

**PERTANYAAN YANG SERING DIAJUKAN  
KEWAJIBAN PENGAMANAN PEMANFAATAN JARINGAN INTERNET  
UNTUK WARUNG INTERNET (WARNET) DAN HOTSPOT**

**1. Mengapa pengamanan pemanfaatan jaringan Internet perlu?**

Beberapa tahun terakhir, Indonesia mendapat sorotan dari komunitas Internet internasional terkait sejumlah laporan terjadinya fraud (penipuan), aktivitas tidak sah (termasuk spamming, virus, malware/spyware dan sejenisnya), serangan cyber, hingga kriminal seperti perjudian, narkoba, terorisme, pornografi, child abuse (kejahatan dan penistaan anak di bawah umur), trafficking (perdagangan manusia, wanita, anak), penggelapan uang, money laundry (pencucian uang) serta kejahatan perpajakan yang berasal dari dan atau berlangsung di Indonesia memanfaatkan fasilitas dan jaringan (infrastruktur) Internet.

Kejadian ini menimbulkan kerugian ekonomi, sosial dan teknis berbagai pihak di luar negeri dan juga di dalam negeri. Banyak dari aktivitas ini merupakan tindak kriminal dan merupakan kejahatan terorganisir di Internet yang menjadi sasaran penindakan aparat penegak hukum di seluruh dunia.

Tingginya frekuensi kejadian dan kualitas kasus yang terus meningkat, telah menempatkan Indonesia pada urutan tertinggi (berdasarkan survey lembaga pengamat dan bisnis di Internet). Akibatnya, dunia Internet Indonesia mendapat sanksi teknis dan dikucilkan dari transaksi bisnis di Internet.

Citra bangsa dan negara Indonesia di Internet dirugikan dan ini berpengaruh di dalam pergaulan Internasional. Pemerintah menghadapi tuntutan dari berbagai negara untuk menanggulangi permasalahan ini dan diminta untuk secepatnya bekerjasama dengan lembaga keamanan Internet lain yang sudah ada di sejumlah negara. Tekanan internasional sangat mungkin terjadi bila tidak ada upaya untuk mulai menangani masalah ini secara konkrit.

Secara ekonomi, selama beberapa tahun terakhir, transaksi bisnis di Internet dari dan ke Indonesia telah banyak ditolak sehingga potensi ekonomi dalam negeri tidak dapat dipromosikan. Indonesia juga telah kehilangan kesempatan untuk mendapatkan manfaat dari perputaran bisnis di Internet yang sedikitnya telah mencapai angka \$ 250 milyar / tahun (survey konsultan bisnis Internet).

Dengan meningkatnya pemanfaatan Internet di bidang layanan publik, birokrasi, pendidikan dan bisnis maka semakin tinggi tuntutan masyarakat di Indonesia terhadap upaya pengamanan jaringan infrastruktur Internet nasional.

Sebagai landasan hukum, adalah Undang-undang Nomer 36 Tahun 1999 Tentang Telekomunikasi yang telah mengamanatkan kewajiban pengamanan ini kepada para penyelenggara. Selanjutnya diterbitkan Peraturan Menteri Komunikasi dan Informatika Nomor 27 Tahun 2006 (diperbaharui Nomor 26 Tahun 2007) Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet. Regulasi ini akan terus ditingkatkan, dilengkapi dan disempurnakan dengan perangkat hukum, operasional pelaksana dan fasilitas yang dibutuhkan.

## **2. Siapa yang akan melakukan pengamanan dan pemantauan?**

Lembaga yang melakukan pengamanan infrastruktur Internet adalah Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII) yang dibentuk oleh Menteri Komunikasi dan Informatika yang anggotanya terdiri dari unsur aparat Pemerintah (termasuk penegak hukum), pakar dari berbagai bidang terkait, akademisi, praktisi dan profesional di bidang telekomunikasi dan Internet.

