LAMPIRAN

Lampiran 1. Rangkuman Wawancara dengan Key Personel PT. NCS

Berikut ini merupakan rangkuman wawancara dengan personel dari PT. NCS (yang melibatkan Pak Toto selaku Manager Departemen TI dan sdri. Dian Kardasih selaku Supervisor IT Application) yang terkait dengan topik penelitian ini. Wawancara ini dirangkum melalui korespodensi langsung, secara tertulis (melalui *e-mail*), hingga pembicaraan melalui telepon.

Apakah sebelumnya PT NCS telah memiliki IT Policy ? [Standard ISO 27002 sesi 5.1.1]

- ⇨ Belum. Kalaupun ada sifatnya masih *ad-hoc* atau karena adanya permintaan dari *customer* dari PT. NCS dalam perjanjian kerja sama yang dibuat.

Siapa pula yang akan bertanggung jawab jika suatu ketika PT NCS memilih untuk mengembangkan IT Policy atau bahkan IT Security Policy serta proses sosialisasinya ? [Standard ISO 27002 sesi 6.1.1 dan sesi 6.1.2]

- ⇨ Sebenarnya, dalam menghadapi tantangan akan kebutuhan akan eksistensi dari IT Policy, PT. NCS telah mengembangkan tim kecil yang

bertanggung jawab dalam menyiapkan hal tersebut (berikut juga dengan konsep auditnya). Tim yang terdiri dari 3 personel tersebut, meliputi:

- *Supervisor IT Application* (saya sendiri),
- *Customer Service Manager*, dan
- *Business Development Manager.*

Mengenai tim tersebut, apakah ada SK (Surat Ketetapan) tim atau kelompok kerja tersebut sebagai tim yang bertanggung jawab dalam penyusunan suatu IT Policy / konsep audit?

⇨ Sejauh ini belum ada.

Apa yang menjadi tanggung jawab dari tim tersebut? [Standard ISO 27002 sesi 6.1.3]

⇨ Proses audit internal dan eksternal dari PT. NCS. Dari sisi internal berarti audit dari sisi manajerial perusahaan sedangkan dari sisi eksternal berarti dari sisi *customer*.

⇨ Proses audit internal umumnya mengatur sejumlah hal seperti aturan penghapusan data *customer* (yang sifatnya rahasia) secara berkala, *update* anti-virus, dan lain sebagainya.

⇨ Proses audit eksternal bertujuan untuk memastikan apakah perjanjian kerja sama yang dibuat dengan *customer* yang bersangkutan telah sesuai dengan realisasinya.

Atas dasar apa pula proses pemilihan atau pembentukan dari tim tersebut?

⇨ Mengenai atas dasar apa tim ini dibentuk, barangkali alasannya:

- Personel yang terlibat merupakan orang yang mengerti akan infrastruktur / teknologi.
- Personel tersebut juga personel yang memiliki hubungan langsung dengan *customer*.
- Disamping itu, personel yang terlibat juga merupakan personel yang terbilang cukup mengerti tentang operasional dari PT. NCS.

Apakah penyusunan suatu policy di PT. NCS tidak membutuhkan keterlibatan orang yang berada pada level direktur? Lantas, jika suatu policy selesai disusun, siapa pula yang berhak untuk merevisi, memperbaiki hingga bahkan menyetujui policy tersebut? Dan siapa pula yang bertanggung jawab dalam proses sosialisasinya kelak?

⇨ Direktur sangat terlibat dalam penyusunannya, namun hanya pada tahap review saja. Karena nantinya direktur yang memberikan tanda tangan (pengesahannya). Kami dari tim tersebut hanya sebatas penyusunan konsep. Sedangkan sosialisasi dilakukan oleh tim IT dan HRD untuk yang sifatnya general.

Berbicara tentang aset infrastruktur TI bisakah dijelaskan tentang inventori (aset TI khususnya) yang terdapat pada kantor pusat PT. NCS dan kantor cabang yang terletak di Kemanggisan dan G2?

⇨ Kira-kira rincian inventori aset TI yang kami miliki adalah sebagai berikut:

Untuk Pusat:

Jumlah Workstation : 2 unit

Jumlah Server : 10 Unit

Server yang diakses dari luar sejumlah 2 unit, Server Website dan Server Email

Database Server yang ada menggunakan SQL Server 2005 dan Foxpro database

Presentase OS :

1. Windows XP 100 % pada workstation
2. Windows Server 2003 100% pada Server

Untuk layanan Email, aplikasi server yang digunakan adalahMailer daemon.

Untuk Cabang:

A. Cabang Kemanggisan, Jakarta

Jumlah Server : 3 Unit (OS Windows Server 2003)

Jumlah Works Station : 78 User (OS Windows Xp)

Sedangkan Database yang digunakan adalahSQL Server 2005

B. Cabang G2, Jakarta

Jumlah Server : 2 Unit (OS Windows Server 2003 dengan Database Foxpro)

Jumlah User : 127 User (OS Windows XP)

Lampiran 2. Dokumen Kebijakan Keamanan Informasi

Berikut ini merupakan sejumlah bentuk kebijakan keamanan informasi yang penulis susun sesuai dengan hasil risk assessment dari PT. NCS. Kebijakan keamanan informasi ini disusun dengan mengacu referensi pada sejumlah sumber seperti SANS, InfoSec, BSI Global, dan ISO27001Security.com.

Policy Document Name	*Acceptable Encryption Policy*
Owner	PT. NCS
Prepared By	Junian Dani
Approved By	IT Manager of PT. NCS
Revision	1.0 - Initial Release

1.0 Tujuan

Tujuan dari kebijakan ini adalah untuk memberikan panduan yang membatasi penggunaan metode enkripsi yang telah terbukti bekerja secara efektif.

2.0 Ruang Lingkup

Kebijakan ini diterapkan kepada semua karyawan PT. NCS dan afiliasinya.

3.0 Kebijakan

Standard algoritma seperti DES, Blowfish, RSA, RC5 dan IDEA seharusnya digunakan sebagai basis untuk teknologi enkripsi. Algoritma-algoritma tersebut merupakan metode pengacakan (chiper) yang digunakan terhadap aplikasi. Sebagai contoh, Pretty Good Privacy (PGP) dari Network Associate menggunakan kombinasi IDEA dan RSA atau Diffie-Hellman, sedangkan Secure

Socket Layer (SSL) menggunakan enkripsi RSA. Tingkat kedalaman kunci untuk cryptosystem simetrik minimal harus 56 bit. Sedangkan tingkat kedalaman kunci untuk cryptosystem non simetrik harus memberikan kekuatan yang equivalen. Tingkat kebutuhkan kedalaman kunci dari PT NCS akan direview setiap tahunnya dan di-upgrade jika memungkinkan secara teknologi.

4.0 Sanksi dan Ancaman

Setiap karyawan yang ditemukan melanggar kebijakan ini akan diberikan tindakan disipliner hingga pemutusan hubungan kerja.

5.0 Definisi

Term	**Definition**
Enkripsi *Proprietary*	Algoritma yang tidak dibuat atau dimiliki oleh publik. Pengembang dari algoritma ini dapat berupa vendor, individu atau institusi pemerintah.
Enkripsi Simetris	Metode enskripsi yang memiliki kunci serupa untuk proses enkripsi dan dekripsi data.
Enkripsi Asimetris	Metode enksipsi yang memiliki 2 kunci berbeda dimana satu untuk menjalankan proses enkripsi dan lainnya untuk proses dekripsi data (contoh: enkripsi kunci publik).

Policy Document Name	*Acceptable Use Policy*
Owner	PT. NCS
Prepared By	Junian Dani
Approved By	IT Manager of PT. NCS
Revision	1.0 - Initial Release

1.0 Rangkuman

Kebijakan ini tidak dimaksudkan untuk membatasi kultur yang dibangun oleh PT NCS yang mengedepakan ketebukaan, kepercayaan, dan integritas. Kebijakan ini dijalankan untuk melindungi keryawan, partner dari PT NCS dari aksi merugikan atau ilegal yang dilakukan individu-individu baik disengaja maupun sebaliknya.

