Arrohmani 0110215038
Agung Prayoga 0110215050
Rufaidah Taqiyyah 0110215026
M. Hamzah Nashirullah K 0110215040

Kode Etik Profesional IT untuk Melindungi Informasi Elektronik

Dalam rangka mendukung bisnis universitas, staf IT yang melakukan tugas rutin mungkin memiliki akses ke data dalam aplikasi, email dan sistem file atau pada desktop, server dan jaringan dan sistem lain yang harus dilindungi oleh universitas.
Dalam menjalankan tugasnya, Staf IT akan mematuhi kebijakan universitas yang berlaku termasuk kebijakan keamanan informasi harvard dan kebijakan komunikasi elektronik harvard.

Sebagai organisasi IT Harvard :

- Staf TI akan menerima komunikasi dan pelatihan mengenai kode etik
- Staf TI akan diminta untuk setiap tahun meninjau dan menegaskan kode etik
- Kepemimpinan TI akan memberikan panduan tentang kode etik ini karena tantangan diamati atau dihadapi
- Kepemimpinan TI akan meninjau dan merevisi kode etik sesuai kebutuhan dalam menanggapi setiap insiden atau sebagai perubahan teknologi

Sebagai IT Profesional :

- Kita mempunyai access terhadap informasi electronic user,beberapa diantaranya bersifat pribadi dan rahasia

- Kita membutuhkan access informasi electronic user utk dikembangkan,tes,implementasi,dan dukungan terhadap aplikasi universitas,system,dan jaringan utk memastikan berjalan semestinya.Untuk melindungi terhadap ancaman seperti serangan malware dan virus.Untuk melindungi integritas dan keamanan informasi,untuk berjalannya bisnis dan membantu menangani ancaman terhadap kampus dan individual

- Ini adalah bagian dari tugas untuk membantu melindungi semua informasi electronic user dari access yang tidak sah

Sebagai IT Professional :

- Kita hanya membutuhkan informasi untk melancarkan pekerjaan atau sesuatu yang ditugaskan utk kita memperolehnya berdasarkan arahan universitas / hukum yang sah.

- kami hanya menggunakan informasi yang terkumpul untuk tujuan yang diperolehnya, lindungi dengan benar informasi yang ada dalam kepemilikan kita dan buanglah dengan benar setelah tidak lagi dibutuhkan untuk tujuan bisnis

- kami tidak akan membaca dengan teliti atau memeriksa informasi elektronik pengguna untuk tujuan apa pun selain untuk menangani masalah tertentu

- Kami mengerti bahwa kegagalan untuk memenuhi kode etik dianggap melanggar kepercayaan dan merupakan dasar tindakan disipliner sampai dan termasuk pemecatan

- kami akan menandatangani pengakuan tahunan bahwa kami menerima, membaca, dan memahami kode etik ini

Dibawah ini adalah beberapa contoh dari kode etik dalam prakteknya. contoh ini dimakasudkan untuk menggambarkan code of conduct in practice, tapi tidak menyeluruh. jika ada kebutuhan untuk pengecualian terhadap prinsip dan contoh dalam kode etik ini, persetujuan harus diperoleh dari universitas CIO, universitas CSO atau sekolah CIO

Teknisi Lapangan

- Teknis tidak boleh meminta atau bertanya kepada user terhadap Password atau PIN mereka dan jangan sampai mengamati mereka ketika sedang mamasukkan Password atau PIN

- Teknisi tidak boleh membuka email atau file saat memecahkan masalah kecuali pengguna memberikan izin khusus dan harus memeriksa hanya contenc email atau file yang diperlukan untuk memecahkan masalah tertentu

- Akses jarak jauh ke desktop untuk tujuan dukungan hanya dapat terjadi dengan persetujuan pengguna akhir melalui prompt desktop tertentu

kualitas insinyur, pengembang, manajer proyek dan analisis bisnis

- Ketika pengembangan, pengujian analisis, Menjaga atau memecahkan masalah dalam aplikasi universitas, catatan hanya boleh diinterogasi jika terkait dengan masalah yang sedang diselidiki

- Ketika sedang menampilkan contoh halaman, file, alur bisnis atau laporan dokumentasi keluar,tindakan yang tepat harus diambil untuk menyamarkan informasi untuk melindungi identitas individu yang terkait dengan datanya

