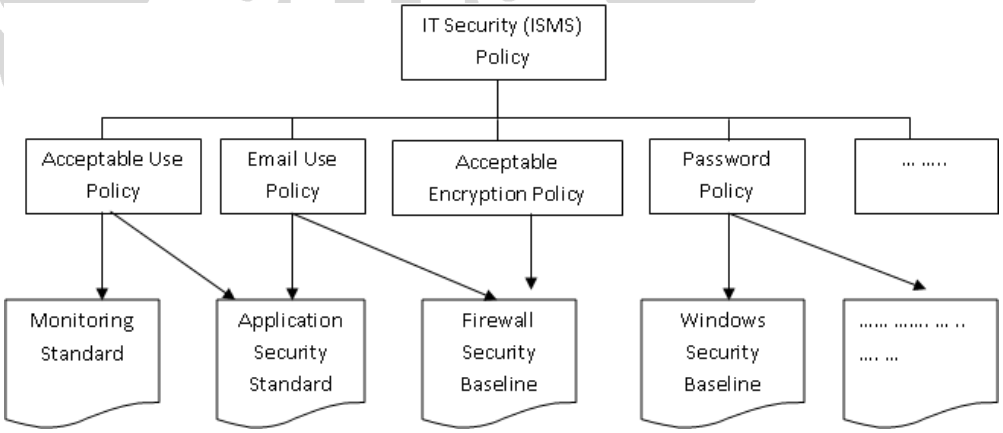
Sejumlah domain selebihnya tidak masuk dalam fokus penelitian ini dikarenakan serangkaian argumen yang melatarinya (seperti tingkat prioritas domain pada perusahaan tempat dijadikannya studi kasus, batasan waktu penelitian, serta belum adanya regulasi pemerintah yang mendorong kemunculan kebijakan yang dimaksud).

Adapun fokus objek penelitian studi kasus lebih menitikberatkan pada kantor pusat dari PT. NCS berikut 2 kantor cabang utama yang juga berlokasi di Jakarta. Kedua kantor cabang yang dimaksud adalah kantor cabang kemanggisan dan kantor cabang G2.

4.2. PENDEFINISIAN KEBIJAKAN KEAMANAN INFORMASI

Setelah melalui serangkaian analisa terhadap data yang diperoleh dengan sejumlah metode pengumpulan data sebagaimana telah dijelaskan sebelumnya, maka penulis berusaha merumuskan dan mendefinisikan kebijakan keamanan yang sesuai dengan kondisi perusahaan PT. NCS. (Adapun bentuk detail dari kebijakan keamanan yang dimaksud dapat direview pada Lampiran 2 tentang dokumen kebijakan keamanan informasi).

Secara garis besar, dapat dijelaskan bahwa kebijakan keaman yang diturunkan kedalam beberapa aspek tersebut merupakan acuan dalam penciptaan panduan teknis dalam ruang lingkup keamanan informasi.



Gambar 5 Struktur Kebijakan Keamanan dan Standard

Adapun kebijakan yang dikembangkan setidaknya mencakup sejumlah kebijakan berikut:

- *Acceptable Encryption Policy*

  Kebijakan ini bertujuan untuk memberikan panduan yang membatasi penggunaan algoritma enkripsi yang telah diterima oleh publik dan telah terbukti bekerja dengan efektif.

- *Acceptable Use Policy*

  Tujuan dari kebijakan ini adalah sebagai batasan dalam penggunaan yang dapat diterima terhadap peralatan komputer atau infrastruktur IT yang relevan pada PT. NCS. Aturan-aturan ini dimaksudkan untuk melindungi pegawai dan PT. NCS sendiri. Penggunaan yang tidak sesuai dengan kebijakan ini atau turunannya ataupun prosedur yang diturunkannya dapat mengakibatkan serangan virus, eksploitasi secara tidak sah terhadap sistem jaringan dan layanan-layanan perusahaan serta permasalahan hukum.

- *Audit Vulnerability Scan Policy*

  Kebijakan ini bertujuan untuk menentukan persetujuan tentang proses pemindaian (*scanning*) keamanan jaringan yang diberikan oleh Internal atau External Auditor kepada PT. NCS. Kebijakan ini juga menentukan piranti yang digunakan, proses serta tujuan dari audit yang dimaksud.

- *Email Use Policy*

  Kebijakan ini dibuat untuk menghindari rusaknya *image* publik dari PT NCS ketika suatu email keluar dari organisasi tersebut, maka masyarakat umum akan menilai bahwa pesan yang muncul dari email tersebut merupakan suatu pernyataan resmi dari PT. NCS.

- *Email Retention Policy*

  Kebijakan ini dimaksudkan untuk membantu para karyawan dalam menentukan durasi waktu infomasi yang dikirimkan atau diterima melaui email seharusnya disimpan.