Internet/Intranet/Extranet serta sistem terkait, meliputi (namun tidak terbatas) peralatan komputer, piranti lunak, sistem operasi, media penyimpanan, akun jaringan yang memberikan layanan seperti email, WWW, FTP merupakan properti dari PT NCS. Sistem-sistem tersebut digunakan untuk tujuan bisnis dalam rangka melayani kepentingan perusahaan. Silahkan mereview kebijakan SDM untuk detail lebih lanjut.

Keamanan efektif merupakan suatu usaha bersama yang melibatkan partisipasi dan dukungan dari setiap keryawan PT. NCS dan afiliasinya yang bergelut dengan informasi dan/atau sistem informasi. Adalah tanggung jawab dari semua pengguna komputer untuk mengetahui dan menjalankan aktivitas mereka sesuai dengan garis pedoman ini.

2.0 Tujuan

Tujuan dari kebijakan ini adalah sebagai menjelaskan penggunaan yang diperbolehkan terhadap peralatan komputer pada PT. NCS. Aturan-aturan ini ditempatkan untuk melindungi karyawan dan PT. NCS. Penggunaan yang tidak tepat dapat menimbulkan sejumlah resiko pada PT NCS yang meliputi serangan virus, sistem jaringan dan layanan yang rentan serta persoalan hukum.

3.0 Ruang Lingkup

Kebijakan ini diterapkan kepada karyawan, kontraktor, konsultan, pekerja sementara, dan pekerja lainnya pada PT. NCS meliputi semua personil yang berafiliasi dengan pihak ketiga. Kebijakan ini diterapkan kepada semua peralatan yang dimiliki atau disewakan oleh PT. NCS.

4.0 Kebijakan

4.1 Penggunaan Umum dan Kepemilikan

1. Administrasi jaringan PT. NCS dimaksudkan untuk memberikan tingkat privacy yang layak, pengguna seharusnya perduli bahwa data yang mereka ciptakan pada sistem perusahaan merupakan properti dari PT. NCS. Oleh karena kebutuhan untuk melindungi jaringan PT. NCS, pihak manajemen tidak dapat menjamin kerahasiaan informasi yang tersimpan pada peralatan jaringan milik PT. NCS.

2. Kebijakan ini merekomendasikan bahwa semua informasi yang dianggap sensitif atau rentan oleh pengguna sebaiknya dienkripsi.
3. Untuk tujuan pemeliharaan jaringan dan keamanan, individu berwenang dalam PT. NCS dapat memantau peralatan, sistem dan lalu lintas jaringan kapanpun, sesuai degan kebijakan Audit yang dimiliki oleh PT. NCS.
4. PT. NCS menyediakan hak untuk audit sistem dan jaringan secara berkala untuk memastikan kesesuaian (*compliance*) dengan kebijakan ini.

4.2 Keamanan dan Informasi Proprietary

1. Antar muka pengguna terhadap informasi terkandung dalam Internet/Intranet/Extranet serta sistem terkait seharusnya diklasifikasikan sebagai rahasia dan tidak rahasia, sebagaimana didefinisikan dalam garis pedoman kerahasiaan perusahaan, dimana lebih lengkapnya dapat ditemukan dalam kebijakan yang dikeluarkan bagian Sumber Daya Manusia. Contoh-contoh dari informasi rahasi meliputi (namun tidak terbatas pada): rahasia perusahaan, tujuan strategis perusahaan, informasi sensitif perusahaan, rahasia dagang, spesifikasi, daftar pelanggan, dan data riset. Para karyawan diharapkan mengambil semua langkah yang diperlukan guna mencegah akses tanpa hak terhadap informasi tersebut.
2. Jagalah password dalam keadaan aman dan jangan berbagi penggunaan akun. Pengguna yang berhak bertanggung jawab terhadap keamanan password dan akun yang dimilikinya. Password pada tingkatan sistem

seharusnya diganti dalam kurun waktu 3 bulan, sedangkan password pada tingkatan pengguna seharusnya diganti dalam kurun waktu 6 bulan.

3. Semua PC, laptop dan workstation seharusnya diamankan dengan *screensaver* terlindungi password yang secara otomatis aktif dalam jangka waktu 5 menit atau kurang, atau dengan mekanisme logging-off ketika peralatan tersebut ditinggalkan oleh penggunanya.
4. Informasi yang terdapat pada komputer portable (laptop atau PDA) cenderung rentan, perhatian khusus menjadi mutlak diperlukan. Perlindungan terhadap laptop (sebagai contoh) seharusnya memnuhi ketentuan pada "Laptop Security Tips".
5. Semua host yang digunakan oleh karyawan yang terhubung dengan jaringan Internet/Intranet/Extranet PT. NCS, apakah dimiliki secara pribadi oleh karyawan maupun perusahaan, akan secara berkelanjutan diuji piranti lunak anti virus terpilih dengan database virus terkini kecuali jika dikendalikan oleh kebijakan kelompok atau departemen.
6. Para karyawan harus dengan sangat hati-hati ketika membuka lampiran e-mail yang dikirimkan dari pengirim tak dikenal, yang mungkin mengandung virus, bom email, atau kode Trojan horse.

4.3. Penggunaan yang tidak Diperbolehkan (*Unacceptable Use*)

Sejumlah aktivitas berikut, secara umum dilarang. Para karyawan dapat dibebaskan dari pembatasan-pembatasan ini selama dalam sejumlah hal masih dalam cakupan tanggung jawab pekerjaannya yang sah (misalnya, staff sistem

administrasi mungkin memiliki kebutuhan untuk menonaktifkan akses jaringan dari suatu host jika host tersebut mengganggu layanan produksi). Tanpa kriteria tersebut maka sejumlah hal / aktivitas yang disebutkan berikut menjadi hal ilegal untuk dilakukan.

Daftar dibawah ini merupakan rangkaian aktivitas yang masuk kedalam kategori penggunaan sistem / infrastruktur TI yang dilarang.

Aktivitas-aktivitas Sistem dan Jaringan

Aktivitas-aktivitas berikut secara tegas dilarang, dengan tanpa perkecualian:

1. Pelanggaran terhadap hak individu atau perusahaan yang dilindungi oleh hak cipta, rahasia dagang, hak paten atau kekayaan intelektual lainnya, atau aturan serta hukum-hukum sejenis yang meliputi (namun tidak terbatas pada) instalasi atau distribusi produk piranti lunak bajakan maupun piranti lunak lainnya yang tidak layak secarfa lisensi untuk digunakan pada PT. NCS.
2. Penyalinan tanpa hak terhadap material yang dilindungi oleh hak cipta, digitalisasi dan distribusi gambar dari majalah, buku-buku atau sumber-sumber lain yang juga dilindungi oleh hak cipta, musik, dan instalasi terhadap semua jenis piranti lunak berhak cipta untuk PT. NCS ataupun pengguna akhir tanpa memiliki lisensi yang aktif secara tegas dilarang.
3. Penyebaran program-program berbahaya kedalam jaringan atau server (seperti *virus*, *worm*, *trojan horse*, bom email dan lain-lain).

4. Pengungkapan *password* akun Anda kepada pihak lain atau mengizinkan penggunaan akun Anda oleh pihak lain.
5. Menggunakan aset komputasi PT. NCS untuk secara aktif memperoleh atau mengirimkan materi yang melanggar hukum maupun norma-norma yang berlaku.
6. Membuat pemberian produk atau jasa secara curang dari semua yang berasal dari akun PT. NCS.
7. Membuat pernyataan tentang garansi, baik secara langsung maupun tidak, kecuali jika memang merupakan bagian kewajiban pekerjaan.
8. Mengganggu komunikasi jaringan atau mengancam keamanan jaringan. Keamanan jaringan meliputi, (namun tidak terbatas pada), akses terhadap data dimana karyawan atau individu yang bersangkutan bukan merupakan penerima yang seharusnya atau masuk kedalam (*login*) server atau akun dimna individu tersebut secara eksplisit tidak memiliki hak akses yang sah, kecuali jika tugas-tugas tersebut berada didalam cakupan tugas-tugas kesehariannya (*regular*). Dalam hal ini, kata "mengganggu" sebagaimana disebutkan diawal meliputi (namun tidak terbatas pada) *network sniffing, pinged floods, packet spoofing, denial of service, forged routing information* untuk maksud jahat dan lain sebagainya.
9. Permindaian port atau pemindaian keamanan secara tegas dilarang kecuali dengan menyertakan persetujuan kepada departemen IT dan departemen terkait lainnya dari PT NCS.