Pengamanan dan pemantauan dilakukan bersama unsur penyelenggara infrastruktur dan jasa yang dipandang kompeten serta memiliki posisi strategis di dalam komunitas Internet Nasional. Aktivitas semacam ini juga diselenggarakan oleh lembaga sejenis di berbagai negara dan otoritas Internet internasional. ID-SIRTII akan bekerjasama dengan berbagai lembaga sejenis melalui saluran formal antar pemerintahan dan antar lembaga di dalam maupun di luar negeri.

ID-SIRTII adalah lembaga independen yang mengutamakan kepentingan publik. Pemerintah memfasilitasi pembiayaan dan fasilitas ID-SIRTII. Keberadaan unsur Pemerintah berperan sebagai fasilitator, sedangkan fungsi teknis operasional yang membutuhkan keahlian spesifik akan diselenggarakan oleh Pelaksana yang terdiri dari para profesional yang ditunjuk setelah melalui proses seleksi terbuka.

Kebijakan formal (sesuai kepentingan publik) akan dirumuskan bersama anggota yang terdiri dari perwakilan pemangku kepentingan Internet Nasional dan para pakar/ahli terkait. Selain itu dibentuk Dewan Pengawas yang terdiri dari berbagai unsur. Sehingga dalam pelaksanaan tugas ID-SIRTII akan senantiasa terjaga.

## **3. Apakah pengamanan dan pemantauan akan melanggar privacy?**

Sebagaimana lembaga CERT/CSIRT di luar negeri, ID-SIRTII menjalankan fungsi monitoring pada sejumlah simpul utama jaringan Internet Nasional. Tujuan dari monitoring adalah untuk deteksi dini (early warning system) adanya potensi gangguan, ancaman, kemungkinan serangan terhadap infrastruktur Internet.

Pada dasarnya yang dipantau adalah pola (pattern) tertentu traffic Internet yang sedang berlangsung. Perangkat sensor memiliki teknologi identifikasi berdasarkan database pattern untuk mendeteksi pola traffic yang dianggap berbahaya. Bila diketahui ada aktivitas mencurigakan maka sistem akan memberi peringatan.

Perangkat sensor ditempatkan pada core network NAP dalam mode pasif. Artinya, tidak dapat melakukan intervensi pada traffic yang sedang aktif.

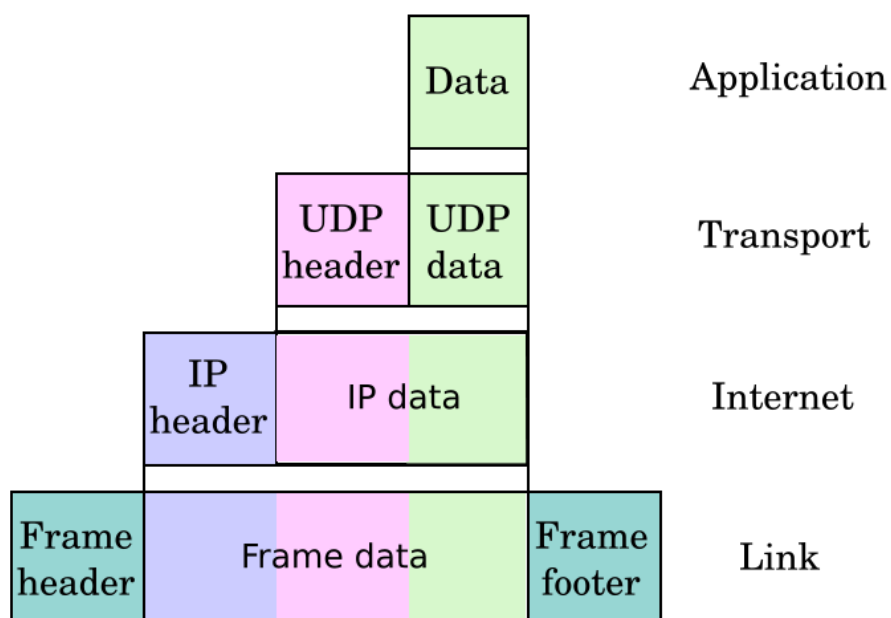
Fungsi pemantauan dimaksudkan sebagai upaya preventif, mencegah terjadinya kemungkinan serangan akibat aktifitas tidak sah di Internet. Lebih jauh, fungsi ini diharapkan mampu memberikan early warning (peringatan dini) terhadap infrastruktur Internet nasional dan yang bersifat kritis (misalnya perbankan, keuangan, transportasi, energi dan pemerintahan / layanan publik) sehingga dapat melakukan tindakan yang diperlukan untuk mencegah dan menanggulangi.

