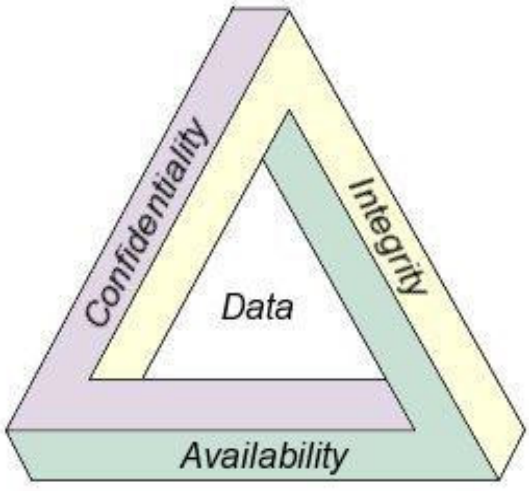
BAB II

LANDASAN TEORI

2.1. KONSEP DASAR KEAMANAN INFORMASI

Selama lebih dari 20 tahun, keamanan informasi telah dibangun atas 3 kunci dasar dari prinsip kunci keamanan informasi yaitu: *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan).



Gambar 1 CIA Triad (www.SafemodeSecurities.com)

2.1.1. *Confidentiality*

Confidentiality (kerahasiaan) berfokus pada upaya untuk menghindari pengungkapan secara tidak sah terhadap informasi yang bersifat rahasia maupun sensitif. Pengungkapan informasi tersebut dapat terjadi secara disengaja, seperti pemecahan sandi untuk membaca informasi, atau dapat terjadi secara tidak disengaja, dikarenakan kecerobohan dari individu dalam menangani informasi.

Sejumlah mekanisme yang sering digunakan untuk mempertahankan konsep confidentiality meliputi (Osborne, 2006):

- Klasifikasi Data

  Merupakan proses pelabelan informasi sehingga masing-masing individu mengetahui siapa yang diizinkan untuk melihatnya dan siapa yang tidak.

- Enkripsi

  Merupakan mekanisme teknis yang digunakan untuk menjaga kerahasiaan (*confidentiality*).

- Pemusnahan Peralatan (*Equipment Disposal*)

  Merupakan segala bentuk usaha / aktivitas yang ditujukan untuk melindungi kearahasiaan suatu informasi ketika tidak lagi dipergunakan dalam media penyimpanan. Beberapa contoh aksi dalam hal ini adalah proses format pada disk sekurang-kurang 7 kali atau lebih, penyobekan kertas (dengan bantun mesin *shredder*), dan lain sebagainya.

2.1.2. *Integrity*

Dalam keamanan informasi, *integrity* (integritas atau keutuhan) berarti bahwa data tidak dapat dibuat, diganti, atau dihapus tanpa proses otorisasi. Dengan kata lain, *integrity* merupakan prinsip yang ditujukan untuk menjaga keakuratan suatu informasi (Osborne, 2006). Sebagai contoh, data yang disimpan pada salah satu bagian dari sistem database telah melewati persetujuan dengan data terkait yang tersimpan pada bagian lain dari sistem database. Adapun tujuan dari *integrity* adalah:

- Menghindari modifikasi informasi dari *user* atau pengguna yang tidak berhak.
- Menghindari akses yang tidak sah atau modifikasi informasi yang tidak disengaja dari pengguna yang tidak berhak.
- Pemeliharaan terhadap konsistensi internal dan ekternal.
    - Konsistensi internal memastikan bahwa data internal tetap konsisten. Sebagai contoh, pada suatu database organisasi, jumlah item yang dimiliki oleh suatu organisasi harus sama dengan jumlah item yang ditampilkan pada database.
    - Konsistensi eksternal menjamin bahwa data yang disimpan pada database konsisten dengan dunia nyata. Serupa dengan contoh sebelumnya, jumlah item yang ada secara fisik pada dunia nyata harus sama dengan jumlah item yang terdapat pada database.

Beragam usaha yang dapat dilakukan untuk menjaga integritas terhadap suatu data atau informasi meliputi:

- *Checksums*

  Merupakan serangkaian angka yang dihasilkan melalui fungsi matematika untuk memastikan bahwa blok data yang diberikan tidak berubah.

- Kontrol Akeses

  Merupakan mekanisme untuk memastikan bahwa individu / pihak tertentu dapat hanya dapat melakukan sejumlah aksi tertentu.