10. Menjalankan pemantauan jaringan yang akan melakukan *intercept* terhadap data, kecuali aktivitas tersebut merupakan bagian dari pekerjaan harian dari karyawan ataupun individu yang bersangkutan.
11. Menghindari proses otentikasi atau keamanan akun jaringan maupun host.
12. Melakukan usaha / tindakan yang dapat menyebabkan suatu layanan tidak dapat diakses oleh pengguna pada sistem / jaringan PT. NCS (misalnya, serangan denial of service)
13. Menggunakan program/skrip/perintah, atau mengirimkan pesan dalam bentuk apapun, dengan maksud untuk mengganggu, atau disable sesi pada terminal pengguna, dengan cara apapun secara lokal maupun melewati Internet/Intranet/Extranet.
14. Memberikan informasi tentang atau daftar karyawan PT. NCS kepada pihak luar dari PT. NCS.

Aktivitas Komunikasi dan Email

1. Mengirimkan pesam email yang tidak diminta, meliputi pengiriman spam atau materi iklan lainnya kepada individu-individu yang tidak secara spesifik me-request materi tersebut.
2. Segala bentuk gangguan via email, telepon, pager apakah melalui bahasa, frekuensi, atau ukuran dari pesan tersebut.
3. Penggunaan tanpa hak atau pemalsuan terhadap informasi *header* email.
4. Membuat dan meneruskan "*chain letters*", "Ponzi" atau skema piramid lainnya dalam berbagai bentuk.

5. Menggunakan atau mengirimkan email yang tidak diminta (spam) dari dalam jaringan PT. NCS.
6. Mengirimkan pesan yang tidak berhubungan dengan bisnis (dari PT. NCS) dalam jumlah besar kepada *newsgroup* (*newsgroup spam*)

4.4. Blogging

1. Blogging oleh karyawan, apakah menggunakan properti dari PT. NCS (baik sistem atau PC), juga diatur dengan dalam kebijakan ini.
2. Kebijakan kerahasiaan informasi yang dimiliki PT. NCS juga berlaku terhadap aktivitas blogging. Sebagai contoh, para karyawan dilarang untuk mengungkapkan atau menyebarkan segala bentuk informasi rahasia atau yang dimiliki oleh PT. NCS, rahasia dagang atau berbagai materi lain yang dicakup dalam kebijakan kerahasiaan informasi dari PT NCS ketika sedang berada dalam suatu aktivitas blogging.
3. Para karyawan tidak diperbolehkan melakukan aktivitas blogging yang dapat membahayakan atau menodai wibawa (*image*), reputasi dari PT NCS dan/atau para karyawannya. Para karyawan dilarang untuk membuat komentar yang bersifat diskriminasi, penghinaan, fitnah atau pernyataam mengganggu lainnya ketika melakukan aktivitas blogging.
4. Para karyawan juga tidak boleh menyatakan pernyataan pribadi, opini atau keyakinan dengan mengatasnamakan PT. NCS ketika tengah melakukan aktivitas blogging. Jika seorang karyawan bermaksud menunjukkan opini atau pernyataan pribadinya pada *blog*, maka yang bersangkutan tidak

boleh menampilkan dirinya (baik secara eksplisit maupun implisit) sebagai perwakilan atau representatif dari PT. NCS. Setiap karyawan dianggap telah mengetahui segala kemungkinan dan resiko yang diakibatkan oleh aktivitas blogging.

5. Terlepas dari semua hukum terkait yang mengatur hak cipta, merk dagang PT. NCS, logo dan properti intelektual lainnya dari PT. NCS juga berlaku pada aktivitas *blogging*.

5.0 Sanksi dan Ancaman

Semua karyawan yang ditemukan melanggar kebijakan ini dapat diberikan tindakan disipliner, hingga meliputi pemutusan hubungan kerja.

6.0 Definisi

Istilah	**Definisi**
Blogging	Aktivitas menulis dalam suatu media blog. Blog (kependekan dari weblog) merupakan jurnal online pribadi yang secara berkala di-update dan dimaksudkan untuk konsumsi publik.
Spam	Pengiriman email yang tidak diminta (bahkan terkadang mengganggu) kepada sejumlah besar penerima.

Policy Document Name	*Automatically Forwarded Email Policy*
Owner	PT. NCS
Prepared By	Junian Dani
Approved By	IT Manager of PT. NCS
Revision	1.0 - Initial Release

1.0 Tujuan

Untuk menghindari penyingkapan atau penyebaran informasi sensitif perusahaan secara tidak sah atau kurang berhati-hati.

2.0 Cakupan

Kebijakan ini mencakup email terusan secara otomatis yang ditujukan kepada semua karyawan, vendor dan agen yang beroperasi atas nama PT. NCS.

3.0 Kebijakan

Para karyawan harus sepenuhnya berhati-hati ketika mengirimkan segala email dari dalam PT. NCS menuju jaringan luar. Tanpa persetujuan dari manager dari Department TI, email dari PT. NCS tidak akan secara otomatis diteruskan kepada pihak luar. Informasi sensitif, sebagaimana didefinisikan pada kebijakan, tidak boleh diteruskan dengan media apapun, kecuali jika email tersebut bersifat kritis terhadap bisnis dan dienkripsi sesuai dengan Kebijakan Enkripsi / *Acceptable Encryption Use* (pada bagian sebelumnya).

4.0 Sanksi dan Ancaman

Semua karyawan yang ditemukan melanggar kebijakan ini dapat diberikan tindakan disipliner hingga pemutusan hubungan kerja.

5.0 Definisi

Istilah	**Definisi**
Email	Pengiriman informasi secara elektronik melalui protokol mail seperti SMTP.
Email Terusan (*Fowarded Email*)	Email yang dikirimkan kembali dari jaringan internal menuju pihak luar.
Informasi Sensitif	Informasi dianggap sebagai sensitif jika informasi tersebut dapat membahayakan reputasi dari PT. NCS jika tersebar atau terkuak secara tanpa hah / sah kepada pihak-pihak diluar organisasi atau perusahaan.
Unauthorized Disclosure	Memberikan atau menyebarkan informasi yang terbatas atau rahasia baik disengaja maupun sebaliknya kepada pihak-pihak yang tidak perlu mengetahui informasi tersebut.

Policy Document Name	*Email Use Policy*
Owner	PT. NCS
Prepared By	Junian Dani
Approved By	IT Manager of PT. NCS
Revision	1.0 - Initial Release

1.0 Tujuan

Dokumen kebijakan ini bertujuan untuk menghindari hal-hal yang dapat mengganggu atau merusak *image* / wibawa PT. NCD ketika email dikirimkan keluar dari PT. NCS menuju masyarakat umum (yang akan dilihat sebagai pernyataan resmi dari PT. NCS).

2.0 Cakupan

Kebijakan ini melingkupi penggunaan email yang dikirimkan dari alamat email PT. NCS. Kebijakan ini berlaku kepada semua karyawan,vendor, dan para agen yang beroperasi dibawah PT.NCS

3.0 Kebijakan

3.1 Penggunaan yang Dilarang

Sistem email PT. NCS seharusnya tidak digunakan untuk membuat arau mendistribusikan pesan-pesan bernada ofensif, termasuk komentar berbau rasial, gender, cacat fisik, warna rambut, umur, orientasi seksual, pronografi, kepercayaan agama, atau hal-hal berbau politik. Para karyawan yang menerima pesan email dengan isi sebagaimana dimaksud sebelumnya baik dari para

karyawan PT. NCS maupun pihak luar perusahaan sebaiknya segera melaporkan masalah ini kepada supervisor atau manager .