Selain fungsi pemantauan, ID-SIRTII melakukan pengumpulan rekaman transaksi koneksi (log). Pengumpulan ini dimaksudkan sebagai alat bantu analisa dan alat

bukti bagi proses penyidikan dan penindakan hukum (law enforcement) bila terjadi tindak pidana atau pelanggaran hukum lainnya. Proses rekaman transaksi koneksi (log) dilakukan sendiri oleh ISP, kemudian dikirimkan ke ID-SIRTII dalam format terenkripsi untuk kemudian langsung disimpan dan diamankan.

Perekaman transaksi koneksi (log) inipun tidak mencakup keseluruhan informasi traffic hingga sampai ke konten melainkan hanya meliputi sebagian informasi layer transport (sesuai standar TCP/IP Layer) yaitu antara lain:

- a. IP address (alamat IP, identitas Internet)
- b. Jenis protocol akses (TCP, UDP, HTTP, FTP, SMTP)
- c. Alamat port asal (source) maupun tujuan (destination)
- d. Waktu (time stamp) yang lamanya diakumulasikan (durasi).



**Diagram TCP/IP Stack**

Sehingga jelas bahwa content (isi) dan atau kandungan data transaksi Internet, BUKAN bagian yang akan dipantau ID-SIRTII dan atau dicatat dalam rekaman transaksi koneksi oleh ISP. ID-SIRTII juga TIDAK AKAN MELAKUKAN PERUBAHAN APAPUN terhadap asal, identitas, tujuan, kandungan dan catatan waktu transaksi yang dipantau oleh sistem pemantauan maupun yang dicatat di dalam log.

Pemerintah, Departemen Kominfo, Ditjen Postel, ID-SIRTII dan aparat penegak hukum (polisi, jaksa) yang nantinya terlibat dalam aktivitas ini, sangat menghargai hak asasi, kebebasan dan kerahasiaan Individu yang dijamin oleh konstitusi. Semua hak warga negara terkait aktivitas ini dilindungi proporsional.

Namun apabila terjadi tindak pidana dan atau pelanggaran hukum, maka aparat hukum berwenang untuk memanfaatkan segala sumber daya untuk melakukan

penegakan (enforcement). Data yang ada pada ID-SIRTII dapat dimanfaatkan untuk maksud tersebut sesuai dengan peraturan perundangan yang berlaku.

#### **4. Apakah hanya Warnet yang dikenai kewajiban ini?**

**TIDAK.** Kewajiban ini terutama ditujukan kepada operator infrastruktur dan jasa layanan Internet. Misalnya operator telekomunikasi, NAP (Network Access Provider – penyelenggara infrastruktur jaringan, interkoneksi dan akses Internet internasional) dan ISP (Internet Service Provider – penyedia jasa dan layanan Internet). Selanjutnya, kewajiban dikenakan pada penyelenggara akses Internet publik yang merupakan distribution channel (saluran distribusi layanan), termasuk dalam klasifikasi ini adalah Warnet, HotSpot dan sejenisnya.

Saluran distribusi layanan juga dikenai kewajiban karena umumnya digunakan masyarakat luas (publik) secara bebas sehingga tidak teridentifikasi. Pengguna layanan seperti Warnet dan HotSpot sebagian besar bukanlah member (anggota) yang tercatat (terdokumentasi) identitasnya sehingga tidak mudah diidentifikasi.

Pengguna Warnet dan sejenisnya memiliki mobilitas tinggi (sering berpindah) dan tidak terikat pada satu penyelenggara layanan saja. Sifat akses anonim dan acak ini berpotensi besar untuk dimanfaatkan pelaku tindak pidana dan atau pelanggar hukum dalam menjalankan aksinya. Sehingga penyelenggara Warnet dan HotSpot sering dianggap terlibat atau memfasilitasi terjadinya tindak kejahatan.