- Untuk tujuan presentasi, pengembangan, testing, analisis, pemeliharaan atau masalah, tindakan yang tepat harus diambil untuk menyamarkan informasi untuk melindungi identitas indvidu yang terkait denga datanya

Insinyur jaringan

- Data yang melintasi jaringan tidak boleh dipantau kecuali untuk pemeliharaan, diagnosa spesifik dan tujuan proteksi sistem (ex. menscan proteksi virus)

- Akses terhadap informasi log hanya boleh digunakan untuk tujuan bisnis dan diperlukan untuk mendukung integritas sistem

Staf Helpdesk

- tidak menanyakan passwor atau pin pengguna

- hanya dapat meneruskan email ke bagian lain ketika diminta oleh kotak pesan pemilik

Administrasi Sistem dan Database

- data yang berada pada file log dan database tidak boleh diungkapkan selain dari kebutuhan grup IT untuk Pengembangan, pemeliharan, mengatasi masalah atau melakukan diagnosa kecuali dibawah petunjuk dari universitas atau hukum yang sah
- informasi tentang akses khusus pengguna terhadap jaringan, sistem, database, atau sumber laiun berbasis komputer tidak boleh diungkapkan kepada siapapun selain pemilik kecuali dibawah arahan dari universitas atau hukum yang sah atau untuk tujuan pengembangan, pengetesan, pemeliharaaan, pelindungan dan mendukung sistem IT

- tampilan dari data apapun yang terkandung di dalma file log dan database yang jatuh diluar dari tanggung jawab kerja karyawan adalah sangat dilarang

Product Control dan Operator Komputer

- semua akses secara fisik terhadap pusat data universitas harus berdasarkan prosedur penggunaan akses yang berlaku, semua permintaan akses dari individu yang tidak sah harus dirujuk supervisor atau manager.

- semua permintaan akses terhadap sistem harus berdasarkan prosedur penggunaan akses yang berlaku. semua permintaan akses terhadap sistem diluar dari operator khusus yang berdasarkan prosedur penggunaan akses harus dirujuk dari supervisor atau manager.

- semua permintaan akses hak istimewa untuk sistem produksi untuk pemberian akses harus berdasarkan prosedur yang berlaku. termasuk dalam ketepatan waktu dan akurasi catatan dari permintaan dan waktu kembali dari hak istimewa yang diminta untuk akses hak istimewa

Security Engginers

- profesional keamanan informasi harvard mematuhi kode etik yang ketat melalui sertifikasi mereka oleh dewan sertifikasi keamanan sistem internasional, yang mengharuskan mereka :
    1. melindungi masyarakat yang persemakmuran dan infrastrukturnya

2. bertindak secara terhormat, jujur, tanggng jawab, adil dan sah
3. menyediakan pelayanan yang rajin dan kompeten untuk penyuruh

- Ketika sedang meluncurkan sebuah investigasi/penyelidikian harus waspada terhadap kemungkinan aktifitas yang jahat (dari alat otomatis, pengguna, atau pihak ketiga) insinyur keamanan harus bertindak secara bertanggung jawab dan etis, khususnya :
  - Selidiki hanya dalam lingkup yang sudah teridentifikasi alasannya
  - acak aktivitas berbahaya ke mesin asal dan hubungi pemilik dan dukungan TI mereka, bagikan informasi dan bantu proses resolusi

- Jika individu menolak untuk berpartisipasi pada resolusi tersebut, security engineers harus :
  - meluncurkan proses eskalasi dengan mendapat persetujuan manajemen terlebih dahulu untuk melakukan tindakan lebih lanjut
  - mengikuti jalan eskalasi yang sudah ditentukan yang meliputi pemberitahuan ke lokal manajemen. CISO, HR, & OGC

- Saat melakukan forensik pada komputer yang diakusisi, security engineers harus :
  - membatasi aktifitas investigasi secara sempit, hanya mengerjakan informasi relevan.
  - hanya melihat informasi pribadi individu jika diperlukan untuk investigasi
  - menyimpan bahan-bahan investigasi yang fisik maupun digital dengan aman terkunci. contoh : salinan hard drive
  - memelihara rantai hak asuh untuk bukti, membutuhkan tanggung jawab dan menandatangani setiap langkah dari proses

SELESAI
TERIMA KASIH