3.2 Penggunaan Pribadi

Penggunaan sumber daya (dalam hal ini sistem atau jaringan) PT. NCS untuk email pribadi dalam jumlah yang pantas dapat diperbolehkan, namun email yang tidak berhubungan dengan urusan perusahaan / kantor tersebut sebaiknya disimpan secara terpisah dari email yang berkaitan dengan urusan perusahaan / kantor.

3.3 *Monitoring*

Para karyawan PT. NCS tidak dapat mengharapkan privasi terhadap data / informasi yang mereka simpan, kirimkan atau terima melalui sistem email perusahaan. PT. NCS dapat sewaktu-waktu memantau pesan-pesan email tanpa pemberitahuan terlebih dahulu.

4.0 Sanksi dan Ancaman

Setiap karyawan yang ditemukan melanggar kebijakan ini dapat dikenakan tindakan disipliner hingga pemutusan hubungan kerja.

5.0 Definitions

Term	**Definition**
Email	Pengiriman informasi secara elektronis melalui protokol

	mail seperti SMTP atau IMAP.
Forwarded email	Email yang dikirimkan ulang dari suatu jaringan internal kepada pengguna yang lain atau pihak luar.
Surat atau email berantai (*Chain email or letter*)	Pesan email yang yang dikirimkan berturut-turut kepada sejumlah orang atau pengguna email. Pesan email jenis ini umumnya memberikan arahan kepada penerimanya untuk meneruskan pesan email tersebut kepada sejumlah penerima lainnya dengan iming-iming keberuntungan atau uang jika arahan tersebut diikuti.
Informasi Sensitif	Suatu informasi dianggap sensitif jika informasi tersebut dapat mengganggu reputasi suatu organisasi atau perusahaan (dalam hal ini PT. NCS) jika disebarkan kepada pihak luar tanpa persetujuan dari organisasi atau perusahaan yang bersangkutan.
Unauthorized Disclosure	Memberikan atau menyebarkan informasi yang terbatas atau rahasia baik disengaja maupun sebaliknya kepada pihak-pihak yang tidak perlu mengetahui informasi tersebut.

Policy Document Name	*Information Sensitivity Policy*
Owner	PT. NCS
Prepared By	Junian Dani
Approved By	IT Manager of PT. NCS
Revision	1.0 - Initial Release

1.0 Tujuan

Kebijakan ini dimaksudkan untuk membantu para karyawan dalam menentukan informasi apa saja yang dapat disampaikan kepada pihak-pihak diluar perusahaan, maupun sebaliknya tanpa persetujuan khusus dari PT. NCS

Informasi yang dicakupi dalam pedoman ini meliputi informasi yang disimpan atau dibagi melalui cara / peralatan apapun. Hal ini meliputi: informasi elektronis, informasi diatas kertas, dan informasi yang disampaikan atau dibagi secara lisan atau visual (seperti telepon atau *video conference*).

Semua karyawan diharapkan memahami klasifikasi informasi dan panduan penanganannya. (Sebagai contoh, informasi rahasia atau sensitif dari PT. NCS tidak boleh dibiarkan tertinggal pada ruang meeting atau ruang yang terbuka untuk pihak luar).

Setiap bentuk pertanyaan berkaitan dengan klasifikasi terhadap suatu bagian spesifik dari informasi harap dialamatkan menuju Manager Departement IT PT . NCS

2.0 Cakupan

Semua informasi yang terdapat pada PT. NCS dikategorikan kedalam 2 klasifikasi utama:

- Informasi Publik PT. NCS
- Informasi Rahasia atau Sensitif PT. NCS

Informasi publik yang dimaksud disini adalah informasi yang telah dinyatakan sebagai pengetahuan umum oleh masyarakat dan dapat secara bebas diberikan kepada siapapun tanpa mengganggu reputasi atau wibawa dari PT. NCS.

Sedangkan informasi rahasia atau sensitif merupakan ketegori informasi yang berisi semua jenis informasi lainnya yang tidak tergolong kedalam informasi publik (sebagaimana dijelaskan sebelumnya) dan oleh karenanya harus dilindungi agar tetap aman. Informasi yang termasuk dalam kategori ini seperti rahasia dagang, pengembangan program aplikasi, informasi harga serta *customer* dan lain sebagainya. Informasi rahasia atau sensitif yang dimakud disini juga meliputi informasi lainnya yang tidak terlalu kritis seperti direktori telepon internal perusahaan, informasi data karyawan, dan lain-lain yang tidak membutuhkan tingkatan perlindungan yang tinggi.

Para karyawan PT. NCS dianjurkan untuk turut mengamanankan suatu informasi yang tergolong dalam kategori informasi rahasia atau sensitif. Jika seorang karyawan mengalami kesulitan dalam menentukan klasifikasi suatu informasi

(atau bagian spesifik dalam informasi tersebut) berikut penanganan yang perlu diambil, maka yang bersangkutan diharapkan menghubungi manager atau supervisornya.

3.0 Kebijakan

Pedoman berikut memberikan rincian tentang bagaimana melindungi informasi pada sejumlah tingkatan / klasifikasi pada PT. NCS.

3.1 **Tingkatan Kerahasiaan yang Rendah:** meliputi informasi umum perusahaan; sejumlah informasi teknis serta personil (baik dalam bentuk tercetak atau *form* elektronis).

Hak Akses diberikan kepada: karyawan PT. NCS, kontraktor, orang-rang atau pihak-pihak tertentu yang memiliki kebutuhan bisnis untuk mengetahuinya.

Proses Distribusi didalam PT. NCS: Surat standard perusahaan, metode pengiriman file secara elektronik atau email yang diakui.

Proses Distribusi diluar PT. NCS: Surat standard perusahaan, metode pengiriman file secara elektronik atau email yang diakui.

Proses Distribusi secara elektronik: Tidak ada pembatasan yang diberlakukan kecuali pesan atau informasi tersebut dikirimkan kepada penerima yang berhak.

Media Penyimpanan: Jagalah dari jangkauan orang-orang yang tidak berhak; hapus dari papan tulis; jangan dibiarkan tertinggal diatas meja; serta dilindungi dari ancaman kehilangan atau kerusakan. Informasi berbasis elektronis yang masuk dalam kategori ini sebaiknya memiliki kontrol akses secara individu jika memungkinkan.

Metode Penghapusan Data: informasi berbasis kertas yang masuk dalam kategori ini yang telah *out-of-date* atau tidak lagi terpakai harus dibuang atau dimasukkan kedalam kerangjang sampah yang disediakan oleh PT. NCS. Sedangkan informasi atau data yang tersimpan secara elektronik sebaiknya dihapus dengan metode penghapusan standard.

Penalti terhadap penyebaran informasi secara disengaja: Peringatan hingga tindakan disipliner lainnya serta tuntutan proses hukum yang berlaku.

3.2 **Tingkatan Kerahasiaan yang Sedang:** meliputi informasi bisnie, finansial, teknis dan informasi sebagian besar personil PT. NCS (baik dalam bentuk tercetak atau *form* elektronis).

Hak Akses diberikan kepada: karyawan PT. NCS, kontraktor, orang-rang atau pihak-pihak tertentu yang memiliki kebutuhan bisnis untuk mengetahuinya dengan proses penandatanganan dokumen NDA (*Non Disclosure Agreement*).

Proses Distribusi didalam PT. NCS: Surat standard perusahaan, metode pengiriman file secara elektronik atau email yang diakui.

Proses Distribusi diluar PT. NCS: Surat standard perusahaan, metode pengiriman file secara elektronik atau email yang diakui.

Proses Distribusi secara elektronik: Tidak ada pembatasan yang diberlakukan kecuali pesan atau informasi tersebut dikirimkan kepada penerima yang berhak namun harus dienkripsi (atau dikirimkan melalui suatu jalur privat (*private link*) terhadap penerima yang berada diluar PT. NCS.

