TUGAS
KEAMANAN SISTEM INFORMASI
1.1.6 - Lab - Develop Cybersecurity Policies and Procedures

Anisatul Latifah
2141762008
SIB – 4C

POLITEKNIK NEGERI MALANG
2024/2025

Bagian 3: Mengembangkan Dokumen Kebijakan

Langkah 1 : Buat Kebijakan Keamanan Informasi

"Beberapa akun diidentifikasi untuk karyawan yang tidak lagi bekerja di ACME Healthcare."

1. **Ikhtisar (Overview)**
   ACME Healthcare bertujuan untuk melindungi data sensitif dan memastikan bahwa hanya karyawan aktif yang memiliki akses ke sistem perusahaan. Akun karyawan yang sudah tidak bekerja di ACME Healthcare akan dinonaktifkan untuk menghindari risiko akses yang tidak sah.

2. **Tujuan (Purpose)**
   Kebijakan ini bertujuan untuk memastikan bahwa semua akun karyawan yang tidak lagi bekerja di ACME Healthcare dihapus atau dinonaktifkan secara tepat waktu guna menghindari pelanggaran keamanan, seperti akses tidak sah ke data dan sistem perusahaan.

3. **Lingkup (Scope)**
   Kebijakan ini berlaku untuk semua karyawan, kontraktor, dan pihak ketiga yang memiliki akses ke sistem ACME Healthcare. Kebijakan mencakup semua akun yang terhubung dengan karyawan, baik yang dikelola oleh perusahaan maupun pihak ketiga.

4. **Kebijakan (Policy)**
   a. **Penghapusan Akun:** Semua akun yang terkait dengan karyawan yang telah berhenti bekerja di ACME Healthcare harus dihapus atau dinonaktifkan **dalam waktu 24 jam** setelah hari terakhir kerja karyawan tersebut.
   b. **Pelaporan oleh HR:** Departemen HR harus memberi tahu Departemen IT tentang setiap karyawan yang keluar minimal **3 hari sebelum** hari terakhir kerja.
   c. **Tanggung Jawab Departemen IT:** Departemen IT bertanggung jawab untuk menonaktifkan atau menghapus akun, serta memastikan bahwa tidak ada akses ke jaringan, data, atau aplikasi perusahaan yang tetap aktif.
   d. **Audit Berkala:** Tim IT harus melakukan audit sistem secara berkala **setiap kuartal** untuk memverifikasi tidak ada akun karyawan yang keluar yang masih aktif.
   e. **Pelanggaran:** Setiap kegagalan dalam mengikuti kebijakan ini dapat mengakibatkan tindakan disipliner sesuai dengan pedoman perusahaan.

Langkah 2: Buat Prosedur
Prosedur Penonaktifan Akun Mantan Karyawan:

1. **HR Melaporkan Karyawan Keluar**
   - HR mengirimkan pemberitahuan resmi ke Departemen IT **3 hari** sebelum hari terakhir karyawan.
   - Pemberitahuan harus mencakup daftar akun yang harus dinonaktifkan, termasuk email, VPN, dan aplikasi internal.
2. **Penonaktifan Akun oleh IT**
   - Tim IT menerima laporan dari HR dan memverifikasi semua akun yang terkait dengan karyawan tersebut.
   - Tim IT harus menonaktifkan akun dalam waktu **24 jam** setelah karyawan berhenti bekerja.
   - Jika akun yang dimaksud terkait dengan aplikasi pihak ketiga, tim IT harus berkoordinasi dengan administrator pihak ketiga untuk memastikan akun tersebut juga dinonaktifkan.

3. **Audit Berkala**
   - Tim IT harus melakukan audit sistem setiap **kuartal** untuk memastikan tidak ada akun mantan karyawan yang masih aktif.
   - Hasil audit harus dilaporkan ke manajemen senior untuk evaluasi dan tindakan korektif jika diperlukan.
4. **Penghapusan Akses Fisik**
   - HR bekerja sama dengan keamanan fisik untuk mencabut akses fisik, seperti kartu akses atau kunci keamanan.
5. **Pelaporan Masalah**
   - Jika terjadi masalah dalam menonaktifkan akun, tim IT harus segera melaporkannya kepada manajemen untuk tindakan segera.

Bagian 4: Mengembangkan Rencana Penyebaran dan Evaluasi Kebijakan
Langkah 1: Rencana Implementasi dan Penyebaran

a. **Informasi untuk Rencana Penerapan dan Penyebaran:**
   - Kebijakan akan disebarluaskan melalui email internal, intranet perusahaan, dan pelatihan formal kepada seluruh karyawan.
   - Tim IT dan HR akan dilibatkan secara langsung dalam proses pelatihan dan implementasi kebijakan.
   - Setiap karyawan baru harus menerima pelatihan terkait kebijakan ini selama orientasi karyawan baru.

b. **Tugas dan Acara Spesifik:**
   - **Pelatihan IT dan HR:** Tim IT dan HR akan menerima pelatihan khusus tentang kebijakan ini untuk memastikan kepatuhan.
   - **Sesi Evaluasi:** Setiap **6 bulan**, manajemen akan mengadakan sesi evaluasi untuk memverifikasi bahwa kebijakan dijalankan sesuai dengan prosedur.
   - **Audit Berkala:** Tim IT akan melakukan audit setiap **kuartal** untuk memastikan tidak ada akun mantan karyawan yang masih aktif.

c. **Departemen yang Terlibat:**
   - **Departemen IT:** Bertanggung jawab untuk menonaktifkan akun, melakukan audit berkala, dan melatih staf terkait kebijakan ini.
   - **Departemen HR:** Bertanggung jawab untuk melaporkan keberangkatan karyawan dan memastikan bahwa semua akun terkait dilaporkan ke IT tepat waktu.
   - **Departemen Manajemen:** Bertanggung jawab untuk meninjau laporan audit dan memastikan bahwa kebijakan diterapkan dengan benar.