- *Automatically Forwarded Email Policy*

  Kebijakan ini dimaksudkan untuk menghindari pengungkapan informasi sensitif perusahaan secara tidak sah.

- *Information Sensitivity Policy*

  Kebijakan ini dimaksudkan untuk membantu para pegawai PT. NCS dalam menentukan informasi apa yang dapat diperlihatkan kepada non pegawai diluar dari PT. NCS (serta sebaliknya). Informasi yang dicakup dalam kebijakan ini meliputi: informasi elektronik, informasi pada kertas, dan informasi yang disampaikan secara lisan atau visual (seperti telepon, atau *video conference*).

- *Internet DMZ Equipment Policy*

  Kebijakan ini bertujuan untuk mendefinisikan standard yang sesuai dengan semua peralatan yang dimiliki atau dioperasikan oleh PT. NCS yang berlokasi diluar firewall internet dari PT. NCS. Standard ini dirancang untuk meminimalkan kemungkinan bocor atau hilangnya data sensitif atau rahasia, hak cipta dan lain sebagainya yang dimiliki oleh PT. NCS.

- *Password Policy*

  Kebijakan ini bertujuan untuk membangun standard dalam penciptaan *password* yang kuat, metode proteksi terhadap *password* serta frekuensi perubahannya.

- *Removable Media Policy*

  Kebijakan dimaksudkan untuk meminimalkan resiko kehilangan atau tersebarnya informasi sensitif yang dimiliki oleh PT. NCS dan mengurangi resiko munculnya infeksi malware / virus pada komputer / PC yang dioperasikan oleh PT. NCS.

- *Router Security Policy*

  Kebijakan ini menjelaskan tentang konfigurasi keamanan minimal yang dibutuhkan untuk semua router dan switch yang terhubung ke jaringan *production* atau digunakan dalam kapasitas untuk *production* dari PT. NCS.

- *Server Security Policy*

  Kebijakan ini bertujuan untuk membangun standard terhadap konfigurasi dasar perangkat server internal yang dimiliki ataupun dioperasikan oleh PT. NCS. Implementasi yang efektif akan meminimalisasi akses tanpa hak terhadap informasi atau teknologi milik PT. NCS.

- *Wireless Communication Policy*

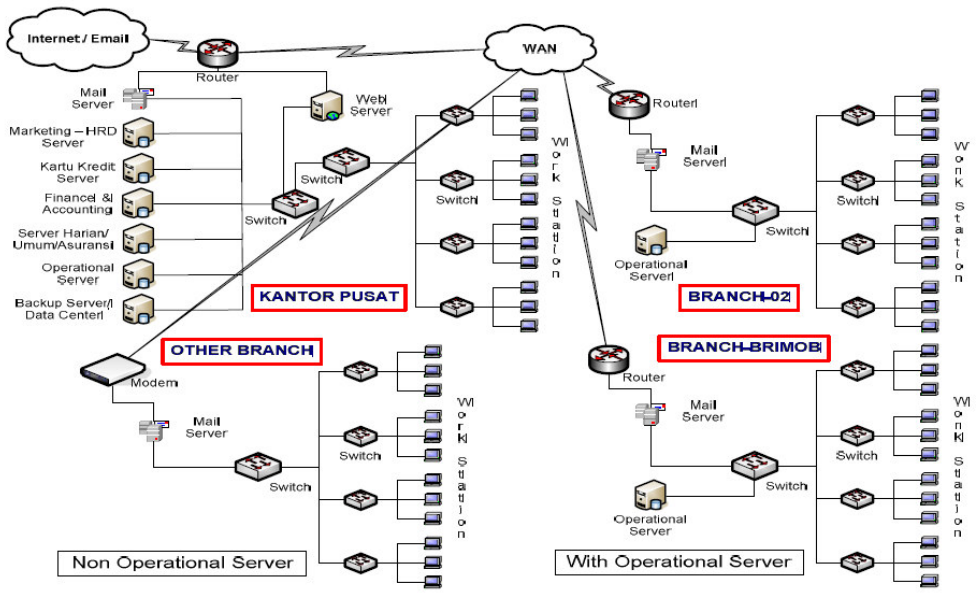
  Tujuan dari kebijakan ini adalah mengamankan dan melindungi aset informasi yang dimiliki oleh PT. NCS. PT. NCS memberikan akses kepada sejumlah sumber daya IT (seperti perangkat kompuer / PC, jaringan, hingga sistem informasi elektronis) sebagai suatu hak keistimewaan yang harus dijaga secara bertanggung jawab untuk menjaga kerahasiaan, integritas dan ketersediaan dari semua aset informasi. Secara lebih spesifik, kebijakan ini menetapkan kondisi-kondisi yang harus dipenuhi oleh infrastruktur wireless ketika terhubung ke jaringan PT. NCS.