Media Penyimpaan: Kontrol akses secara individu sangat direkomendasikan untuk informasi elektronik.

Metode Penghapusan Data: informasi berbasis kertas yang masuk dalam kategori ini yang telah *out-of-date* atau tidak lagi terpakai harus dibuang atau dimasukkan kedalam mesin *shreder* yang disediakan oleh PT. NCS. Sedangkan informasi atau data yang tersimpan secara elektronik sebaiknya dihapus dengan metode penghapusan standard .

Penalti terhadap penyebaran informasi secara disengaja: Peringatan hingga tindakan disipliner lainnya serta tuntutan proses hukum yang berlaku.

3.3 **Tingkatan Kerahasiaan yang Tinggi:** meliputi rahasia dagang dan marketing, operasional, data personel atau karyawan secara rinci, data finansial, kode sumber (*source code*) aplikasi dan informasi teknis

serta informasi lainnya yang turut mempengaruhi reputasi dan wibawa perusahaan (baik dalam bentuk tercetak atau *form* elektronis).

Hak Akses diberikan kepada: karyawan maupun non-karyawan dari PT. NCS yang ditunjuk untuk mengangani informasi yang dimaksud dan menandatangani dokumen NDA (*Non Disclosure Agreement*).

Proses Distribusi didalam PT. NCS: Dikirimkan secara langsung dan diberi label rahasia atau melalui metode pengiriman file secara elektronik atau email yang diakui.

Proses Distribusi diluar PT. NCS: Dikirimkan secara langsung dan disertakan tanda tangan pengirim.

Proses Distribusi secara elektronik: Tidak ada pembatasan yang diberlakukan kecuali pesan atau informasi tersebut dikirimkan kepada penerima yang berhak namun harus dienkripsi dengan kuat (misalnya melalui PKI) terhadap penerima.

Media Penyimpaan: Kontrol akses secara individu sangat direkomendasikan untuk informasi elektronik. Pengamanan secara fisik terhadap informasi yang disimpan menjadi hal yang mutlak untuk dilakukan.

Metode Penghapusan Data: informasi berbasis kertas yang masuk dalam kategori ini yang telah *out-of-date* atau tidak lagi terpakai harus dibuang atau dimasukkan kedalam mesin *shreder* yang disediakan oleh PT. NCS. Sedangkan informasi atau data yang tersimpan secara elektronik sebaiknya

dihapus dengan metode penghapusan data yang tidak dapat dengan mudah dikembalikan.

Penalti terhadap penyebaran informasi secara disengaja: Tindakan disipliner hingga pemutusan hubungan kerja serta tuntutan proses hukum yang berlaku.

4.0 Sanksi dan Ancaman

Setiap karyawan yang ditemukan melanggar kebijakan ini dapat dikenakan tindakan disipliner hingga pemutusan hubungan kerja.

Policy Document Name	*Password Policy*
Owner	PT. NCS
Prepared By	Junian Dani
Approved By	IT Manager of PT. NCS
Revision	1.0 - Initial Release

1.0 Rangkuman

Password merupakan aspek penting dalam keamanan komputer. Mekanisme ini merupakan perlindungan terdepan terhadap akun pengguna. Pemilihan password yang buruk dapat menyebabkan ancaman keamanan terhadap jaringan perusahaan PT. NCS secara keseluruhan. Oleh karena itu, semua karyawan PT. NCS (termasuk kontraktor dan vandor yang memiliki akses terhadap sistem/jaringan PT. NCS) bertanggung jawab terhadap pengambilan langkah yang diperlukan dalam memilih dan mengamankan password mereka.

2.0 Tujuan

Tujuan dari kebijakan ini adalah untuk membangun standard dalam pembuatan password, perlindungan terhadap password tersebut, dan frekuensi pergantiannya.

3.0 Cakupan

Cakupan dari kebijakan ini meliputi semua personel yang memiliki atau bertanggung jawab terhadap suatu akun (atau akses dalam bentuk apapun yang mendukung atau membutuhkan password) pada sistem manapun yang berada pada fasilitas PT. NCS, memiliki akses terhadap jaringan PT. NCS, atau menyimpan informasi apapun yang bersifat non publik milik PT. NCS.

4.0 Kebijakan

4.1 Umum

- Semua password pada level sistem (seperti root, admin NT/Windows, akun administrasi aplikasi, dan lain-lain) harus diganti setidaknya dalam periode 60 hari.
- Semua password pada level pengguna (seperti email, web, komputer desktop / PC, dan lain-lain) harus diganti setidaknya setiap 75 hari.
- Akun pengguna yang diberikan hak keistimewaan pada level sistem dilakukan melalui keanggotaan group tertentu pada sistem atau melalui bantuan program seperti "sudo" harus memiliki password yang unik.
- Password tidak boleh dimasukkan dalam pesan email atau bentuk lain dari komunikasi elektronis.
- Ketika SNMP digunakan, *community string* yang digunakan harus didefinisikan berbeda dengan standard default seperti "public", "private" dan "system" dan harus berbeda dari password yang digunakan untuk log in secara interaktif.
- Semua password pada level pengguna dan sistem harus menyesuaikan dengan garis pedoman yang dideskripsikan dibawah.

4.2 Garis Pedoman

A. Pedoman Pembentukan Password Umum

Password umum yang dimaksud disini adalah password yang digunakan untuk beragam tujuan pada PT. NCS yang meliputi akun pada level pengguna, akun web, akun email, perlindungan melalui screen saver, password terhadap voicemail, dan login pada router lokal.

Password yang lemah memiliki karakteristik berikut:

- Password mengandung kurang dari 15 karakter
- Password merupakan suatu kata atau gabungan kata yang terdapat pada kamus (baik Bahasa Inggris maupun Bahasa Indonesia)
- Password yang digunakan merupakan kata yang umum digunakan seperti:
    - Nama keluarga, hewan peliharaan, teman, rekan kerja, karakter-karakter fantasi, dan lain-lain.
    - Nama komputer, perintah, situs, perusahaan, hardware, software.
    - Tanggal kelahiran atau hari ulang tahun dan informasi personal lainnya seperti alamat dan nomor telepon.
    - Kata atau angka yang memiliki pola seperti aaabbb, qwerty, zyxwvuts, 123321, dan lain-lain.
    - Semua bentuk kata yang dieja terbalik.

Password yang kuat memiliki karakteristik berikut:

- Mengandung baik karakter huruf besar dan huruf kecil.

- Memiliki digit dan karakter tanda baca layaknya surat. Misalnya, 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Terdiri dari setidaknya 15 karakter alphanumeris dan merupakan suatu passphrase.
- Bukan merupakan kata dalam bahasa apapun, logat, dialek, jargon, dan lain-lain.
- Tidak berdasarkan atas informasi personal, nama keluarga, dan lain-lain.
- Password sebaiknya tidak pernah ditulis atau disimpan secara online.

B. Standard Perlindungan Password

Jangan menggunakan password akun PT. NCS untuk akses non PT NCS (seperti akun ISP personal, web mail personal, dan lain-lain). Ketika memungkinkan, jangan menggunakan password yang sama untuk beragam kebutuhan akses PT. NCS. Sebagai contoh, gunakan password berbeda/terpisah terhadap akun NT/Windows dan akun UNIX.

Jangan membagi password PT. NCS dengan siapapun, termasuk asisten administratif atau sekretaris. Semua password diperlakukan sebagai informasi sensitif/*confidential* dari PT. NCS.

Berikut ini merupakan daftar yang tidak boleh dilakukan berkaitan dengan penggunaan password:

- Dilarang menyampaikan password melalui telepon kepada siapapun
- Dilarang menyampaikan password dalam pesan email

- Dilarang menyampaikan password kepada atasan / boss / manager
- Dilarang berbicara tentang password didepan orang lain
- Dilarang memberikan petunjuk (*hint*) berkenaan dengan format password yang digunakan (Misalnya, "Nama keluarga saya")
- Dilarang menyampaikan password dalam quesioner atau bentuk form lainnya
- Dilarang berbagi password dengan anggota keluarga
- Dilarang mengungkapkan password kepada rekan kerja ketika sedang berlibur

Jika seseorang membutuhkan suatu password, arahkan menuju dokumen ini atau menghubungi departemen IT dari PT. NCS.