Kewajiban pengamanan juga berlaku bagi penyelenggara jaringan dan layanan Internet yang bersifat private atau closed group (kelompok tertutup). Termasuk dalam klasifikasi ini adalah coporate (perusahaan) besar yang memiliki jaringan dan akses Internet sendiri serta memiliki banyak pengguna yang tersebar, juga jaringan lembaga pendidikan dan jaringan pemerintahan (pusat dan daerah).

Khusus untuk operator telekomunikasi, NAP dan ISP (dan sejenisnya), termasuk kelompok tertutup, diwajibkan melakukan pemantauan dan menyerahkan rekaman transaksi koneksi (log) secara periodik kepada ID-SIRTII untuk dianalisa.

#### **5. Apakah ada sanksi apabila kewajiban ini tidak dilaksanakan?**

Sesuai peraturan perundangan yang berlaku saat ini, maka Warnet atau HotSpot sebagai saluran distribusi layanan yang digolongkan sebagai jasa jual kembali, BUKAN merupakan lembaga yang dapat dikenai sanksi. Karena Warnet belum (atau tidak) diatur secara formal di dalam tatanan industri Internet Nasional.

Namun bila terjadi kasus, sementara Warnet tidak melaksanakan kewajibannya, maka sangkaan keterlibatan dalam tindak pidana dan atau pelanggaran hukum dapat dikenakan pada pemilik dan pengelola Warnet. Juga sanksi penyitaan dan penyegehan hingga pencabutan ijin usaha, pembekuan operasi sesuai proporsi.

Walaupun tidak ada sanksi langsung, namun apabila Warnet tidak melaksanakan kewajiban ini, resikonya sangat besar. Bila sampai ada insiden, potensi kerugian yang akan dialami misalnya akibat penyegehan, tidak akan sebanding.

## 6. Apakah pengamanan ini bermanfaat bagi Warnet dan HotSpot?

**YA.** Pengamanan ini juga bertujuan untuk memberikan manfaat bagi Warnet dan HotSpot. Pemerintah menempatkan Warnet dan HotSpot sebagai salah satu ujung tombak penetrasi pemanfaatan Internet bagi masyarakat luas. Keterbatasan infrastruktur Internet yang memadai telah menyebabkan kesenjangan pemerataan distribusi akses dan harga layanan. Warnet dan HotSpot telah berhasil menjembatani kesenjangan tersebut sehingga posisinya strategis sebagai alternatif akses Internet yang terjangkau dan tersedia hingga ke pelosok.

Pengamanan ini antara lain dimaksudkan untuk membersihkan stigma terhadap Warnet dan HotSpot. Selama ini, karena sifat pengguna yang anonim dan acak, maka dalam banyak kasus Warnet dan HotSpot diduga memfasilitasi pelaku tindak pidana dan atau pelanggar hukum dalam menjadikan aksinya.

Bahkan ada oknum Warnet dan HotSpot yang ternyata juga sengaja memfasilitasi, terlibat dan atau sekaligus menjadi pelaku. Apabila nanti kewajiban pengamanan telah dilaksanakan oleh Warnet, maka akan terjadi perubahan sifat pengguna, menjadi teridentifikasi dan terbatas sehingga mengurangi peluang dan mencegah terjadinya penyalahgunaan. Sehingga Warnet dan HotSpot akan menjadi tempat yang aman dan nyaman bagi publik untuk mengakses Internet.

Dengan melaksanakan kewajiban pengamanan ini Warnet dan HotSpot dapat terhindar dari tuduhan keterlibatan dalam tindak pidana atau pelanggaran hukum.

## 7. Bagaimana cara Warnet melaksanakan kewajiban ini?

Warnet dan HotSpot melaksanakan kewajiban dengan cara melakukan pencatatan identitas setiap pengguna layanannya. Data ini kemudian disimpan dan diamankan selama 1 (satu) tahun. Bila dibutuhkan, atau ketika terjadi kasus, data ini akan diminta oleh aparat penegak hukum untuk dianalisa, diverifikasi dan selanjutnya dapat dijadikan petunjuk untuk melakukan penyidikan dan atau menjadi alat bukti.

