DO'S & DONT'S
PT PLN ENJINIRING

Sistem Manajemen Keamanan Informasi

www.plne.co.id

1

PENANGANAN INFORMASI RAHASIA

THINGS TO DO

- ✓ Mengajukan peminjaman/akses informasi Perusahaan sesuai dengan Kebijakan;
- ✓ informasi dan/atau dokumen rahasia wajib dikendalikan sesuai klasifikasi dan sesuai kebijakan yang berlaku di Perusahhaan;
- ✓ Menyimpan seluruh informasi dan/atau dokumen rahasia dalam bentuk Hardcopy dan disimpan ditempat yang aman dan terkunci;
- ✓ Memberi password pada informasi dan/atau dokumen rahasia yang bersifat softcopy;
- ✓ Hanya mendistribusikan informasi dan/atau dokumen rahasia kepada pihak yang mempunyai otorisasi;
- ✓ Memusnahkan seluruh informasi dan/atau dokumen rahasia yang bersifat Kritikal namun sudah tidak digunakan.

THINGS TO AVOID

- ✗ Membuang informasi dan/atau dokumen rahasia di tempat sampah tanpa dihancurkan terlebih dahulu;
- ✗ Memberikan akses ke informasi dan/atau dokumen rahasia kepada pihak yang tidak terotorisasi tanpa terlebih dahulu mendapatkan izin dari pemilik informasi;
- ✗ Memperbanyak dan/atau mendistribusikan informasi dan/atau dokumen rahasia tanpa Izin;
- ✗ Meninggalkan informasi dan/atau dokumen rahasia pada mesin printer dan/atau fotocopy.

2

PENGENDALIAN ASET & PIHAK KETIGA

PLN Enjiniring

THINGS TO DO

- ✓ Mengembalikan asset Perusahaan pada saat berakhirnya kontrak atau masa kerja atau pada saat karyawan mengundurkan diri;
- ✓ Personil vendor yang mengakses informasi dan/atau dokumen rahasia dan/atau masuk ke area Perusahaan, wajib menandatangani Perjanjian Kerahasiaan (NDA);
- ✓ Pengguna asset bertanggung jawab atas pengamanan dan perlindungan asset secara fisik;
- ✓ Adanya kontrak dan/atau SLA sesuai layanan yang diberikan oleh Vendor atau Pihak Ketiga;
- ✓ Memastikan kesesuaian kepatuhan dengan Perjanjian;
- ✓ Perubahan dalam Perjanjian atau kontrak harus dikendalikan dan diinformasikan kepada Perusahaan.

THINGS TO AVOID

- ✗ Meninggalkan asset di area public tanpa pengawasan;
- ✗ Tidak mengembalikan asset inventaris Perusahaan setelah berakhirnya kontrak atau masa kerja atau pada saat karyawan mengundurkan diri;
- ✗ Pihak Ketiga tidak mematuhi kebijakan Perusahaan;
- ✗ Tidak ada Perjanjian Kerahasiaan (NDA) dengan Pihak Ketiga.

3

PENGENDALIAN MOBILE DEVICE & TELEWORKING

PLN Enjiniring

THINGS TO DO

- ✓ Melakukan pendataan user yang mendapatkan akses VPN dan penggunaan mobile device milik pribadi dan/atau Perusahaan;
- ✓ Memberikan pengamanan terhadap mobile device (Password, antivirus, dll).

THINGS TO AVOID

- ✗ Tidak ada kontrol terhadap perangkat pribadi yang digunakan untuk bekerja;
- ✗ Tidak memberikan pengamanan terhadap mobile device;
- ✗ Menggunakan jaringan yang tidak aman saat melakukan kegiatan teleworking (akses ke jaringan Perusahaan).

4

PENGGUNAAN REMOVABLE MEDIA

PLN Enjiniring

THINGS TO DO

- ✓ Removable Media hanya diperbolehkan untuk pemindahan informasi dan pengguna;
- ✓ Setiap Removable Media wajib untuk dilakukan scan menggunakan anti-virus;
- ✓ Setiap Personil bertanggung jawab atas perlindungan dan penanganan informasi sesuai dengan klasifikasi informasi yang terkandung di dalamnya.

THINGS TO AVOID

- ✗ Menyimpan Informasi dan/atau dokumen Rahasia secara Permanen pada Removable Media yang berukuran kecil (USB, Memory Card);
- ✗ Tidak memberikan Password pada informasi dan/atau dokumen rahasia yang tersimpan pada Removable Media.