Jika memungkinkan, sebaiknya tidak menggunakan fitur "Remember Password" pada aplikasi-aplikasi yang digunakan (misalnya, Eudora, Outlook Express, Yahoo Messanger, dan lain-lain).

Mengulang pernyataan sebelumnya, dilarang menuliskan password dan menyimpannya dimanapun. Disamping itu, setiap entitas terkait dari PT. NCS dilarang menyimpan password pada suatu file pada sistem komputer manapun (termasuk perangkat portabel seperti PDA, dan lain sebagainya) tanpa menggunakan enkripsi.

Jika suatu akun atau password diduga telah dikompromi atau dikuasai oleh secara tanpa hak atau tidak sah pihak lainyang tidak bertanggung jawab, segera laporkan insiden tersebut kepada Departemen IT dari PT. NCS dan lakukan pergantian semua password terhadap akun yang dimaksud.

C. Standard Pengembangan Aplikasi

Pengembang aplikasi harus memastikan program yang dibuat telah melakukan sejumlah tindakan pencegahan berikut guna meminimalisir ancaman keaman. Aplikasi:

- Sebaiknya mendukung otentikasi pengguna individu dan bukan group.
- Sebaiknya tidak menyimpan password yang format teks atau bentuk format lainnya yang dapat dengan mudah dikembalikan dalam format aslinya.
- Sebaiknya mendukung mekanisme otentikasi melalui TACACS+ , RADIUS dan / atau X.509 jika dianggap memungkinkan.

D. Penggunaan Password dan Passphrese untuk pengguna *Remote Access*

Akses menuju jaringan PT. NCS melalui remote access dikendalikan menggunakan otentikasi password sekali pakai (one-time) atau sistem kunci publik dan privat dengan pemakaian *passphrase* yang kuat.

E. *Passphrases*

Passphrase umumnya digunakan pada otentikasi asimetris. Sistem *Public Key Infrastructure* (PKI) sebagai contoh, merupakan relasi matematis diantara kunci publik yang diketahui oleh semua pihak dan dan kunci privat yang hanya diketahui oleh pengguna yang bersangkutan. Tanpa passphrase untuk membuka kunci privat, pengguna tidak dapat memperoleh akses.

Passphrase tidak serupa dengan password. Passphrase merupakan versi yang lebih panjang dari password sehingga membuatnya lebih aman untuk digunakan. Passphrase umumnya terdiri dari beberapa kata. Oleh karena itu, passphrase menjadi lebih aman terhadap "dictionary attacks."

Passphrase yang baik relatif panjang dan mengandung kombinasi huruf besar dan huruf kecil serta karakter numerik dan tanda baca. Salah satu contoh passphrase yang baik adalah sebagai berikut:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

Semua aturan diatas yang diterapkan pada password juga diterapkan pada passphrase.

5.0 Sanksi dan Ancaman

Setiap karyawan yang ditemukan melanggar kebijakan ini daoat dikenakan tindakan disipliner hingga pemutusan hubungan kerja.

Policy Document Name	*Router Security Policy*
Owner	PT. NCS
Prepared By	Junian Dani
Approved By	IT Manager of PT. NCS
Revision	1.0 - Initial Release

1.0 Tujuan

Dokumen ini menjelaskan tentang konfigurasi keamanan minimal yang dibutuhkan terhadap semua router dan switch yang terkoneksi menuju jaringan / sistem *production* atau digunakan dalam kapasitas *production* pada PT. NCS

2.0 Cakupan

Setiap router dan switch yang terkoneksi pada jaringan production PT. NCS terlingkupi melalui kebijakan ini. Sedangkan router dan switch yang berada pada jaringan internal PT. NCS tidak turut berdampak terhadap kebijakan ini. Disamping itu, router dan switch didalam area DMZ jatuh dibawah *Internet DMZ Equipment Policy*

3.0 Kebijakan

Setiap router harus memenuhi konfigurasi standard berikut:

1. Tidak ada akun pengguna yang dikonfigurasi pada router. Semua router harus menggunakan TACACS+ untuk semua proses otentikasi pengguna.
2. Fitur enable password yang terdapat pada router harus disimpan dalam format terenkripsi.
3. Lakukan pemblokiran sejumlah hal berikut pada router:
    a. *IP directed broadcasts*

b. Paket data yang masuk pada router dengan alamat yang tidak valid (sebagaimana didefinisikan dalam RFC1918)

c. TCP small services

d. UDP small services

e. Semua layanan web yang berjalan pada router

4. Penggunaan *community string* SNMP yang menjadi standard perusahaan.
5. Aturan tentang hak akses akan ditambahkan sesuai dengan tuntutan bisnis yang semakin berkembang.
6. Router harus dimasukkan dalam suatu sustem manajemen perusahaan (*enterprise management system*) dengan kapabilitas akses atau kontak pada titik tertentu.
7. Setiap router harus memiliki pernyataan berikut (yang disampaikan melalui *banner* pada router)

   "DILARANG MENGAKSES SECARAILEGAL ATAU TANPA HAK MENUJU PERALATAN JARINGAN INI. Anda harus memiliki izin yang tertuang secara eksplisit untuk mengakses atau mengkonfigurasi peralatan ini. Semua aktivitas yang dilakukan pada perlatan ini akan dicatat, dan pelanggaran terhadap kebijakan ini akan mengakibatkan jatuhnya tindakan disipliner, dan dapat dilaporkan kepada badan penegak hukum. Tidak terdapat hak privasi terhadap peralatan ini."

8. Telnet tidak boleh digunakan dalam jaringan untuk mengkonfigurasi router, kecuali jika terdapat *tunnel* khusus yang melindungi keseluruhan jalur komunikasi. SSH lebih dipilih sebagai protokol untuk manajemen.

4.0 Sanksi dan Ancaman

Setiap karyawan yang ditemukan melanggar kebijakan ini dapat dikenakan tindakan disipliner hingga pemutusan hubungan kerja.

5.0 Definisi

Istilah	**Definisi**
Jaringan *Production*	Jaringan *Production* atau jaringan produksi merupakan jaringan yang digunakan dalam bisnis atau aktivitas harian dalam PT. NCS.

Policy Document Name	*Server Security Policy*
Owner	PT. NCS
Prepared By	Junian Dani
Approved By	IT Manager of PT. NCS
Revision	1.0 - Initial Release

1.0 Tujuan

Tujuan dari kebijakan ini adalah untuk membangun standard konfigurasi dasar terhadap peralatan server internal yang dimiliki dan / atau dioperasikan oleh PT. NCS. Implementasi secara efektif terhadap kebijakan ini akan meminimalisir akses tanpa otorisasi atau illegal menuju teknologi dan informasi prorpitary yang dimiliki oleh PT. NCS

2.0 Cakupan

Kebijakan ini diterapkan kepada semua peralatan server yang dimiliki dan / atau dioperasikan oleh PT. NCS. Kebijakan ini secara spesifik ditujukan kepada peralatan server yang berada pada jaringan internal PT. NCS. Untuk standard konfigurasi peralatan pada jaringan external atau DMZ dapat merujuk pada

3.0 Kebijakan

3.1 Kepemilikan dan Tanggung Jawab

Semua server internal yang dikelola pada jaringan PT. NCS harus dimiliki oleh group operasional yang bertanggung jawab terhadap administrasi ssstem. Panduan konfigurasi server harus dibangun dan dipelihara oleh setiap group operasional, sesuai dengan kebutuhan bisnis dan disetujui oleh Departemen TI. Group

opersional harus memantau kepatuhan terhadap konfigurasi yang dimaksud. Setiap group operasional harus membangun proses untuk pergantian panduan konfirguasi, yang meliputi proses review dan persetujuan oleh Departemen TI.