Warnet dan HotSpot **TIDAK** dibebani untuk melakukan verifikasi data (keaslian) identitas yang diberikan pengunjung/pengguna layanannya. Pencatatan dilakukan apa adanya sesuai yang ditunjukkan/diberikan oleh yang bersangkutan. Warnet juga **TIDAK** perlu mengirimkan data pencatatan identitas kepada ID-SIRTII dan atau aparat penegak hukum, melainkan cukup disimpan dan diamankan sendiri.

Pemerintah juga tidak menentukan format tertentu, karena setiap Warnet dan HotSpot memiliki karakteristik sistem yang berbeda. Dimana, mungkin merupakan bagian dari investasi aplikasi billing system yang tidak sederhana dan tidak mudah untuk diubah dalam waktu singkat serta akan menjadi proses yang membebani Warnet dan HotSpot. Sehingga, format sederhana non digital (termasuk dokumen fisik) berupa kopi kartu identitas dan atau catatan akses, tetap dapat diterima sebagai bukti pencatatan. Meskipun demikian, bentuk digital akan lebih baik.

ID-SIRTII akan menyarankan format digital generik yang lebih praktis dan disukai karena mudah untuk diolah (analisa dan verifikasi). Misalnya format citra (image) digital (.jpg, .gif, .tiff, .bmp) untuk hasil scanning kartu identitas. Sedang untuk

data akses dapat disimpan dalam bentuk comma delimited (.csv) yang dihasilkan oleh aplikasi spreadsheet biasa yang umumnya sudah tersedia di setiap Warnet dan HotSpot. Atau apabila ada aplikasi database yang memadai, format .dbf, .mdb yang mampu menyimpan data akses dan citra (image) sekaligus dalam satu file.

Beberapa software house (developer) kini menawarkan aplikasi billing system yang sudah dilengkapi fitur pendataan pengunjung, terintegrasi dengan catatan waktu serta dapat disimpan dalam format digital file generik.

Data yang perlu dicatat sebaiknya terdiri dari:

- e. Nomor kartu identitas (SIM, KTP, Kartu Pelajar/Mahasiswa)
- f. Nama lengkap (opsional: nama kecil, julukan)
- g. Alamat lengkap (opsional: nomer telepon, hp)
- h. Jenis kelamin, Tanggal lahir, Pekerjaan, Status
- i. Catatan waktu akses (mulai, berakhir, durasi)
- j. Catatan terminal akses dan IP yang digunakan
- k. Opsional: copy kartu identitas dan atau foto.

Tidak semua pengunjung Warnet dan HotSpot memiliki kartu identitas yang formal seperti contoh di atas. Misalnya pelajar di bawah umur, pengunjung lingkungan sekitar atau member (pelanggan tetap) yang mungkin juga sudah dikenal, dapat langsung dicatat identitas berdasarkan PENGAKUAN ybs.

Kartu identitas juga dapat digantikan kartu nama, kartu pengenalan atau sejenisnya. Warnet dan HotSpot TIDAK dibebani kewajiban untuk melakukan validasi terhadap informasi yang diberikan oleh pengunjung dicatat apa adanya. Pendataan TIDAK dimaksudkan untuk mempersulit atau menimbulkan resistensi dan penolakan pengunjung yang akan merugikan Warnet dan HotSpot dalam jangka panjang.

Catatan waktu sangat penting, karena itu semua aplikasi pendataan ini sebaiknya menyesuaikan dengan time server referensi yang ditunjuk oleh Ditjen Postel atau yang disediakan oleh ISP. Formatnya mengikuti standar **DD/MM/YYYY** untuk penanggalan dan **HH:MM:SS** untuk waktu/jam. Kesamaan dan akurasi catatan waktu akan dapat mempertajam analisa dan verifikasi apabila terjadi insiden.

Catatan terminal akses, ada baiknya apabila dispesifikasikan lebih detail, seperti tambahan informasi MAC address, IP yang digunakan riwayat pemindahan dan perubahan (sering dipertukarkan). Karena mungkin, 'data sampah' yang tersimpan dalam terminal akses juga akan digunakan oleh aparat penegak hukum.