2.1.3. *Availability*

Availability menjamin bahwa pengguna sistem yang berhak memiliki akses tanpa interupsi terhadap sistem dan jaringan. Hal tersebut memastikan bahwa informasi atau sumber daya akan selalu tersedia ketika dibutuhkan.

Bentuk-bentuk usaha yang dapat dilakukan untuk menjaga ketersediaan data meliputi:

- *Redundant Systems* atau implementasi sistem berganda kedalam suatu infrastruktur (seperti *disk array* atau mesin-mesin yang di-*cluster*).
- Perangkat Lunak Anti Virus untuk menghentikan *worm* atau program berbahaya lainnya yang mengganggu kondisi jaringan.

- Penerapan perangkat IPS guna mengantisipasi ancaman serangan tertentu (seperti DDoS) yang dapat mengganggu ketersediaan suatu layanan.

Dengan kemunculan *e-commerce*, terdapat suatu prinsip lain yang juga ditambahkan kedalam prinsip CIA, yaitu prinsip *nonrepudiation*.

2.1.4. *Nonrepudiation*

Nonrepudiation dapat didefinisikan sebagai prinsip yang memastikan suatu aksi atau transaksi menjadi tidak dapat dibantah. Dalam kebanyakan kasus, berbagai layanan yang diturunkan melalui prinsip ini telah menggantikan penggunaan tanda tangan atau peranan notaris pada dokumen berbasis kertas.

W. Ford sebagai salah seorang pionir penerapan PKI pada e-commerce, mengklasifikasikan sejumlah jenis *nonrepudiation* (Ford & Baum, 1997). Diantaranya adalah sebagai berikut:

- *Nonrepudiation* pada tanda terima

  Melalui mekanisme ini pengirim dapat membuktikan bahwa pesan telah dikirimkan kepada orang yang tepat. Hal ini dimaksudkan untuk menghindari situasi dimana pihak pengirim telah mengirimkan pesan atau informasi namun tidak dapat membuktikan bahwa pihak penerima telah mendapatkannya.

- *Nonrepudiation* bagi pengirim

  Merupakan mekanisme yang mampu membuktikan bahwa suatu pesan datang dari orang yang tepat. Hal ini dimaksudkan untuk menghindari situasi dimana pesan yang diterima kemudian dibantah oleh pihak pengirim.

- *Nonrepudiation* terhadap waktu

  Merupakan mekanisme yang mendefinisikan waktu ketika suatu pesan atau informasi dikirimkan.

2.2. MANAJEMEN RESIKO

Berdasarkan definisi yang terdapat pada CISA Manual Review 2007, manajemen resiko merupakan proses identifikasi kerentanan dan ancaman terhadap sumber daya informasi yang digunakan oleh organisasi objektif bisnis, dan memutuskan tindak lanjut yang akan diambil untuk mengurangi resiko ke tingkatan yang dapat diterima berdasarkan nilai sumber informasi tersebut terhadap organisasi.

Terdapat dua hal dalam definisi tersebut yang membutuhkan sejumlah klarifikasi. Pertama, proses dari manajemen resiko merupakan proses iteratif yang berkelanjutan. Hal ini dikarenakan lingkungan bisnis yang secara konstan berubah dan ancaman serta kerentanan baru muncul setiap harinya. Kedua, pemilihan tindah lanjut yang digunakan untuk mengatur resiko harus seimbang dengan

produktivitas, biaya, efektifitas tindak lanjut tersebut serta nilai dari aset informasi yang dilindungi.

Terdapat sejumlah pendekatan yang dapat dilakukan dalam menghadapi resiko. Beberapa pendekatan yang dimaksud adalah:

- Menghindari Resiko (*Risk Avoidance*), dimana jika memungkinkan suatu proses atau aktivitas tidak diimplementasi untuk menghindari resiko yang lebih besar.
- Mengurangi Resiko (*Risk Mitigation*), melalui proses pendefinisian dan implementasi kontrol untuk melindungi infrastruktur IT.
- Transfer Resiko (*Risk Transfering*), berbagi resiko dengan partner atau ditransfer berdasarkan cakupan asuransi.
- Menerima Resiko (*Risk Acceptance*), merupakan tindakan formal untuk menerima eksistensi dari suatu resiko karena dampaknya yang kurang signifikan namun tetap melakukan proses pemantauan terhadap resiko.
- Menghilangkan Resiko (*Risk Elimination*), dimana jika memungkinkan sumber dari suatu resiko dihilangkan.