4.3. ANALISA RESIKO

Secara umum proses dalam risk assessment ini terdiri dari 4 tahapan utama yaiatu: proses identifikasi sistem yang signifikan, proses identifikasi aset,

identifikasi ancaman yang turut menyertainya serta perumusan kontrol yang sebaiknya diambil guna meminimalisir resiko yang ada.

4.3.1. Topologi Jaringan



Gambar 6 Topologi Konektivitas Jaringan PT. NCS

4.3.2. Identifikasi Sistem Kritis

Dalam PT. NCS terdapat sejumlah aset sistem yang memegang peranan penting dalam operasional proses bisnisnya. Adapun sejumlah sistem yang dimaksud adalah sebegai berikut:

- Aplikasi TTM Cargo

  Aplikasi ini berada di dalam divisi Logistik & Cargo, yang berfungsi melakukan proses tracking atau penelusuran cargo mulai dari cargo tersebut diterima dari konsumen, diproses, dikirim, dijemput, hingga sampai ketangan si penerima (dalam hal ini tujuan akhir dari paket/cargo

tersebut). Di dalam aplikasi ini terdapat juga modul-modul aplikasi yang menjadi bagian dari aplikasi TTM Cargo, yaitu :

- Aplikasi *Outbound*, aplikasi ini mencakup didalamnya proses untuk mengelola data entri transaksi awal paket/cargo yang akan dikirim hingga pengepakan dan pengapalan.
- Aplikasi *Inbound*, aplikasi ini mencakup proses untuk mengelola penjemputan serta pendistribusian paket/cargo kepada si penerima, serta ada laporan apabila paket/cargo tidak dapat didistribusikan kepada si penerima.
- Aplikasi *Track & Trace*, merupakan aplikasi yang digunakan untuk monitoring tentang keberadaan paket/cargo yang dikirim.
- Aplikasi *Performance Audit*, merupakan aplikasi untuk mengontrol proses-proses kegiatan outbound, inbound dan tracking.

- Aplikasi HRD

Sesuai dengan namanya maka aplikasi ini berada di dalam divisi HRD, yang berfungsi untuk mengelola kegiatan-kegiatan yang ada pada divisi HRD. Di dalam aplikasi ini terdapat juga modul-modul aplikasi yang menjadi bagian dari aplikasi HRD, yaitu:

- Aplikasi *Payroll*, menyediakan sejumlah fasilitas untuk mengelola sebuah sistem penggajian yang lengkap, dan membentuk sebuah sub-sistem yang sangat penting dalam prosedur pengolahan data Akuntansi yang terintegrasi. Aplikasi ini memungkinkan

dilakukannya prosedur penggajian dengan menggunakan periode mingguan, tengah-bulanan, bulanan atau semi-bulanan dengan pengamanan berupa *password*. Proses penggajian bisa dilakukan melalui cek atau pendepositoan secara langsung, untuk sebagian atau kesleuruhan karyawan. Riwayat rinci dari pembayaran, potongan-potongan, serta perubahan data karyawan bisa disediakan secara tercetak atau di layar. Aplikasi *payroll* terintegrasi secara penuh dengan jam kerja dan kehadiran yang akan mempermudah masukan datanya, khususnya bagi bagian-bagian atau divisi-divisi di dalam perusahaan yang memiliki sistem penggajian yang sangat sibuk.

- Aplikasi Personal, merupakan aplikasi yang mengelola data-data kepegawaian. Aplikasi ini memproses pendataan karyawan yang masih aktif maupun yang sudah tidak aktif lagi di perusahaan, meliputi data pribadi karyawan, keluarga karyawan, kontak emergency yang dapat dihubungi, performa dan penghargaan-penghargaan yang didapatkan, konpensasi dan benefit yang didapatkan, cuti karyawan, dan informasi lainnya.
- Aplikasi *Placement*, merupakan aplikasi yang digunakan untuk penempatan pegawai. Aplikasi ini memproses data-data karyawan yang berkaitan dengan Pendidikan dan pelatihan, karir dan kompetensi, status dan jabatan, kedisiplinan, dan informasi lainnya.

- Aplikasi *Recruitment*, merupakan aplikasi yang digunakan untuk merekrut pegawai baru. Ada metode penilaian, berdasarkan pengujian yang dilakukan oleh perusahaan maupun pihak ketiga, mengenai layak tidaknya untuk direkrut.
- Aplikasi Jamsostek, merupakan aplikasi yang mengelola data-data mengenai jaminan sosial tenaga kerja (jamsostek) pegawai.

