Buku Panduan Keamanan Informasi

Afiliasi：

Nama：

Kontak untuk Sistem Informasi

Departemen：

No. Telepon：　　-　　-

No. Telepon：　　-　　-

Kebijakan Keamanan Informasi

Sesuai dengan filosofi kami, yaitu “mengejar perdamaian, menghormati kemanusiaan, dan berkontribusi terhadap masyarakat setempat, dengan berpusat pada pelanggan”, AEON menyadari pentingnya keamanan informasi, melindungi informasi penting dari berbagai ancaman, dan berkontribusi terhadap kehidupan yang aman dan sejahtera. Selain itu, AEON menganggap informasi yang beragam sebagai aset vital untuk pengembangan kegiatan bisnisnya dan penciptaan nilai tambah, mengelola informasi ini dengan benar dan aman, dan membangun hubungan kepercayaan yang kokoh dengan semua pihak yang terkait dengan AEON, termasuk pelanggan, masyarakat setempat, mitra bisnis, dan pemegang saham. Untuk mencapai tujuan ini, kami menyajikan Kebijakan Dasar Keamanan Informasi ini sebagai pedoman bagi semua karyawan AEON untuk menjaga tingkat kesadaran yang tinggi mengenai keamanan informasi dan bertindak sesuai dengan itu.

Ditetapkan pada 1 September 2019
AEON Co., Ltd.

Inisiatif Keamanan Informasi

AEON melaksanakan kegiatan-kegiatan berikut untuk menerapkan secara menyeluruh Kebijakan Dasar Keamanan Informasi.

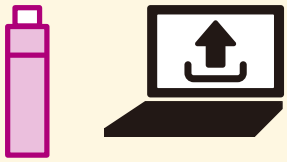
1. Membangun kerangka kerja untuk memelihara dan meningkatkan keamanan informasi secara berkelanjutan.
2. Menyusun peraturan untuk memastikan keamanan informasi dan mematuhinya.
3. Melakukan penilaian risiko yang tepat dan menerapkan langkah-langkah antisipasi yang wajar dan sesuai untuk melindungi informasi.
4. Menyelenggarakan pelatihan keamanan informasi yang sesuai kepada karyawan dan pihak lain untuk meningkatkan kesadaran.
5. Mematuhi semua undang-undang, peraturan, dan kontrak dengan pelanggan, mitra bisnis, dan karyawan, serta menangani informasi dengan tepat.
6. Menetapkan kerangka kerja untuk merespons dengan cepat dan efektif terhadap insiden atau pelanggaran keamanan informasi.
7. Berusaha untuk mempertahankan tingkat keamanan informasi yang setara atau lebih tinggi dari AEON saat melakukan outsourcing operasi.
8. Meminimalkan dampak bencana dan serangan siber serta berupaya memastikan kelangsungan bisnis melalui kegiatan keamanan informasi.
9. Melakukan inspeksi dan audit berkala serta non-berkala terhadap kegiatan-kegiatan di atas dan mengupayakan perbaikan berkelanjutan.
10. Pelanggaran terhadap Kebijakan Dasar ini dan peraturan internal tentang keamanan informasi akan dikenakan sanksi sesuai dengan Peraturan Kerja.

Aturan Keamanan Dasar

Hal-hal yang dilarang

Menggunakan perangkat selain yang dipinjamkan oleh perusahaan

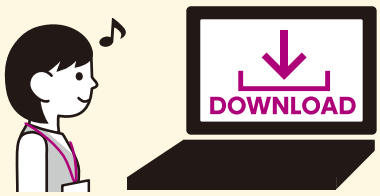
Membawa keluar perangkat yang dipinjamkan oleh perusahaan tanpa izin



Contoh: USB flash drive

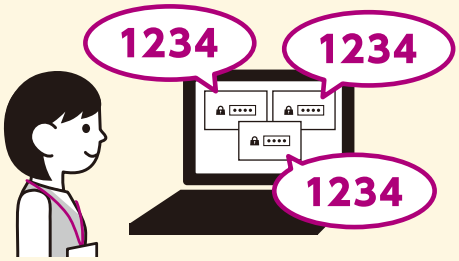
Menggunakan media penyimpanan eksternal tanpa persetujuan sebelumnya

Browsing internet untuk keperluan pribadi selama jam kerja

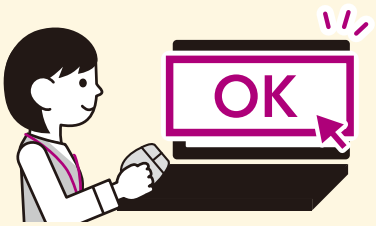


Menggunakan perangkat lunak atau layanan yang tidak diizinkan

Hal-hal yang perlu diperhatikan



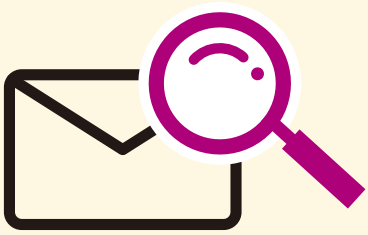
Menggunakan kata sandi yang sama



Mengeklik ‘OK’ dengan ringan tanpa verifikasi

Saat Menggunakan Email

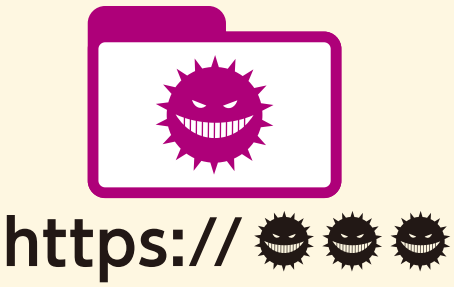
Hal-hal yang perlu diperhatikan saat menerima email