2.3. JENIS-JENIS PENGENDALIAN

Dalam rangka meminimalisir resiko, pihak manajemen dari suatu organisasi dapat menerapkan salah satu atau lebih jenis-jenis pengendalian berikut (Krutz & Vines, 2003).

2.3.1. *Administrative Control*

Administrative Control (Kontrol Administratif) terdiri dari standard, prosedur, kebijakan dan garis pedoman tertulis yang disetujui bersama. *Administrative Control* membentuk bingkai kerja terhadap bisnis yang sedang berjalan dan pengaturan terhadap orang. Hal ini berarti bahwa *Administrative Control* memberitahuan kepada individu-individu dalam organisasi tentang bagaimana bisnis dijalankan dan bagaimana operasional harian seharusnya dilakukan.

Sebagai contoh, hukum dan peratutan yang dibuat oleh badan pemerintah merupakan salah satu jenis *Administrative Control*. Beberapa industri juga turut memiliki standard, prosedur, kebijakan dan garis pedoman yang harus diikuti, seperti standar keamanan data *Payment Card Industry* (PCI) yang harus diikuti oleh Visa dan Master Card sebagai contoh. Contoh-contoh lainnya dari kontrol administratif meliputi kebijakan keamanan perusahaan, kebijakan *password*, kebijakan disiplin, kebijakan perekrutan, dan lain sebagainya.

2.3.2. *Logical Control*

Logical Control (Kontrol Logik atau biasa disebut dengan kontrol teknis) merupakan bentuk pengendalian yang menggunakan data dan piranti lunak untuk memantau dan mengontrol akses terhadap informasi dan sistem komputer. Sebagai contoh: *password*, *firewall* berbasis jaringan dan host, sistem deteksi intrusi jaringan (*Network IDS*), *access control lists*, dan enkripsi data merupakan bentuk-bentuk *Logical Control*.

Salah satu bentuk kontrol logik yang penting untuk diketahui adalah prinsip *least privilege*. Prinsip ini menghendaki seseorang (individu), program atau proses dari sistem tidak diberikan hak istimewa (*privilege*) lebih dari yang dibutuhkan dalam menjalankan tugasnya.

2.3.3. *Physical Control*

Physical Control (Kontrol secara fisik) merupakan bentuk pengendalian yang memantau dan mengontrol lingkungan kerja dan fasilitas komputer. Kontrol ini juga memantau dan mengendalikan akses ke dan dari fasilitas tersebut. Sebagai contoh: pintu, kunci, pemanas dan pendingin ruang, alarm asap dan api, kamera, petugas keamanan, dan lain-lain. Pemisahan jaringan dan tempat kerja kedalam area-area berdasarkan fungsi juga merupakan bentuk kontrol secara fisik.

Salah satu bentuk kontrol fisik yang penting untuk diketahui namun sering terlupakan adalah *separation of duties* (pemisahan kewajiban). Prinsip ini memastikan bahwa seseorang tidak dapat menyelesaikan suatu tugas kritis tanpa

peranan individu/pihak lain. Secara lebih jauh, prinsip ini juga memastikan tidak terjadinya penyalahgunaan wewenang oleh seseorang.

2.4. KLASIFIKASI KEAMANAN UNTUK INFORMASI

Salah satu aspek penting dari keamanan informasi dan manajemen resiko adalah pengenalan terhadap nilai informasi dan pendefinisian prosedur yang layak dan proteksi yang dibutuhkan untuk informasi tersebut. Tidak semua informasi sama sehingga tidak semua informasi membutuhkan perlindungan dengan derajat yang sama. Untuk itu dibutuhkan klasifikasi informasi.

Langkah pertama dalam klasifikasi informasi adalah mengidentifikasi anggota manajemen senior sebagai pemilik atas informasi tertentu untuk diklasifikasikan. Selanjutnya, mengembangkan kebijakan klasifikasi. Kebijakan tersebut sebaiknya menggambarkan label klasifikasi yang berbeda, mendefinisikan kriteria terhadap informasi untuk ditetapkan sebagai label tertentu, dan mendaftarkan kontrol keamanan yang dibutuhkan untuk setiap klasifikasi.

Klasifikasi keamanan informasi yang umum digunakan dalam dunia bisnis adalah: *public*, *sensitive*, *private*, *confidential* (*Federation of American Scientists*, 2002). Sedangkan label klasifikasi keamanan informasi yang umum digunakan dalam pemerintahan atau militer meliputi: *unclassified*, *sensitive but unclassfied*, *confidential*, *secret*, dan *top secret*.