- Aplikasi MCM

  Aplikasi ini berada di dalam divisi *Marketing & Sales*, yang berfungsi untuk mengelola keseluruhan kegiatan yang ada pada divisi *Marketing & Sales*. Di dalam aplikasi ini terdapat juga modul-modul aplikasi yang menjadi bagian dari aplikasi *Marketing & Sales*, yaitu:

  - Aplikasi Telesales, merupakan aplikasi yang digunakan oleh divisi *Marketing & Sales* untuk menjaring pelanggan baru. Aplikasi ini terhubung dengan media komunikasi seperti: telepon, fax dan email.
  - Aplikasi Insentif, merupakan aplikasi untuk memberikan reward kepada staff divisi *marketing* berdasarkan kinerjanya.
  - Aplikasi Data Pelanggan, merupakan aplikasi untuk mengelola data pelanggan.
  - Aplikasi Registrasi, merupakan aplikasi untuk registrasi pelanggan baru.

- Aplikasi GL

  Aplikasi ini berada di dalam divisi *Finance & Accounting*, yang berfungsi untuk mengelola kegiatan-kegiatan yang ada pada divisi *Finance & Accounting*. Di dalam aplikasi ini terdapat juga modul-modul aplikasi yang menjadi bagian dari aplikasi *Finance & Accounting*, yaitu:

  - Aplikasi *Ledger Receivables*, menyediakan sarana untuk secara tepat memelihara rincian dari pelanggan dan hal-hal yang erat kaitannya dengan transaksi penjualan yang dilakukan perusahaan, dan harus ditagihkan kepada pelanggan yang bersangkutan. Melalui fasilitas di layar, informasi-informasi penting segera dapat ditampilkan, misalnya tentang rincian tagihan, informasi pelanggan, umur piutang, dan lain sebagainya. Laporan-laporan yang bersifat komprehensif telah disiapkan dan memungkinkan kita untuk mengontrol secara efektif sisa-sisa piutang yang masih bisa diurus penagihannya.
  - Aplikasi *Ledger Payables*, menyediakan berbagai fasilitas yang diperlukan untuk secara cermat memelihara informasi rinci mengenai vendor (*supplier*) dan transaksi-transaksi perusahaan yang erat dengan kaitannya dengan kegiatan pembelian perusahaan. Segenap aktivitas perusahaan yang berkaitan dengan rencana pembayaran hutang perusahaan dan fasilitas penulisan cek adalah untuk mengendalikan status rekening dari vendor-vendor yang bersangkutan secara efektif. Dengan demikian perusahaan

akan terhindarkan dari kemungkinan kerugian, yaitu berupa potongan tunai, karena membayar lebih awal dari jatuh tempo, dibandingkan harus membayar sejumlah uang yang lebih besar, sementara saat itu perusahaan memiliki posisi keuangan yang mencukupi.

- Aplikasi *General Ledger*, adalah modul inti dari sebuah aplikasi sistem akuntansi. Aplikasi *General Ledger* mengeluarkan laporan-laporan Laba/Rugi, Neraca, serta informasi berkenaan dengan Anggaran dan Realisasinya. Modul *General Ledger* mengakumulasi semua data yang terkait erat dengan sistem akuntansi, yang meliputi modul-modul yang berasal dari Piutang (*Accounts Receivables*), Hutang (*Accounts Payables*), Manajemen Kas, Penggajian, Akuntansi Biaya dan Persediaan.
- Aplikasi *Purchasing*, dimana pihak manajemen dapat melakukan pengendalian terhadap semua tahapan dari siklus pembelian perusahaan, dimulai sejak saat pemesanan tersebut disampaikan kepada supplier sampai dengan pesanan tersebut diterima dengan baik, dan penyelesaian tagihannya. Sistem ini mampu untuk memproses pemesanan pembelian untuk barang-barang yang bebas dibeli, dalam arti bukan termasuk item barang yang kemudian masuk ke dalam stok persediaan, maupun barang-barang yang akan menjadi barang persediaan.

- Aplikasi *Cost Control*, adalah aplikasi yang dibuat untuk memonitor neraca keuangan perusahaan termasuk *cash flow*.
- Aplikasi Manajemen Aset, adalah aplikasi untuk merencanakan, mengendalikan dan mengawasi aset atau sumber daya perusahaan secara fungsional. Pencatatan yang akurat, pengendalian serta perhitungan aset perusahaan adalah sesuatu yang sangat penting di hampir semua sistem keuangan perusahaan. Aplikasi ini menyediakan laporan aset perusahaan untuk memberikan gambaran seutuhnya tentang seberapa besar kekayaan perusahaan sebenarnya.