Contoh yang benar:
○○@aeonpeople.biz

Pastikan alamat penerima benar

Jangan membalas atau meneruskan email sembarangan



Jangan membuka file atau tautan yang mencurigakan

Hal-hal yang perlu diperhatikan saat menerima email

Periksa dengan teliti isi dan penerima

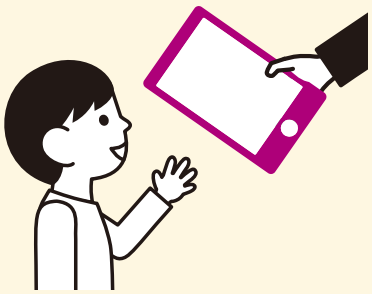
Gunakan kata sandi pada file untuk informasi rahasia

Saat bekerja dari jarak jauh (bekerja di luar kantor)

Hal-hal yang dilarang

Terhubung ke jaringan Wi-Fi publik

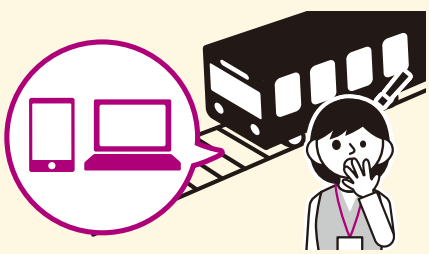
Pengungkapan informasi data/rekaman secara ceroboh ke publik



Keluarga menggunakan peralatan pinjaman dari perusahaan

Hal-hal yang perlu diperhatikan

Kunci perangkat dengan kata sandi saat meninggalkan meja Anda



Selalu bawa perangkat Anda bersama Anda saat bepergian

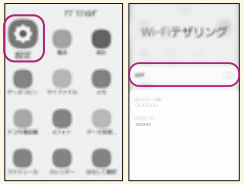
Penting Langkah-langkah yang harus dilakukan jika terinfeksi virus

Langkah awal

Pertama, segera putuskan koneksi dari jaringan!

Mencabut kabel LAN

Memutuskan koneksi Wi-Fi



Mematikan fitur tethering pada smartphone

Langkah terakhir OFF! Matikan daya

Melaporkan insiden

Laporkan ke perusahaan secepatnya

Laporan / Informasi / Konsultasi

Jangan mencoba menyelesaikan masalah sendiri!

Jika Anda tidak dapat menghubungi siapa pun, tetap tenang dan tunggu hingga terhubung!

Mempertahankan kondisi

Pertahankan keadaan saat ini untuk penyelidikan

Jangan mengoperasikan komputer

*Pada prinsipnya, jangan matikan daya

Segera Laporkan dalam Kasus Ini

Segera laporkan ke kontak darurat jika hal berikut terjadi

Perilaku abnormal pada komputer

Reboot berulang

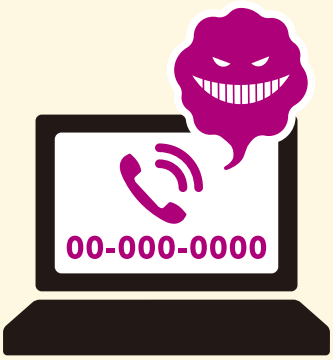
Muncul pesan tidak dikenal

Jendela tidak dapat ditutup

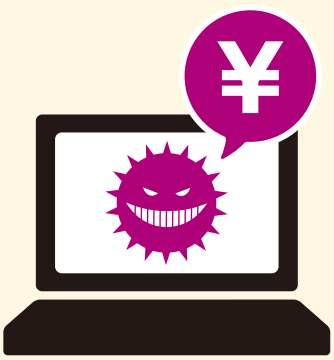
File terenkripsi dan tidak dapat diakses

Data yang disimpan hilang/rusak

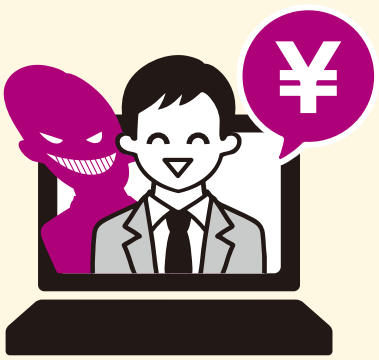
Kontak dari pihak ketiga yang berniat jahat



Menampilkan nomor telepon yang mendesak untuk menghubungi



Permintaan uang sebagai imbalan untuk pemulihan



Permintaan pembayaran dengan menyamar sebagai mitra bisnis

Proses Pelaporan

Deteksi gangguan sistem

Unit bisnis/perusahaan/toko

Perusahaan pemeliharaan dan operasi sistem

Bagian urusan umum di perusahaan

AEON Smart Technology Co., Ltd.

Bagian sistem di perusahaan (termasuk finansial)

Laporan insiden (pemahaman situasi)

Perencanaan ICT (Kantor Keamanan) AEON Co., Ltd.
•Bagian Urusan Umum

Pemberitahuan

Konfirmasi dampak (pemahaman dampak)

Anggota tim tanggap krisis

Pembentukan markas tanggap krisis sesuai kebutuhan

Manajer toko/kepala bagian (manajer sistem)

Pemberitahuan

Pemberitahuan

Presiden di perusahaan/
pejabat penanggung jawab sistem
Bagian terkait di AEON Co., Ltd.

Ketua/presiden direktur/wakil presiden direktur/
pejabat eksekutif bisnis

Pelaksanaan langkah tanggapan

30 menit

30 menit