Sejumlah faktor yang mempengaruhi klasifikasi terhadap suatu informasi meliputi:

- Seberapa berharga nilai dari suatu informasi terhadap organisasi
- Seberapa lama usia dari informasi tersebut
- Apakah informasi tersebut telah menjadi kadaluarsa.

2.5. KONTROL AKSES

Akses terhadap informasi yang dilindungi harus dibatasi kepada individu-individu yang berhak mengakses informasi tersebut. Program-program komputer, dan komputer-komputer yang memproses informasi juga harus dilindungi. Hal ini tentunya membutuhkan mekanisme pada tempatnya untuk mengontrol akses terhadap informasi yang dilindungi tersebut. Dalam implementasinya, mekanisme kontrol akses hendaknya seimbang dengan nilai informasi yang dilindungi. Fondasi dasar dari mekanisme kontrol akses dibangun atas mekanisme identifikasi dan otentikasi.

2.5.1. Identifikasi

Identifikasi merupakan pernyataan tentang siapakah seseorang tersebut atau apakah sesuatu tersebut. Jika seseorang membuat penyataan ”*Hello, my name is John Doe.*”, maka ia membuat klaim atas jati dirinya. Namun, klaim tersebut bisa berarti benar atau sebaliknya. Sebelum John Doe diberikan akses terhadap informasi yang dilindungi, maka akan menjadi penting untuk dipastikan bahwa seseorang yang mengklaim sebagai John Doe tersebut adalah benar John Doe.

2.5.2. Otentikasi

Otentikasi merupakan aksi untuk memverifikasi klaim atas suatu identitas. Ketika John Doe datang ke Bank untuk melakukan penarikan dana, ia menyampaikan kepada teller bank bahwa ia adalah John Doe (yang merupakan aksi klaim atas identitas). Selanjutnya teller bank memintanya untuk menunjukkan ID photo berikut kartu identitas untuk dilakukan pengecekan dan pembandingan bahwa orang yang mengaku sebagai John Doe tersebut adalah benar John Doe.

Menurut Osborne (1997), setidaknya ada tiga jenis otentikasi yang dapat dirangkum sebagai berikut:

- Sesuatu yang Anda ketahui (*Something you know*) – dimana hal ini umumnya berkaitan dengan *password*.
- Sesuatu yang Anda miliki (*Something you have*) – dimana hal ini berkenaan dengan kebutuhan akan objek fisik yang digunakan untuk otentikasi, seperti token penghasil angka, *swipe card*, atau sertifikat X509.
- Sesuatu tentang Anda (*Something you are*) – dimana dalam dunia teknologi dapat berarti identitas *biometric*, yang melibatkan pembaca sidik jari, pengenal suara, pemindai retina mata, dan lain sebagainya.

2.6. ISO/IEC 27002 SEBAGAI STANDAR KEAMANAN INFORMASI

ISO/IEC 27002 merupakan suatu standard yang dipublikasikan International Organization (ISO) dan International Electrotechnical Comission (IEC) sebagai ISO/IEC 17799:2005 yang kemudian dinomor ulang sebagai ISO/IEC 27002:2005 pada Juli 2005. Standard ini diberi judul *Information Technology – Security Techniques – Code of practice for information security management*. Disamping itu, standard ini merupakan revisi dari versi yang pertama kali dipublikasikan oleh ISO/IEC pada tahun 2000, yang juga merupakan salinan dari British Standard 7799-1:1999.

ISO/IEC 27002 menyediakan rekomendasi *best practice* terhadap manajemen keamanan informasi untuk digunakan oleh mereka yang bertanggung jawab untuk proses inisiasi, implementasi, dan pemeliharaan Information Security Management Systems (ISMS) pada suatu organisasi.