- Aplikasi *City Courier*

  Aplikasi ini terdiri dari sejumlah modul-modul aplikasi yang beberapa diantaranya adalah:

  - Aplikasi *Billing*, merupakan aplikasi untuk proses penagihan pembayaran *in-voice* pada *city courier*.
  - Aplikasi *Complain Handling*, merupakan aplikasi untuk proses penanganan kriteria dari pelanggan/konsumen.
  - Aplikasi *Printing*, merupakan aplikasi untuk mengelola dokumen-dokumen yang akan dicetak, seperti pencetakan *billing*, dll.
  - Aplikasi Kartu Kredit, merupakan aplikasi untuk mengelola pengiriman kartu kredit.

Selanjutnya, sejumlah sistem kritis tersebut yang telah didesktipsikan sebelumnya dirumuskan kedalam tabel identifikasi (lihat Tabel 4.1). Tabel berikut mengidentifikasi sejumlah sistem dimaksud berdasarkan fungsi, pemilik data, data yang mengalir pada sistem tersebut, pengguna yang berhak menggunakannya hingga batasan sumber daya pada sistem tersebut. Adapun fokus bahasan identifikasi ini terbatas pada kantor pusat PT. NCS di Jakarta.

Tabel 4.1 Identifikasi Sistem Kritis

Nama Sistem	Fungsi	Pemilik Data	Data	Pengguna yang berhak	Batasan Sumber Daya
Email	Menyediakan layanan email	IT Department	Personal, Arsip Rahasia Perusahaan, Arsip sensitif perusahaan	Para karyawan PT. NCS	Mail Server, email client, arsip email
Aplikasi TTM Cargo	Melakukan proses tracking dan penelusuran cargo	Divisi Logistik & Cargo	Data Cargo / barang	Karyawan pada Divisi & Cargo	TTM Cargo front-end, database server
Aplikasi HRD	Mengelola kegiatan yang ada pada divisi HRD	Manager Divisi HRD	Data personal karyawan, penggajian, recruitment	Karyawan Divisi HRD	HRD client Appl, database server
Aplikasi MCM	Mengelola kegiatan divisi Marketing & Sales	Manager Divisi Marketing & Sales	Data pelanggan, insentif	Karyawan Divisi MCM	MCM front-end, database server
Aplikasi GL	Mengelola kegiatan divisi finance & accounting	Manager Divisi Finance & Accounting	Data vendor, rugi laba, pembelian	Karyawan Divisi Fonace & Accounting	GL front-end, database server
Aplikasi System Warehouse	Mengelola data paket / cargo pada warehouse	Manager Divisi Logistik & Cargo	Data Cargo / barang	Karyawan pada Divisi & Cargo	Warehouse Client, database server

4.3.2. Identifikasi Aset

Berdasarkan hasil wawancara dengan sejumlah key personnel dari PT. NCS dan observasi langsung menuju perusahaan yang dimaksud serta kajian sejumlah dokumen pendukung, maka dapatlah dirumuskan sejumlah aset yang dimiliki atau dioperasikan atau dikuasakan pada PT. NCS. Adapun aset yang teridentifikasi disini merupakan aset yang dinilai memiliki dampak atau pengaruh terhadap proses pengembangan kebijakan keamanan informasi.

Hasil dari rumusan tersebut selanjutnya dirangkum dalam dokumen Tabel Daftar Identifikasi Aset PT. NCS (lihat Tabel 4.2). Tabel tersebut mengklasifikasikan sejumlah aset yang ada kedalam 4 kategori utama, yaitu aset informasi, aset *software*, aset *hardware* / infrastruktur, serta aset fasilitas. Disamping itu, disertakan pula level signifikansi terhadap masing-masing aset yang berhasil teridentifikasi dalam tiga tingkatan.

Tabel 4.2 Daftar Identifikasi Aset

No.	Aset	Pemilik	Level Signifikansi
Aset Informasi			
1	Sensitif		
	Rekam Jejak Karyawan	HRD	Sedang
	Informasi Harga	Div. Marketing	Tinggi
	Data finansial perusahaan	Div. Finance	Tinggi
	Password Account aplikasi / Sistem	User	Sedang
2	Publik		
	Website	PT. NCS	Rendah
	Data Spesifikasi Layanan	PT. NCS	Sedang
	Materi Pemasaran (slide presentasi, brosur)	PT. NCS	Rendah
	Company Profile	PT. NCS	Rendah
Aset Software			
1	Sistem Operasi Microsoft Windows XP Professional	Departemen IT	Sedang
2	Sistem Operasi Windows Server 2003 STD Edition	Departemen IT	Tinggi
3	Mail Server Mailer Daimon	Departemen IT	Tinggi
3	Custom Application*	Departemen IT	Tinggi
Aset Hardware / Infrastruktur			
1	PC / Workstation	Departemen IT	Sedang
2	Server	Departemen IT	Tinggi
3	Hub / Switch	Departemen IT	Sedang
4	Router	Departemen IT	Sedang
5	Modem	Departemen IT	Sedang
6	Access Point (Indoor)	Departemen IT	Rendah
7	Printer	Departemen IT	Sedang
8	UPS	Departemen IT	Rendah
9	Kabel Jaringan (UTP)	Departemen IT	Rendah
Aset Fasilitas			
1	Listrik	PLN	Tinggi