5

PENGGUNAAN AKSES DAN TANGGUNG JAWAB PENGGUNA

PLN Enjiniring

THINGS TO DO

- ✓ Mendaftarkan hak akess khusus dan menghapus akses sesuai dengan ketentuan;
- ✓ Mengunci layer PC/Notebook apabila akan ditinggalkan;
- ✓ Mematikan PC/Notebook apabila sudah tidak digunakan;
- ✓ Memberikan otorisasi pada informasi kritikal yang tersimpan pada perangkat pribadi;
- ✓ Mengaktifkan password pada PC/Notebook dengan menggunakan standar yang berlaku (terdiri dari 8 karakter, kombinasi huruf besar, huruf kecil, angka dan karakter spesial;
- ✓ Mengubah password secara berkala sesuai kebijakan Perusahaan;
- ✓ Mengganti Password setiap ada indikasi pencurian password.

THINGS TO AVOID

- ✗ Menulis Password dan menempelkan di tempat publik;
- ✗ Memberitahukan password pada pihak lain;
- ✗ Menggunakan fitur “Remember Password” pada browser;
- ✗ Melakukan akses jaringan menggunakan fasilitas publik;
- ✗ Password yang dibuat mudah ditebak (contoh: nama, nomor telepon, tanggal dan bulan lahir) dan bukan urutan angka atau karakter yang sama atau berurut (contoh: 123456, abcdef, abc123)

6

PENGGUNAAN AKSES DAN TANGGUNG JAWAB PENGGUNA

PLN Enjiniring

THINGS TO DO

- ✓ Merapihkan area kerja pada saat akan ditinggalkan;
- ✓ Menghapus Informasi Rahasia yang terdapat pada papan tulis dalam ruangan meeting tanpa dihapus;
- ✓ Memastikan tidak ada Informasi Rahasia yang ditinggalkan pada mesin printer dan/atau fotokopi.

THINGS TO AVOID

- ✗ Meninggalkan Informasi Rahasia baik Hardcopy maupun Softcopy di Removable Media atau di PC/Notebook dan ditinggalkan tanpa adanya pengawasan dari Pemilik asset.

7

KEAMANAN FISIK DAN LINGKUNGAN

PLN Enjiniring

THINGS TO DO

- ✓ Seluruh personil pihak ketiga dan/atau tamu yang memasuki area Perusahaan wajib mengisi buku tamu dan menyebutkan kepetingannya;
- ✓ Tidak memperkenankan personil Pihak Ketiga dan/atau tamu memasuki area terbatas dan tertutup tanpa mengiukuti kebijakan dan tanpa didampingi PIC Perusahaan;
- ✓ Seluruh personil pihak ketiga dan/atau tamu yang akan memasuki ruangan server wajib didampingi oelh tim IT Perusahaan dari sejak masuk hingga keluar dari ruangan;
- ✓ Personil pihak ketiga dan/atau tamu bekerja di area aman sesuai kebijakan Perusahaan dan tidak diperbolehkan mengambil gambar dan/atau video di area terbatas termasuk di dalam Ruangan Server.

THINGS TO AVOID

- ✗ Meminjamkan ID Card atau Access Card kepada siapapun;
- ✗ Membiarkan personil pihak ketiga dan/atau tamu masuk ke area terbatas tanpa didampingi oleh PIC Perusahaan;
- ✗ Membiarkan personil pihak ketiga dan/atau tamu bekerja di area terbatas tanpa pengawasan dari PIC Perusahaan.

8

EMAIL

PLN Enjiniring

THINGS TO DO

- ✓ Memeriksa isi dan lampiran dari email yang akan dikirimkan;
- ✓ Memastikan alamat email yang dituju sesuai;
- ✓ Memberikan password pada file yang berisi Informasi Rahasia, diman password wajib dikirimkan melalui email atau media terpisah;
- ✓ Menghapus seluruh email yang mencurigakan.

THINGS TO AVOID

- ✗ Mengirimkan email dan password dalam waktu yang bersamaan dalam 1 (satu) email;
- ✗ Membalas email sampah (spam)
- ✗ Klik link atau download file pada email yang mencurigakan / spam / tidak dikenal.

9

KEBIJAKAN & KOMITMEN SISTEM MANAJEMEN TERINTEGRASI PT PLN ENJINIRING

PLN Enjiniring

PT PLN Enjiniring sesuai dengan visi dan misi, serta untuk mencapai tujuan, sasaran dan kinerja perusahaan, menetapkan kebijakan dan komitmen dalam menerapkan Sistem Manajemen Terintegrasi (SMT) sebagai berikut:

1. Manajemen PT PLN Enjiniring menetapkan kebijakan Sistem Manajemen Terintegrasi yang mencakup Sistem Manajemen Mutu (SMM) sesuai ISO 9001:2015, Sistem Manajemen Anti Penyuapan (SMAP) sesuai ISO 37001:2016, Sistem Manajemen Keselamatan dan Kesehatan Kerja (SMK3) sesuai dengan PP No 50 Tahun 2012, Manajemen Risiko sesuai ISO 31000:2018, Sistem Manajemen Keamanan Informasi (SMKI) sesuai ISO 27001:2022, Sistem Manajemen Pengamanan (SMP) sesuai Peraturan Kapolri No.04 Tahun 2020, Sistem Manajemen Kepatuhan (SMK) sesuai ISO 19600:2014, dan Sistem Manajemen Kelangsungan Usaha (SMKU) sesuai ISO 22301:2019 dan memastikan kebijakan tersebut sesuai dengan sifat dan skala kemampuan operasional PT PLN Enjiniring.
2. Seluruh jajaran manajemen dan karyawan PT PLN Enjiniring berkomitmen untuk:
   a. Memenuhi persyaratan sistem manajemen sesuai dengan standar atau peraturan yang berlaku
   b. Menyediakan kerangka kerja untuk menetapkan, mengkaji, meninjau, dan mencapai sasaran Sistem Manajemen Terintegrasi
   c. Peningkatan dan perbaikan berkelanjutan terhadap Sistem Manajemen Terintegrasi

10

KEBIJAKAN & KOMITMEN SISTEM MANAJEMEN TERINTEGRASI PT PLN ENJINIRING

3. Seluruh jajaran manajemen dan karyawan PT PLN Enjiniring berkomitmen untuk menerapkan secara konsisten dan memastikan kesesuaian terhadap ketentuan serta peraturan perundang-undangan yang berlaku terhadap:
   3.1. Sistem Manajemen Mutu (SMM) sesuai ISO 9001:2015 untuk menjamin kepuasan pihak berkepentingan dengan menghasilkan produk yang memenuhi syarat mutu yang berlaku dengan menerapkan prinsip tepat waktu, tepat mutu dan tepat biaya untuk menjaga loyalitas pihak berkepentingan.
   3.2. Sistem Manajemen Anti Penyuapan (SMAP) sesuai ISO 37001:2016 yang:
      a) melarang praktik penerimaan maupun pemberian suap
      b) mendorong peningkatan kepedulian dengan itikad baik, atau atas dasar keyakinan yang wajar, tanpa takut tindakan balasan;
      c) menjelaskan wewenang dan kemandirian dari fungsi kepatuhan anti penyuapan
      d) menjelaskan konsekuensi jika tidak sesuai dengan kebijakan anti penyuapan
   3.3. Mengelola risiko perusahaan sesuai ISO 31000:2018 Pedoman Manajemen Risiko untuk melindungi perusahaan dari risiko yang dapat menghambat pencapaian tujuan perusahaan.

11

KEBIJAKAN & KOMITMEN SISTEM MANAJEMEN TERINTEGRASI PT PLN ENJINIRING

3.4. Sistem Manajemen Keselamatan dan Kesehatan Kerja (SMK3) sesuai PP No 50 Tahun 2012 untuk memastikan setiap tenaga kerja dan pihak berkepentingan merasa aman, nyaman dan sehat di lingkungan PT PLN Enjiniring dengan melakukan identifikasi dan pengendalian semua potensi bahaya serta aspek-aspek dampak lingkungan yang terkandung pada seluruh aktifitas operasional perusahaan dan menyediakan sarana dan prasaranan K3 yang memadai.
3.5. Sistem Manajemen Pengamanan sesuai Peraturan Kapolri No 04 Tahun 2020.
3.6. Sistem Manajemen Keamanan Informasi sesuai ISO 27001:2022 untuk menyediakan layanan informasi yang berorientasi pada kepuasan pengguna serta memenuhi aspek keamanan, keandalan, dan efisiensi.
3.7. Sistem Manajemen Kepatuhan sesuai ISO 19600:2014 untuk membantu perusahaan dalam mempertahankan integritas dan menghindari atau meminimalkan masalah ketidakpatuhan
3.8. Sistem Manajemen Kelangsungan Usaha ISO 22301:2019 untuk membantu perusahaan menjadi lebih siap dalam menghadapi gangguan dan bencana serta menjaga bisnis tetap berjalan dalam situasi sulit

Kebijakan Sistem Manajemen Terintegrasi (SMT) disampaikan untuk dipahami dan dilaksanakan oleh semua pihak yang bekerja di PT PLN Enjiniring sesuai dengan tugas dan tanggungjawabnya masing-masing dengan memperhatikan prinsip-prinsip Tata kelola Perusahaan Yang Baik (GCG), Risiko dan Kepatuhan (GRC) Kebijakan SMT secara berkala akan dievaluasi agar senantiasa sesuai dengan tujuan perusahaan maupun peraturan berlaku.

12

13