Adapun cakupan dari standard ini meliputi 12 domain utama, yaitu:

- *Risk Assessment and threatment* – analisa resiko keamanan informasi suatu organisasi
- *Security policy*
- *Organization of information security* – tata kelola keamanan informasi
- *Asset Management* – inventori dan klasifikasi aset informasi
- *Human resouces security* – aspek keamanan untuk perekrutan, dan pemindahan karyawan, hingga meninggalkan organisasi

- *Physical and enviromental security* – proteksi terhadap fasilitas komputer
- *Communication and Operation management* – manajemen pengendalian keamanan secara teknis pada level sistem dan jaringan
- *Access Control* – pembatasan terhadap hak akses ke jaringan, sistem, aplikasi, fungsi dan data.
- *Information systems acquisition, development and maintenance* – pembangunan keamanan kedalam aplikasi
- *Information Security incident management* – antisipasi dan respon yang sepantasnya terhadap pelanggaran keamanan sistem informasi
- *Business continuity management* – perlindungan, pemeliharaan, dan perbaikan terhadap sistem dan proses bisnis yang kritis
- *Compliance* – memastikan kecocokan dengan hukum, standard, kebijakan keamanan informasi dan peraturan lainnya yang berlaku

Berhubung luasnya domain masalah yang terdapat pada standard tersebut dan terbatasnya waktu penelitian yang ada, fokus dari penulisan tesis ini lebih dititikberatkan pada domain kedua dan ketiga yaitu tentang *security policy* dan *organization of information security*.

2.7. SEKILAS TENTANG PT. NCS

PT. NUSANTARA CARD SEMESTA (NCS) adalah perusahan pelayanan jasa yang bergerak dibidang pengiriman (kurir), antara lain pengiriman kartu kredit, rekening koran, surat tagihan (billing), brosur, majalah, paket dan dokumen lainnya dari perusahaan ke perusahaan lain (b2b) ataupun dari perusahaan ke nasabahnya.

Hingga saat ini wilayah yang dijangkau oleh layanan PT. NCS adalah seluruh Daerah Khusus Ibukota Jakarta, Bogor, Depok, Tangerang, Bekasi, Krawang, Cikampek, Purwakarta, Cilegon dan Serang. PT. NCS dalam memperluas pelayanannnya telah membuka Kantor Cabang di berbagai kota besar di seluruh Indonesia antara lain Medan, Padang, Palembang, Balikpapan, Samarinda, Ujung Pandang, Surabaya, Semarang, Yogyakarta, Solo, Malang, Purwokerto, Cirebon, Batam, Pontianak, Banjarmasin, Manado, Gorontalo, Pakanbaru, Jambi, Ambon, Banda Aceh, Denpasar dan lain-lain, sehingga akan lebih menjamin penyampaian kiriman ke tujuan-tujuan tersebut. Untuk wilayah-wilayah yang belum memiliki kantor cabang, PT. NCS bekerja sama dengan agen-agen yang berada di masing-masing kota tersebut.

Dalam kegiatan operasionalnya, PT. NCS melayani berbagai perusahaan dalam pengiriman dokumen dan paket, antara lain perusahaan di bidang perbankan, asuransi, media cetak dan elektronik, telekomunikasi, industri dan perdagangan. Saat ini, PT. NCS telah mencapai jumlah pengiriman lebih dari 3.000.000 kiriman per-bulannya.

Sumber daya manusia yang profesional didukung teknologi terkini dan sistem real time on line, menjadikan kualitas pelayanan seluruh jaringan NCS di 338 kota besar Indonesia mampu memberikan kepuasan kepada kustomer. Kerahasiaan data, ketepatan waktu, serta keakuratan penanganan merupakan tujuan dan prinsip yang tidak bisa ditawar oleh setiap karyawan NCS.

2.7.1. Latar Belakang PT. NCS

PT. NUSANTARA CARD SEMESTA didirikan di Jakarta pada tanggal 6 Desember 1994, berdasarkan Akte Notaris Abdoellah Hamidy, S.H. No. 6 dan telah memperoleh pengesahan dari Menteri Kehakiman Republik Indonesia dengan Keputusan Menteri Nomor C2-3.410.HT.01.01 tahun 1995, tertanggal 14 Maret 1995, serta berdasarkan Surat Keputusan Divisi Perdagangan No. SIUP. 3989/09/03/PS/XII tahun 1994. Modal awal yang dimiliki oleh perusahaan sebesar Rp. 120.000.000; (seratus dua puluh juta rupiah), yang terdiri dari 1.200 (seribu dua ratus) lembar saham dengan nilai nominal masing-masing saham sebesar Rp. 100.000; (seratus ribu rupiah). Akte pendirian tersebut telah mengalami perubahan, perubahan terakhir dengan akte No. 1 Tanggal 1 Agustus 2003 yang dibuat dihadapan H. Rizul Sudarmadi, S.H. Notaris di Jakarta tentang peningkatan modal dasar perseroan menjadi Rp. 460.000.000; yang terbagi atas 4.600 lembar saham dan telah disetor penuh. Akte perubahan tersebut telah mendapat pengesahan dari Menteri Kehakiman dan Hak Azasi Manusia sesuai

dengan surat Keputusan: No. C-2283HT.01.04.TH.2003 tanggal 25 September 2003.