Tabel 4.3 Daftar Identifikasi Aset (Lanjutan)

2	Koneksi/Jaringan Internet	ISP	Sedang
3	Jaringan Telepon	Provider Telekomunikasi (TELKOM)	Tinggi

4.3.3. Identifikasi Ancaman

Terhadap masing-masing aset yang berhasil teridentifikasi pada tahap sebelumnya (yaitu identifikasi aset), selanjutnya dianalisa kembali akan sejumlah ancaman berpotensi muncul menyertainya. Adapun rumusan ancaman yang berhasil diidentifikasi selanjutnya dirangkum dalam Tabel Identifikasi Ancaman (Lihat Tabel 4.3). Serupa dengan proses identifikasi sebelumnya, proses identifikasi ancaman ini membatasi fokus bahasan pada kantor pusat PT. NCS berikut 2 kantor cabang pembantu yang juga belokasi di Jakarta.

Tabel 4.4 Identifikasi Ancaman

No.	Aset	Klasifikasi Aset	Ancaman
1	Rekam Jejak Karyawan	Aset Informasi (Sensitif)	• Hilang / Dicuri • Termodifikasi tanpa sengaja / hak • Out of Date / Obsolete • Rusak
2	Informasi Harga	Aset Informasi (Sensitif)	• Hilang / Dicuri • Termodifikasi tanpa sengaja / hak • Bocor pada pihak yang tidak berhak
3	Data Finansial Perusahaan	Aset Informasi (Sensitif)	• Hilang / Dicuri • Termodifikasi tanpa sengaja / hak • Bocor pada pihak yang

Tabel 4.3 Identifikasi Ancaman (Lanjutan)

			tidak berhak
4	Password Account Aplikasi / Sistem	Aset Informasi (Sensitif)	• Kesalahan User (Lupa) • Sharing password • Password lemah • Tidak diganti secara berkala
5	Website	Aset Informasi (Publik)	• Hacker (Defacing Website) • Out of date • Malware / Virus / Worm
6	Data Spesifikasi Layanan	Aset Informasi (Publik)	• Out of date • Hilang / Dicuri • Rusak
7	Materi Pemasaran (slide presentasi, brosur)	Aset Informasi (Publik)	• Out of Date • Hilang / Dicuri
8	Company Profile	Aset Informasi (Publik)	• Out of Date
9	All Operating Systems	Aset Software	• Malware / Virus / Worm
10	Mail Server Application	Aset Software	• Spam • Malware / Virus / Worm
10	Custom Application	Aset Software	• Bugs • Malware / Virus / Worm • Kesalahan User
11	PC / Workstation	Aset Hardware	• Rusak / Cacat • Hilang / Dicuri
12	Server	Aset Hardware	• Rusak / Cacat • Hilang / Dicuri
13	Hub / Switch	Aset Hardware	• Rusak / Cacat • Hilang / Dicuri
14	Router	Aset Hardware	• Misconfiguration • Rusak / Cacat • Hilang / Dicuri
15	Modem	Aset Hardware	• Misconfiguration • Rusak / Cacat • Hilang / Dicuri
16	Access Point	Aset Hardware	• Misconfiguration • Rusak / Cacat • Hilang / Dicuri

Tabel 4.3 Identifikasi Ancaman (Lanjutan)

17	UPS	Aset Hardware	• Rusak / Cacat • Hilang / Dicuri
18	Printer	Aset Hardware	• Rusak / Cacat • Hilang / Dicuri
19	Listrik	Aset Fasilitas	• Terjadi Pemadaman
20	Koneksi / Jaringan Internet	Aset Fasilitas	• Bottleneck • Malware / Virus / Worm • Hacker
21	Jaringan Telepon	Aset Fasilitas	• Terputus dari Jaringan Telepon

4.4. IDENTIFIKASI DAN PERUMUSAN KONTROL

Berdasarkan proses identifikasi ancaman pada tahapan sebelumnya, kemudian disimpulkan sejumlah kontrol serta objektif yang perlu diambil oleh pemegang keputusan PT. NCS. Tabel inidentifikasi kontrol berikkut merupakan rangkuman terhadap hasil identifikasi dan perumusan sejumlah kontrol yang dimaksud. Setiap ancaman yang berpotensi muncul pada suatu aset akan dianalisa kembali nilai dampak serta probabilitas terjadinya.