Kesimpulan :
Kebijakan ini bertujuan untuk melindungi sistem ACME Healthcare dari risiko yang diakibatkan oleh akun mantan karyawan yang masih aktif. Dengan prosedur yang jelas dan audit berkala, risiko pelanggaran keamanan dapat dikurangi secara signifikan. Rencana penyebaran dan pelatihan akan memastikan bahwa setiap individu memahami tanggung jawabnya dalam mematuhi kebijakan ini.

Information Security Policy Templates

1. Ikhtisar (Overview)
Tim Infosec ACME Healthcare memiliki tujuan untuk melindungi data, sistem, dan jaringan perusahaan dari risiko yang muncul akibat akun-akun yang tetap aktif meskipun karyawan yang terkait dengan akun tersebut sudah tidak lagi bekerja di perusahaan. ACME Healthcare berkomitmen melindungi informasi perusahaan, karyawan, dan mitra dari risiko akses yang tidak sah.
Sistem terkait internet, perangkat mobile, akun jaringan, perangkat penyimpanan, dan semua sumber daya IT yang dimiliki atau disewa oleh ACME Healthcare adalah properti perusahaan. Sistem ini hanya digunakan untuk kepentingan bisnis yang mendukung operasi perusahaan. Setiap karyawan dan pihak terkait bertanggung jawab untuk mematuhi pedoman ini dan berpartisipasi dalam menjaga keamanan informasi.

2. Tujuan (Purpose)
Tujuan dari kebijakan ini adalah untuk menghapus atau menonaktifkan akun mantan karyawan yang tidak lagi bekerja di ACME Healthcare guna melindungi data sensitif dan mencegah akses tidak sah. Penggunaan yang tidak tepat dapat menimbulkan risiko seperti pelanggaran data, serangan malware, dan implikasi hukum.

3. Lingkup (Scope)
Kebijakan ini berlaku untuk semua karyawan, kontraktor, konsultan, serta pihak ketiga yang memiliki akses ke sistem dan jaringan ACME Healthcare. Kebijakan mencakup semua perangkat dan akun yang terkait dengan ACME Healthcare, baik yang dimiliki perusahaan, disewa, atau dikelola oleh karyawan.

4. Kebijakan (Policy)

4.1 Penggunaan Umum dan Kepemilikan (General Use and Ownership)

a. Informasi yang terkait dengan akun karyawan yang disimpan dalam sistem perusahaan tetap menjadi milik ACME Healthcare.
b. Setiap akun karyawan yang sudah tidak bekerja di ACME Healthcare harus dihapus atau dinonaktifkan **dalam waktu 24 jam** setelah hari terakhir kerja karyawan tersebut.
c. Tim IT bertanggung jawab untuk memonitor dan menghapus akun yang tidak aktif secara berkala melalui audit internal.
d. Karyawan atau departemen lain yang mengetahui mantan karyawan masih memiliki akses ke sistem harus segera melaporkannya ke tim IT. Departemen HR wajib melaporkan setiap karyawan yang keluar kepada tim IT minimal **3 hari** sebelum hari terakhir kerja.

4.2 Keamanan dan Informasi Rahasia (Security and Proprietary Information)

a. Semua akun mantan karyawan yang tersimpan di perangkat mobile atau sistem komputasi yang terhubung ke jaringan internal harus dihapus atau dinonaktifkan.
b. Kata sandi akun yang tidak aktif harus diganti segera setelah penonaktifan.
c. Sistem dan perangkat yang digunakan untuk mengakses jaringan perusahaan harus dilindungi oleh layar kunci otomatis.

4.3 Penggunaan yang Tidak Diperbolehkan (Unacceptable Use)

a. Membiarkan akun karyawan yang telah keluar tetap aktif setelah mereka tidak lagi bekerja di ACME Healthcare tanpa izin khusus adalah pelanggaran serius.
b. Akses yang tidak sah, seperti penggunaan akun karyawan yang tidak aktif oleh pihak ketiga, dilarang keras
c. Penggunaan perangkat lunak atau alat yang memungkinkan akses ilegal ke akun

mantan karyawan juga dilarang.

5. Kepatuhan (Compliance)

5.1 Pengukuran Kepatuhan (Compliance Measurement)

Tim Infosec akan memverifikasi kepatuhan terhadap kebijakan ini melalui audit berkala, laporan sistem, dan umpan balik dari departemen terkait.

5.2 Pengecualian (Exceptions)

Setiap pengecualian terhadap kebijakan ini harus disetujui oleh Tim Infosec sebelum diimplementasikan.

5.3 Ketidakpatuhan (Non-Compliance)

Karyawan yang melanggar kebijakan ini akan dikenakan tindakan disipliner, hingga dan termasuk pemutusan hubungan kerja.

6. Standar, Kebijakan, dan Proses Terkait

- Kebijakan Perlindungan Data
- Kebijakan Akses Minimum
- Kebijakan Kata Sandi

7. Definisi dan Istilah

Lihat SANS Glossary untuk definisi lengkap tentang istilah yang digunakan, seperti "Proprietary Information" dan "Spam" :

a. Spam

Electronic junk mail or junk newsgroup postings.

b. Proprietary Information

Proprietary information is that information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.