## **8. Apakah data pencatatan dapat digunakan untuk tujuan lain?**

**YA.** Data tersebut adalah hak Warnet dan HotSpot, tentu saja dapat dipergunakan untuk tujuan dan kebutuhan sendiri. Jauh sebelum ada ID-SIRTII, AWARI dan ID-HOTSPOT telah lama mengkampanyekan pendataan pengunjung Warnet dan HotSpot. Tujuannya adalah agar industri Warnet dan jasa layanan HotSpot memiliki data dan informasi pasar yang akurat dan terkini. Data tersebut sangat

penting sebagai bahan analisa dan kajian bagi manajemen untuk forecast (peramalan bisnis), kondisi trend pasar dan menentukan strategi bisnis.

Pada dasarnya yang dibutuhkan oleh aparat penegak hukum hanyalah informasi identitas pengunjung, minimal nomor kartu identitas, nama, alamat dan catatan waktu akses serta terminal yang digunakan. Informasi lain sifatnya opsional. Bila Warnet dan HotSpot dapat menyediakan data dan informasi yang lebih lengkap, sangat mungkin akan membantu percepatan proses penyidikan.

Upaya mendapatkan informasi harus dilakukan dengan cara yang baik dan tepat serta mengutamakan kenyamanan pengunjung, sehingga tidak merugikan Warnet dan HotSpot. Misalnya pencatatan melalui program promosi membership customer reward, client feedback dsb. Dengan memiliki data pengunjung, Warnet dan HotSpot dapat mengetahui profil pelanggan sehingga dapat menentukan produk dan layanan yang terbaik. Evaluasi data bisa menghasilkan rekomendasi pada manajemen untuk senantiasa melakukan improvisasi, revitalisasi dan inovasi.

Data yang dihasilkan, apabila diolah dengan tepat akan membantu Warnet dan HotSpot untuk terus beradaptasi menjawab berbagai tantangan di dalam perkembangan industri retail akses Internet. Oleh karena itu kewajiban pendataan justru sangat menguntungkan bagi Warnet dan HotSpot, baik secara bisnis maupun politis. Menghindari stigma, terlindungi hak dan bisnisnya serta memiliki modal data yang akurat untuk mengembangkan bisnis serta inovasinya.

## **9. Siapa yang menanggung pembiayaan pelaksanaan kewajiban?**

Dalam Undang-undang Nomor 36 Tahun 1999 Tentang Telekomunikasi, kewajiban pengamanan (pasal 39), kewajiban perekaman pemakaian fasilitas serta perekaman informasi (pasal 41), untuk digunakan dalam proses peradilan pidana (pasal 42), akan menjadi tanggung jawab penyelenggara jasa. Sehingga segala macam konsekuensi yang timbul termasuk investasi dan biaya operasional menjadi tanggungan pelaku usaha itu sendiri.

ID-SIRTII sebagai lembaga pelaksana operasional peraturan teknis pengamanan infrastruktur jaringan Internet Nasional, memperhatikan dan melakukan antisipasi kemungkinan permasalahan biaya investasi dan operasional. Salah satu cara yang mereduksi beban biaya bagi Warnet dan HotSpot adalah dengan memberikan rekomendasi format data yang efisien.

Dengan menggunakan format digital text .csv, untuk menyimpan informasi nomor identitas, nama dan alamat (opsional, waktu penggunaan dan informasi terminal akses) akan dibutuhkan kapasitas penyimpanan sebesar 500 bytes. Asumsi dalam sehari sebuah Warnet dan HotSpot mendapat kunjungan unik sekitar 100 (seratus) orang maka dalam 1 (satu) tahun (360 hari) akan dibutuhkan kapasitas penyimpanan sebesar  $500 \text{ bytes} \times 100 \times 360 = 18.000.000 \text{ Bytes}$  atau sekitar 18 Mega Bytes tanpa kompresi apapun.