Melalui pendekatan kualitatif yang digunakan, nilai dari kedua kolom terakhir merupakan hasil skala dari 1 hingga 5. Dimana untuk nilai dampak, 1 menunjukkan sangat tidak signifikan atau dapat diabaikan, 2 menujukkan tidak signifikan, 3 menunjukkan level signifikansi rata-rata, 4 menunjukkan relatif signifikan, 5 menunjukkan sangat signifikan. Hal yang sama juga berlaku pada bagian probabilitas (yang menujukkan kemungkinan terjadinya suatu resiko pada persusahaan studi kasus), dimana angka 1 menunjukkan sangat jarang terjadi, 2

menunjukkan jarang terjadi, 3 menujukkan normal terjadi, 4 menunjukkan sering terjadi, dan 5 menjukkan sangat sering terjadi. Proses penentuan rating pada kedua atribut tersebut merupakan hasil olahan observasi langsung menuju perusahaan studi kasus serta diperkuat dengan tinjauan sejumlah dokumen pendukung dan wawancara terhadap sejumlah pihak berwenang pada perusahaan tersebut.

Setelah penentuan kedua atribut yang dimaksud, maka dirumuskanlah kontrol objektif serta kebijakan yang dinilai relevan terhadap setiap ancaman tersebut.

Tabel 4.4 Identifikasi dan Perumusan Kontrol

No.	Aset	Resiko / Ancaman	Nilai Dampak	Probabilitas	Kontrol Objektif	Kebijakan yang sesuai
1	**Aset Informasi**					
	Rekam Jejak Karyawan	Hilang / Dicuri	5	1		Acceptable Use Policy
		Termodifikasi tanpa sengaja / hak	3	3	Penerapan skema otentikasi yang layak	Acceptable Use Policy
		Out of Date / Obsolete	2	3		Acceptable Use Policy
		Rusak	5	2		Acceptable Use Policy
	Informasi Harga	Hilang / Dicuri	3	1	Penempatan data dalam lokasi yang lebih aman (seperti safety box)	Acceptable Use Policy
		Termodifikasi tanpa sengaja / hak	4	2	Penerapan skema otentikasi yang layak	Acceptable Use Policy

Tabel 4.4 Identifikasi dan Perumusan Kontrol (Lanjutan)

		Bocor pada pihak yang tidak berhak	4	3	Penggunaan enkripsi	Acceptable Use Policy, Information Sensitivity Policy
	Data finansial perusahaan	Hilang / Dicuri	5	1	Penempatan data dalam lokasi yang lebih aman (seperti safety box)	Acceptable Use Policy
		Termodifikasi tanpa sengaja / hak	4	2	Penerapan skema otentikasi yang layak	Acceptable Use Policy, Email Retention Policy
		Bocor pada pihak yang tidak berhak	5	1	Penggunaan enkripsi	Acceptable Use Policy, Information Sensitivity Policy
	Password Account Aplikasi / Sistem	Kesalahan User (Lupa)	2	4	Peningkatan security Awareness	Password Policy
		Sharing password	2	4	Peningkatan security Awareness	Password Policy
		Password lemah	2	4	Peningkatan security Awareness	Password Policy
		Tidak diganti secara berkala	2	3	Peningkatan security Awareness	Password Policy
	Website	Hacker (Defacing Website)	2	2	Tidak membuka layanan yang tidak dibutuhkan	Server Security Policy
		Out of date	1	2		Acceptable Use Policy
		Malware / Virus / Worm	2	2	Perlindungan dengan solusi Anti Virus	Server Security Policy
	Data Spesifikasi Layanan	Out of date	3	2		Acceptable Use Policy
		Hilang / Dicuri	2	1		Acceptable Use Policy

Tabel 4.4 Identifikasi dan Perumusan Kontrol (Lanjutan)