Nama-nama pemegang saham dan pengurus adalah Reni Sitawati Siregar sebagai Komisaris dan Budiyanto Darmastono sebagai Direktur Utama. Pada tanggal 4 Mei 2001 dilakukan perubahan dan penyesuaian Akte Notaris, yang dikeluarkan oleh Notaris Yonsah Minasa, S.H., di Jakarta dimana dimasukkan Ir. Mahatma Indra Siregar sebagai salah satu pemegang saham.

PT. NUSANTARA CARD SEMESTA (PT. NCS) yang semula beralamat di Jl. Tali Raya G-1 No. 16, Slipi, Jakarta Barat, dengan nomor telepon (021) 533 2240, seperati yang tertera dalam surat keputusan di atas, bergerak dalam bidang pelayanan jasa pengiriman (kurir), antara lain pengiriman kartu kredit, rekening koran, surat tagihan (billing), brosur, majalah, paket dan dokumen lainnya dari perusahaan ke perusahaan lain (b2b) ataupun dari perusahaan ke nasabahnya.

2.7.2. Profil Perusahaan

Nama Perusahaan : PT NUSANTARA CARD SEMESTA (NCS)
Didirikan pada 1994 (No. 459/SIJPT/DIRJEN/1995)

Alamat : Jl.Brigjend Katamso No. 7 Slipi Jakarta Barat 11420
Telepon: 569 69 777 Fax : 569 68 877
Website : www.ptncs.com

Lini Bisnis :

- Layanan Pengiriman Express pintu ke pintu (*Express door to door Service*) melalui Udara, Darat dan Laut
- Transportasi Intermoda (Domestik dan International)
- Layanan Logistik (*Warehousing and Distribution*)
- Solusi Layanan Kurir Terkostumisasi

Keanggotaan / *Agency*:

- ASPERINDO (Ass. Of Indonesian Express Delivery Companies)
- Agen kargo Perusahaan Penerbangan Garuda resmi (dengan No. 8184)

Pemegang Saham : 1. Budiyanto Darmastono
2. Reni S Siregar
3. Mahatma Indra Siregar

Kurir dan Armada Pengiriman : - Jumlah Kurir : 2,500 (Seluruh Indonesia)
: 1,500 (Jadebotabek)
- Jumlah Truk & Van : 45 unit

Jumlah Staff Pendukung: 1,000 staff

Cabang dan Agen : - Cabang : 32

- Agen : 50

Total : 82

Sub-Agen (Agen Tidak Langsung) : 60

Volume Transaksi Rata-rata (2006) : > 3,000,000 kiriman / bulan

Layanan Logistik :

- *MGM Warehouse and Distribution* untuk Citibank di Wisma Aldiron dengan luas 125 meter persegi ; dioperasikan oleh 4 staff ; 250 SKU;barcode label system
- *Reward Warehouse and Distribution* untuk Citibank di Wisma Atl degan luas bangunan 170 meter persegi ; dioperasikan oleh 3 staff ; 150 SKU; barcode label system
- *Reward Warehouse and Distribution* untuk HSBC di Slipi dengan luas bangunan 60 meter persegi ; dioperasikan oleh 2 staff ; 70 SKU; barcode label system

VISI PT NCS : Menjadi Perusahaan kurir pilihan yang menjangkau seluruh pelosok Indonesia dengan layanan Dokumen dan Barang paling cepat, aman dan kompetitif.

MISI PT NCS : Mengoperasikan teknologi terkini yang aplikatif dan menyiapkan jaringan diseluruh Indonesia serta meningkatkan Kualitas dan Kuantitas Sumber daya manusia.

Objektif PT. NCS : Sumber daya manusia yang profesional didukung teknologi terkini dan sistem real time on line, menjadikan kualitas pelayanan seluruh jaringan NCS di 338 kota besar Indonesia mampu memberikan kepuasan kepada pelanggan. Kerahasiaan data, ketepatan waktu, serta keakuratan penanganan merupakan prinsip yang tidak bisa ditawar oleh setiap karyawan NCS.

2.7.3. Struktur Organisasi Perusahaan