- Semua server harus didaftarkan didalam *enterprise management system.* Dalam hal ini, sejumlah informasi minimal yang dibutuhkan adalah:
    - Lokasi server
    - Versi sistem operasi berikut hardware yang digunakan
    - Fungsi utamanya (jika dimungkinkan)
- Informasi pada *enterprise management system* harus berada pada kondisi yang *up-to-date*.
- Perubahan konfigurasi untuk server pada jaringan *production* harus mengikuti prosedur manajemen perubahan.

3.2 Pedoman Konfigurasi Umum

- Konfigurasi system operasi seharusnya sesuai dengan pedoman yang dikeluarkan oleh Departemen TI pada PT. NCS.
- Aplikasi atau layanan yang tidak digunakan harus dinonaktifkan.
- Akses terhadap layanan sebaiknya dicatat dan dilindungi melalui metode kontrol akses seperti *TCP Wrappers*, jika memungkinkan.
- Update keamanan terkini harus diinstall pada system sesegera mungkin. Satu-satunya pengecualian untuk tidak melakukan proses update ini adalah ketika proses yang dimaksud mengganggu kebutuhan atau proses atau bisnis yang tengah berjalan.

- Selalu gunakan prinsip standard keamanan: hak akses minimal yang dibutuhkan ketika menjalankan suatu fungsi atau tugas.
- Dilarang menggunakan akun *root* jika akun tanpa hak keistimewaan khusus mampu melakukan tugas yang dimaksud.
- Jika metodologi untuk mengamankan suatu koneksi tersedia, maka akses harus diamankan melalui metodologi tersebut (misalnya, koneksi jaringan terenkripsi menggunakan SSH atau IPSec).
- Semua server secara fisik harus terletak pada suatu lingkungan yang memiliki mekanisme control akses
- Semua server secara spesifik dilarang beroperasi pada area / ruangan yang tidak dapat dikontrol.

3.3 *Monitoring*

- Semua event yang berkaitan dengan keamanan pada system sensitive atau kritis haru dicatat dan diaudit sebagaimana diuraikan dibawah:
    - Semua *log* (catatan) yang berhubungan dengan keamanan akan disimpan secara online minimal selama 1 minggu.
    - Backup tape harian secara incremental akan disimpan minimal selama 1 bulan.
    - Backup tape backup mingguan secara penuh yang berkenaan dengan *log* akan dipertahankan selama minimal 1 bulan.
    - Backup penuh bulanan akan disimpan atau dipertahankan minimal selama 2 tahun.

- Kejadian yang berkenaan dengan keamanan akan dilaporkan kepada Departemen TI, yang kemudian akan me-review log yang dimaksud. Tindakan korektif akan dilakukan jika dibutuhkan. Kejadian atau event yang berkenaan dengan keamanan yang dimaksud disini meliputi (namn tidak terbatas pada):
    - Serangan-serangan pemindaian port
    - Bukti akses secara ilegal atau tanpa otorisasi sebagaimanan mestinya terhadap akun-akun khusus tertentu
    - Kejadian ganjil lainnya yang terjadi pada system / jaringan PT. NCS.

3.4 *Compliance*

- Audit akan dilaksanakan secara regular dengan organisasi atau departemen berwenang baik didalam maupun diluar PT. NCS.
- Audit akan diatur oleh group audit internal. Group ini akan memilah temuan (*finding*) yang ada serta melaporkan temuan tersebut kepada staff pendukung untuk untuk proses perbaikan atau justifikasi.
- Setiap usaha akan dilakukan gunak menghindarkan proses audit dari kegagalan operasional atau kerusakan.

4.0 Sanksi dan Ancaman

Setiap karyawan yang ditemukan melanggar kebijakan ini dapat dikenakan tindakan disipliner hingga pemutusan hubungan kerja.

5.0 Definisi

Istilah	**Definisi**
DMZ	*De-militariezed Zone*. Suatu segemen jaringan external menuju jaringan production perusahaan.
Server	Dalam konteksi kebijakan ini, server didefinisikan sebagai server yang terletak pada jaringan internal PT. NCS. Desktop serta peralatan lainnya tidak termasuk dalam cakupan kebijkan ini.

Policy Document Name	*Internet DMZ Equipment Policy*
Owner	PT. NCS
Prepared By	Junian Dani
Approved By	IT Manager of PT. NCS
Revision	1.0 - Initial Release

1.0 Tujuan

Tujuan dari kebijakan ini adalah untuk mendefinisikan standard yang harus dipenuhi oleh semua peralatan yang dimiliki dan / atau dioperasikan oleh PT. NCS yang berlokasi diluar *firewall / router* internet perusahaan. Standard ini dirancang untuk meminimalkan kemungkinan bocor atau hilangnya data sensitif atau rahasia, hak cipta dan lain sebagainya yang dimiliki oleh PT. NCS.

Peralatan yang berada diluar *firewall / router* internal PT. NCS dianggap sebagai bagian dari "*de-militarized zone*" (DMZ) merupakan entitas yang tercakup melalui kebijakan ini.

Kebijakan ini mendefinsikan sejumlah standard berikut:

The policy defines the following standards:

- Tanggung Jawab terhadap Kepemilikan
- *Requirement* terhadap konfigurasi yang aman
- Requirement terhadap kegiatan operasional
- *Requirement* terhadap control perubahan

2.0 Cakupan

Semua peralatan yang dikelola dalam area DMZ yang dimiliki dan / atau dioperasikan oleh PT. NCS (meliputi host, router, switch, dan lain-lain) harus mengikuti kebijakan ini

Semua peralatan baru yang berada dibawah kebijakan ini hari dikonfigurasi berdasarkan dokumen konfigurasi yang direferensikan, kecuali jika diberikan eksepsi dari Departemen TI PT. NCS dengan alas an tertentu. Semua peralatan (baik saat ini maupun dimasa depan) yang dikelola ada infrastruktur jaringan publik harus tunduk kepada kebijakan ini.

3.0 Kebijakan

3.1. Kepemilikan dan Tenggung Jawab

Peralatan dan aplikasi didalam cakupan kebijakan ini harus dikelola oleh group pendukung yang disetujui oleh Departemen TI (terhadap system DMZ, aplikasi atau manajemen jaringan).

Group pendukung tersebut akan bertanggung jawab sebagai berikut:

- Setiap perangkat harus didokumentasikan pada suatu dokumen maupun format tertentu yang berisi:
    - Lokasi dari suatu Host

- Versi Sistem operasi dan Hardware.
- Fungsi utama dan aplikasi-aplikasi yang ada didalamnya.

- Akses terhadap *log* yang terdapat pada peralatan dan system harus diberikan kepada karyawan pada Departemen TI jika dibutuhkan.
- Pergantian terhadap peralatan yang ada serta instalasi peralatan baru harus mengikuti prosedur atau proses manajemen perubahan yang berlaku di PT. NCS.

3.2. Kebijakan Konfigurasi Umum

Semua peralatan (yang berada pada area DMZ) harus memenuhi kebijakan konfigurasi berikut:

- *Hardware*, system operasi, layanan dan aplikasi harus terlebih dahulu disetujui oleh Departemen TI sebelum dilakukan proses pemasangan atau konfigurasi.
- Konfigurasi system operasi harus sesuai dengan standard instalasi dan konfigurasi host dan router.
- Semua *update* keamanan yang direkomendasikan (baik oleh Departemen TI maupun vendor) harus diinstall. Hal ini tidak saja berlaku untuk semua layanan yang telah diinstall namun juga terhadap semua layanan-layanan yang (baik secara temporer maupun permanen) dinonaktifkan. Individu atau group yang ditunjuk untuk mengelola layanan tersebut harus secara memastikan bahwa setiap *update* keamanan telah terinstall.