		Rusak	1	2		Acceptable Use Policy
	Materi Pemasaran	Out of Date	2	3		Acceptable Use Policy
		Hilang / Dicuri	2	2		Acceptable Use Policy
	Company Profile	Out of Date	2	3		Acceptable Use Policy
2	**Aset Software**					
	All Client Operating Systems	Malware / Virus / Worm	3	3	Perlindungan dengan solusi Anti Virus	Acceptable Use Policy, Removable Media Policy
	All Server Operating Systems	Malware / Virus / Worm	4	2	Perlindungan dengan solusi Anti Virus	Acceptable Use Policy, Removable Media Policy, Server Security Policy
	Mail Server	Spam	2	4	Menjaga informasi internal dari pihak luar yang tidak berhak	Acceptable Use Policy, Automatically Forwarded Email Policy, Email Use Policy
		Malware / Virus / Worm	3	3	Perlindungan dengan solusi Anti Virus	Acceptabel Use Policy, Email Use Policy
	Custom Application	Bugs	5	2	(out of scope)	(out of scope)
		Malware / Virus / Worm	3	1	Perlindungan dengan solusi Anti Virus	Acceptable Use Policy
		Kesalahan User	3	5	Pemahaman fungsi aplikasi	Acceptable Use Policy
3	**Aset Hardware / Infrastruktur**					
	PC / Workstation	Rusak / Cacat	3	1	Pembatasan Akses fisik	Acceptable Use Policy
		Hilang / Dicuri	4	1	Pembatasan Akses fisik	Acceptable Use Policy
	Server	Rusak / Cacat	4	1	Penempatan data dalam lokasi yang lebih aman / Pembatasan Akses fisik	Server Security Policy, Internet DMZ Equipment Policy
		Hilang / Dicuri	5	1	Pembatasan Akses fisik	Acceptable Use Policy

Tabel 4.4 Identifikasi dan Perumusan Kontrol (Lanjutan)

	Hub / Switch	Rusak / Cacat	2	1	Pembatasan Akses fisik	Acceptable Use Policy
		Hilang / Dicuri	3	1	Pembatasan Akses fisik	Acceptable Use Policy
	Router	Misconfiguration	3	3	Penerapan standard konfigurasi	Router Security Policy
		Rusak / Cacat	4	1	Pembatasan Akses fisik	Acceptable Use Policy
		Hilang / Dicuri	5	1	Pembatasan Akses fisik	Acceptable Use Policy
	Modem	Misconfiguration	3	1	Penerapan standard konfigurasi	Internet DMZ Equipment Policy
		Rusak / Cacat	3	1	Pembatasan Akses fisik	Acceptable Use Policy
		Hilang / Dicuri	4	1	Pembatasan Akses fisik	Acceptable Use Policy
	Access Point	Misconfiguration	2	2	Penerapan standard konfigurasi	Wireless Communication Policy
		Rusak / Cacat	3	1	Pembatasan Akses fisik	Acceptable Use Policy
		Hilang / Dicuri	2	1	Pembatasan Akses fisik	Acceptable Use Policy
	UPS	Rusak / Cacat	1	1	Pembatasan Akses fisik	Acceptable Use Policy
		Hilang / Dicuri	2	1	Pembatasan Akses fisik	Acceptable Use Policy
	Printer	Rusak / Cacat	2	1	Pembatasan Akses fisik	Acceptable Use Policy
		Hilang / Dicuri	3	1	Pembatasan Akses fisik	Acceptable Use Policy
4	**Aset Fasilitas**					
	Listrik	Terjadi Pemadaman	5	1	(out of scope)	Penyediaan Listrik cadangan melalui genset (out of scope)
	Koneksi / Jaringan Internet	Bottleneck	2	2	Implementasi prioritas layanan (QoS)	Internet DMZ Equipment Policy
		Malware / Virus / Worm	3	1	Perlindungan dengan solusi Anti Virus	Acceptable Use Policy
		Hacker	2	1	Implementasi firewall pada	VPN Policy, Extranet Policy

Tabel 4.4 Identifikasi dan Perumusan Kontrol (Lanjutan)

					jaringan intenal	
	Jaringan Telepon	Terputus dari Jaringan Telepon	4	1	(out of scope)	(out of scope)

Secara garis besar, hasil rumusan identifikasi kontrol melalui tabel diatas memerlukan serangkaian tindak lanjut yang perlu diambil oleh para pemegang keputusan pada PT. NCS, yaitu:

- Penerapan kebijakan keamanan yang perlu untuk didokumentasikan, disetujui (oleh pemegang keputusan), didistribusikan serta disosialisasikan ke segenap karyawan PT NCS. Adapun cakupan kebijakan keamanan yang dimaksud telah dibahas pada subbab 4.1 (serta lampiran 2 untuk penyajian yang lebih detail).
- Pengembangan prosedur keamanan yang diturunkan dari kebijakan keamanan yang telah didefinisikan sebelumnya. Prosedur tersebut nantinya menjadi bimbingan teknis bagi para karyawan dalam berhubungan infrastruktur IT di PT. NCS.
- Sosialisasi prosedur serta standard yang merupakan penurunan dari kebijakan keamanan yang telah didefinisikan sebelumnya. Untuk menunjang efektifitas realisasinya, proses sosialisasi tersebut hendaknya disertai dengan *reward and punishment* terhadap setiap entitas terkait dalam PT. NCS. Mekanisme ini tentunya mengacu pada mekanisme serupa yang selama ini telah diterapkan pada PT. NCS.