Template Kebijakan Keamanan Informasi

Pengantar.

Risiko pencurian data, penipuan, dan pelanggaran keamanan dapat berdampak buruk pada sistem, infrastruktur teknologi, dan reputasi organisasi. Akibatnya, [nama organisasi] telah membuat kebijakan ini untuk menetapkan langkah-langkah keamanan yang diterapkan untuk memastikan data dan aset informasi tetap aman dan terlindungi.

Tujuan.

Tujuan dari kebijakan ini adalah untuk:

1. melindungi data dan infrastruktur [nama organisasi],
2. menyediakan pedoman langkah-langkah keamanan informasi,
3. menetapkan aturan untuk penggunaan teknologi informasi bagi organisasi dan pribadi, dan
4. membuat acuan bagi sanksi dan tindakan disipliner organisasi untuk pelanggaran kebijakan.

Cakupan.

Kebijakan ini berlaku untuk semua pekerja jarak jauh [nama organisasi], karyawan tetap, dan paruh waktu, kontraktor, relawan, pemasok, magang, dan / atau individu yang memiliki akses ke sistem elektronik, informasi, perangkat lunak, dan / atau perangkat keras organisasi. .

Data Rahasia.

[Nama organisasi] mendefinisikan "data rahasia" sebagai:

Contoh

1. Informasi yang belum dirilis dan diklasifikasikan.
2. Informasi pelanggan, pemasok, dan pemegang saham.
3. Prospek pelanggan dan data terkait penjualan.
4. Paten, proses bisnis, dan / atau teknologi baru.
5. Kata sandi, tugas, dan informasi pribadi karyawan.
6. Kontrak organisasi dan catatan hukum.

Keamanan Perangkat Penggunaan Kantor

Untuk memastikan keamanan semua perangkat dan informasi yang dikeluarkan organisasi, karyawan [nama organisasi] diwajibkan untuk:

1. Menjaga semua perangkat yang dikeluarkan organisasi, termasuk tablet, komputer, dan perangkat seluler, dilindungi kata sandi (minimal 8 karakter).
2. Amankan semua perangkat yang relevan sebelum meninggalkan meja mereka.
3. Dapatkan otorisasi dari Manajer Kantor dan / atau Manajer Inventaris sebelum menghapus perangkat dari lokasi organisasi.
4. Menahan diri dari berbagi kata sandi pribadi dengan rekan kerja, kenalan pribadi, personel senior, dan / atau pemegang saham.
5. Perbarui perangkat secara rutin dengan perangkat lunak keamanan terbaru.

Pemakaian pribadi.

[Nama organisasi] memahami bahwa karyawan mungkin diharuskan menggunakan perangkat pribadi untuk mengakses sistem organisasi. Dalam kasus ini, karyawan harus melaporkan informasi ini kepada manajemen untuk tujuan penyimpanan catatan.

Untuk memastikan sistem organisasi terlindungi, semua karyawan diwajibkan untuk:

1. Jaga agar semua perangkat dilindungi kata sandi (minimal 8 karakter).
2. Pastikan semua perangkat pribadi yang digunakan untuk mengakses sistem terkait organisasi dilindungi kata sandi.
3. Instal perangkat lunak antivirus berfitur lengkap.
4. Perbarui perangkat lunak antivirus secara teratur.
5. Kunci semua perangkat jika dibiarkan tanpa pengawasan.
6. Pastikan semua perangkat dilindungi setiap saat.
7. Selalu gunakan jaringan yang aman dan pribadi.

Keamanan Email.

Melindungi sistem email adalah prioritas tinggi karena email dapat menyebabkan pencurian data, penipuan, dan membawa perangkat lunak berbahaya seperti worm dan bug.

Oleh karena itu, [nama organisasi] mewajibkan seluruh karyawan untuk:

1. Verifikasi keabsahan setiap email, termasuk alamat email dan nama pengirim.
2. Hindari membuka email yang mencurigakan, lampiran, dan mengklik link.
3. Cari kesalahan tata bahasa yang signifikan.
4. Hindari judul dan tautan clickbait.
5. Hubungi departemen TI mengenai email yang mencurigakan.

Mentransfer Data.

[Nama organisasi] mengetahui risiko keamanan dari transfer data rahasia secara internal dan / atau eksternal.

Untuk meminimalkan kemungkinan pencurian data, kami menginstruksikan semua karyawan untuk:

1. Menahan diri dari mentransfer informasi rahasia kepada karyawan dan pihak luar.
2. Hanya transfer data rahasia melalui jaringan [nama organisasi].
3. Dapatkan otorisasi yang diperlukan dari manajemen senior.
4. Verifikasi penerima informasi dan pastikan mereka memiliki tindakan pengamanan yang tepat.
5. Mematuhi undang-undang perlindungan data dan perjanjian kerahasiaan [nama organisasi].
6. Segera beritahu departemen TI jika ada pelanggaran, perangkat lunak berbahaya, dan / atau penipuan.

Tindakan Disiplin.

Pelanggaran kebijakan ini dapat mengakibatkan tindakan disipliner, hingga dan termasuk pemutusan hubungan kerja.

Sanksi disipliner [Nama organisasi] didasarkan pada beratnya pelanggaran. Pelanggaran yang tidak disengaja hanya memerlukan peringatan lisan, pelanggaran yang sering terjadi dengan sifat yang sama dapat menyebabkan peringatan tertulis, dan pelanggaran yang disengaja dapat menyebabkan penangguhan dan / atau penghentian, tergantung pada keadaan kasus.