Apabila ditambahkan dengan hasil scan kartu identitas akan diperlukan tambahan kapasitas sebesar 300 kilobytes per orang dengan asumsi menggunakan format digital .jpg (tanpa kompresi). Dengan jumlah pengunjung unik 100 (seratus)

orang per hari, maka dalam setahun akan dibutuhkan  $300.000 \text{ bytes} \times 100 \times 360 = 10.800.000.000$  Bytes atau sekitar 10.8 Giga Bytes. Data ini dapat disimpan pada media 18 CD (kapasitas standar 650 Mega Bytes) atau 3 DVD (kapasitas standar 4 Giga Bytes) tanpa kompresi dengan biaya kurang dari Rp. 100.000 (seratus ribu rupiah). Biaya ini relatif akan terjangkau.

Dengan asumsi, pada umumnya Warnet dan HotSpot telah memiliki perangkat CD/RW atau DVD/RW dan aplikasi pendataan pengunjung telah terintegrasi dalam billing system, maka biaya yang harus dikeluarkan untuk melaksanakan kewajiban ini, secara teknis (khusus untuk media penyimpanan) masih dapat terjangkau, sehingga tidak membebani investasi atau cash flow operasional.

Apabila Warnet dan HotSpot belum memiliki billing system, perangkat CD/RW atau DVD/RW maka diperlukan biaya investasi. Estimasi untuk Warnet kecil dengan kekuatan belasan PC atau kurang, diperlukan investasi Rp 500.000 (lima ratus ribu rupiah) untuk pembelian billing system dan Rp 500.000 (lima ratus ribu rupiah) untuk pembelian perangkat CD/RW atau DVD/RW.

Estimasi untuk Warnet besar dengan kekuatan puluhan PC, diperlukan investasi Rp 1.500.000 (satu juta lima ratus ribu rupiah) untuk pembelian billing system dan Rp 500.000 (lima ratus ribu rupiah) untuk pembelian perangkat CD/RW atau DVD/RW. Biaya ini dikeluarkan sekali sebagai investasi, dimana billing system dan perangkat CD/RW atau DVD/RW sebenarnya adalah kelengkapan operasional dan layanan Warnet bukan khusus ditujukan untuk pelaksanaan kewajiban ini saja.

#### **10. Selain pencatatan identitas pengunjung, apakah ada kewajiban lain, misalnya keharusan menyediakan CCTV?**

**TIDAK.** Saat ini masih belum dibutuhkan rekaman video. Meskipun demikian, apabila Warnet dan HotSpot dapat menyediakan CCTV dan rekamannya tentu akan sangat membantu proses penyidikan dan pembuktian apabila terjadi kasus. Dari sudut kepentingan Warnet dan HotSpot sendiri, CCTV sebenarnya juga diperlukan sebagai alat bantu pengawasan keamanan, terutama untuk Warnet yang memiliki banyak terminal di ruangan yang terpisah. CCTV membantu efisiensi operator, pengawas Warnet dalam melaksanakan tugas. Banyak kejadian seperti pencurian perangkat menimpa Warnet pada masa sebelumnya, CCTV dapat membantu mencegah hal semacam ini terulang.

Tidak menutup kemungkinan di masa depan, apabila Warnet telah berkembang dan menghadapi berbagai masalah keamanan serius, keberadaan CCTV akan menjadi kebutuhan yang mungkin harus disediakan. Demikian juga dengan implementasi teknologi pengawasan lainnya. Pemerintah dan ID-SIRTII akan menyesuaikan kebutuhan tersebut PADA WAKTU DAN KONDISI YANG TEPAT dan secara umum tidak merugikan kepentingan Warnet dan HotSpot.

ID-SIRTII akan selalu memperhatikan masukan, saran dan kritik dari masyarakat Internet Nasional, khususnya komunitas Warnet dan HotSpot serta sedapat mungkin mengakomodasi seluruh kepentingan secara rasional dan proporsional.

#### **Daftar Istilah**

1. CSIRT = Computer Security Incident Response Team
2. CERT = Computer Emergency Response Team
3. CCTV = Closed Circuit Television

**::: Copyright © 2007, ID-SIRTII :::**