- Aplikasi dan layanan yang tidak melayani kebutuhan bisnis harus dinonaktifkan.
- Aplikasi dan layanan yang tidak digunakan untuk akses oleh publik atau masyarakat umum harus dibatasi melalui mekanisme ACL (*Access Control List*).
- Setiap layanan atau protokol yang dinyatakan tidak aman (berdasarkan ketentuan yang dibuat oleh Departemen TI dari PT NCS) harus digantikan dengan layanan atau protocol serupa yang lebih aman jika memang tersedia.
- Proses administrasi secara *remote* harus dilakukan melalui jalur yang aman (misalnya menggunakan koneksi terenkripsi dari SSH atau IPSec). Ketika metodologi koneksi jalur aman tidak tersedia, maka mekanisme *one-time password* (seperti DES/SofToken) harus digunakan untuk semua level akses.
- Semua isi yang terdapat pada host harus di-update diatas suatu saluran atau jalur yang aman
- Semua kejadian / event yang berkenaan dengan keamanan harus dicatat dan diaudit secara berkala oleh entitas berwenang yang ditunjuk. Hal tersebut meliputi:
    - Proses *login* yang gagal dilakukan oleh pengguna.
    - Kegagalan dalam memperoleh akses khusus
    - Pelanggaran terhadap kebijakan hak akses.

3.3. Prosedur Manajemen Perubahan dan Instalasi Baru

Semua instalasi baru dan perubahan terhadap konfigurasi pada peralatan dan aplikasi yang telah ada harus mengikuti prosedur atau kebijakan berikut:

- Perubahan konfigurasi juga harus mengikuti prosedur manajemen perbahan yang berlaku di PT. NCS.
- Departemen TI harus dilibatkan dalam pembuatan atau perancangan system / aplikasi sebelum proses *deployment* atau instalasinya dilakukan
- Departemen TI harus dilibatkan baik secara langsung maupun melalui prosedur manajemen perubahan yang telah berlaku dalam menyetujui semua bentuk perubahan konfigurasi ataupun proses *deployment*.

4.0 Sanksi dan Ancaman

Setiap karyawan yang ditemukan melanggar kebijakan ini dapat dikenakan tindakan disipliner hingga pemutusan hubungan kerja. Sedangkan penyedia layanan yang ditemukan melanggar kebijakan ini dapat dikenakan penalti secara finansial hingga pemutusan ikatan kontrak.

Policy Document Name	*Wireless Communication Policy*
Owner	PT. NCS
Prepared By	Junian Dani
Approved By	IT Manager of PT. NCS
Revision	1.0 - Initial Release

1.0 Rangkuman

Tujuan kebijakan ini adalah untuk mengamankan dan melindungi aset informasi yang dimiliki oleh PT. NCS. OT. NCS menyediakan peralatan komputer, jaringan, dan sistem informasi elektronis lainnya dalam memenuhi misi dan objektif dari perusahaan. PT. NCS memberikan akses menuju sumber daya tersebut sebagai suatu hak keistimewaan yang harus digunakan secara bertanggung jawab guna menjaga kerahasiaan, integritas, dan ketersediaan terhadap semua aset informasi.

Kebijakan ini menetapkan kondisi peralatan / infrastruktur nirkabel yang harus dipenuhi dalam keterhubungannya denga jaringan PT. NCS. Hanya perangkat / infrastruktur nirkabel yang memenuhi standard yang didefinisikan dalam kebijakan ini yang diberikan hak akses terhadap konektivitas dengan jaringan PT. NCS.

2.0 Cakupan

Semua karyawan, kontraktor, konsultan, serta pekerja semetara pada PT. NCS, termasuk pula semua personil yang turut memelihara perangkat / infrastruktur nirkabel pada PT. NCS merupakan entitas yang terlingkupi melalui kebijakan ini. Kebijakan ini diterapkan pada semua perangkat / infrastruktur nirkabel yang

terhubung pada jaringan PT. NCS (yang memberikan konektivitas nirkabel pada peralatan pada level endpoint seperti laptop, desktop, telepon selular, serta PDA. Kebijakan ini juga melingkupi semua perangkat nirkabel yang memiliki kapabilitas dalam mengirimkan paket data. Setiap bentuk pengecualian harus mendapatkan persetujuan dari Departemen TI dari PT. NCS.

3.0 Kebijakan

Requirement terhadap Akses Jaringan secara Umum

Semua perangkat / infrastruktur nirkabel yang berada pada site PT. NCS atau terhubung menuju jaringan PT. NCS, atau menyediakan akses terhadap informasi PT. NCS yang dikategorikan sebagai rahasia atau sensitif oleh PT. NCS harus memperoleh perlakuan sebagai berikut:

- Harus dipasang, didukung, dan dijaga tim pendukung yang telah disetujui oleh Departemen TI.
- Menggunakan protokol otentikasi yang disetujui oleh Departemen TI pada PT. NCS.
- Menggunakan protokol enkripsi yang disetujui oleh PT. NCS.
- Menjaga alamat perangkat keras (MAC Address) yang didaftarkan.

- Tidak mengganggu akses nirkabel yang telah ada pada PT. NCS.

4.0 Sanksi dan Ancaman

Setiap karyawan yang ditemukan melanggar kebijakan ini dapat dikenakan tindakan disipliner hingga pemutusan hubungan kerja.pelanggaran terhadap kebijakan ini yang dilakukan oleh pekerja sementara, kontraktor atau vendor dapat menyebabkan pemutusan kontrak dengan PT. NCS.

Policy Document Name	*Removable Media Policy*
Owner	PT. NCS
Prepared By	Junian Dani
Approved By	IT Manager of PT. NCS
Revision	1.0 - Initial Release

1.0 Rangkuman

Media penyimpanan portabel (*removable media*) telah dikenal sebagai sumber infeksi malware dan juga telah secara langsung dikaitkan dengan peristiwa kehilangan informasi sensitif pada banyak organisasi.

2.0 Tujuan

Untuk meminimalisir resiko hilang atau terkuaknya informasi sensitif yang dijaga oleh PT. NCS dan mengurangi resiko infeksi malware pada komputer-komputer yang dioperasikan oleh atau pada PT.NCS.

3.0 Cakupan

Kebijakan ini meliputi semua komputer dan server yang beroperasi pada PT. NCS.

4.0 Kebijakan

Para staff PT. NCS hanya dapat menggunakan media penyimpanan *portable* milik PT. NCS pada komputer kerjanya. Media penyimpanan portable ini tidak boleh terkoneksi atau digunakan pada komputer yang tidak dimiliki atau disewakan oleh PT. NCS tanpa izin secara eksplisit dari Departemen TI PT. NCS. Informasi

sensitif dapat disimpan pada media penyimpanan portable namun harus diekripsi sesuai dengan kebijakan relevan lainnya (dalam hal ini *Acceptable Encryption Use*).

5.0 Sanksi dan Ancaman

Setiap karyawan yang ditemukan melanggar kebijakan ini dapat dikenakan tindakan disipliner hingga pemutusan hubungan kerja.

6.0 Definisi

Istilah	**Definisi**
Media Penyimpanan *Portable* (*Removable Media*)	Peralatan atau media yang dapat ditulis dan dibaca oleh pengguna dan dapat dipindahkan dari suatu komputer ke kamputer lainnya tanpa proses modifikasi pada komputer tujuan. Media atau peralatan ini meliputi *flash memory*, camera, pemutar MP3,dan PDA; hard drive portable; CD dan DVD; dan disket.
Enksipsi	Prosedur yang digunakan untuk mengkonversi data dari format aslinya menuju format lainnya yang tidak mudah terbaca atau tidak dapat digunakan oleh siapapun tanpa informasi atau alat bantu yang dibutuhkan untuk membalikkan proses tersebut.
Informasi Sensitif	Informasi dianggap sebagai sensitif jika informasi

	tersebut dapat membahayakan reputasi dari PT. NCS jika tersebar atau terkuak secara tanpa hah / sah kepada pihak-pihak diluar organisasi atau perusahaan.
Malware	Piranti lunak berbahaya layaknya *virus*, *worm* maupun *spyware*.