1. **Struktur dokumen IS/IT Guideline**
2. Front Matter
3. Title :

“Data Security Policy: Workstation Full Disk Encryption”

1. Description :

Kebijakan ini dimaksudkan untuk bertindak sebagai pedoman bagi organisasi yang ingin menerapkan atau memperbarui enkripsi disk lengkap dengan kebijakan kontrol.

1. Sponsor :

PT Asuransi Jasa Indonesia yang akan memberikan perlindungan sepenuhnya atas risiko peluncuran dan operasional PT Pasifik Satelit Nusantara.

1. Authority

Adapun authority atau pengesahan kebijakkan ini dilakukan oleh :

|  |  |  |  |
| --- | --- | --- | --- |
| Disiapkan Oleh  Tanggal :  TTD | Disetujui Oleh  Tanggal :  TTD | Disetujui Oleh  Tanggal :  TTD | Disetujui Oleh  Tanggal :  TTD |
| Nama :  Jabatan : | Nama :  Jabatan : | Nama :  Jabatan : | Nama :  Jabatan : |

1. Level :

Kebijakan ini berlaku untuk level organisasi perusahaan setingkat dengan divisi.

1. Goal :

Kebijakan ini dibuat untuk melindungi keamanan data-data yang ada di perusahaan sesuai dengan alignment goals AG07 Security of Information, Processing Infrastructure and Applications, and Privacy pada COBIT 2019.

1. Purpose

Tujuannya adalah mewujudkan perlindungan data yang sesuai dengan Standard Policy yang berlaku di dalam perusahaan untuk memberikan rasa aman terhadap karyawan perusahaan dalam bisnis perusahaan.

1. Scope
2. Semua workstation PT Pasifik Satelit Nusantara pada desktop dan laptop (tergantung pada jenis data yang Anda pegang dan beberapa keamanan fisik organisasi menyesuaikan ini hanya untuk menutupi laptop).
3. Semua mesin virtual PT Pasifik Satelit Nusantara.
4. Pengecualian: Jika ada bisnis yang perlu dibebaskan dari kebijakan ini (terlalu mahal, terlalu rumit, berdampak buruk pada persyaratan bisnis lainnya) penilaian risiko harus dilakukan dan disahkan oleh Manajer Keamanan.
5. Roles and Responsibility

Departmen IT.

1. Definitions

Dalam keilmuan (ilmiah), fakta dikumpulkan untuk menjadi data. Data kemudian diolah sehingga dapat diutarakan secara jelas dan tepat sehingga dapat dimengerti oleh orang lain yang tidak langsung mengalaminya sendiri, hal ini dinamakan [deskripsi](https://id.wikipedia.org/wiki/Deskripsi).

Keamanan adalah keadaan bebas dari bahaya. Istilah ini bisa digunakan dengan hubungan kepada kejahatan, segala bentuk kecelakaan, dan lain-lain.

Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di dekripsi (kebalikan dari proses enkripsi) dahulu.

1. Revision History :

Berdasarkan dokumen yang tercatat pada kebijakan PT Pasifik Satelit Nusantara ini, belum ada perubahan atau riwayat revisi.

1. Effective Date :

Tanggal efektif kebijakan ini terlaksana mulai dari 22 Februari 2019, tepat setelah Satelit Nusantara Satu diluncurkan.

1. Review Plan
2. 29 Juni 2016 telah dilaksanakan Rapat Persiapan Pelaksanaan Kontrak membahas tentang jadwal pelaksanaan kegiatan pembangunan SMFR Transportable dan persiapan Survei Lapangan di 24 Unit Pelaksana Teknis (UPT) dan 64 Kantor Pos dan Program Mutu.
3. Tahun 2016 Subdit Monitoring dan Penertiban PPI, Direktorat Pengendalian SDPPI telah melakukan Kegiatan Penertiban terpadu Alat dan Perangkat Telekomunikasi di 6 (enam) lokasi.
4. 19 Januari 2019 telah dilaksanakan uji static fire pada Roket Falcon 9.
5. Body
6. Guideline checklists, multiple with content
7. Start condition

Data Security Policy: Workstation Full Disk Encryption adalah produk standar.

1. Forward method

BIOS akan dikonfigurasikan dengan kata sandi aman (sebagaimana ditentukan oleh kebijakan kata sandi) yang disimpan oleh TI. Urutan boot akan diperbaiki ke HDD terenkripsi.

1. Check done item

Sinkronisasi dengan kredensial Windows akan dikonfigurasikan sehingga lingkungan pra boot dicocokkan dengan pengguna kredensial dan hanya satu log masuk diperlukan.

1. Reversion method

Jika penggantian diperlukan oleh pengguna untuk pemeliharaan atau penggunaan darurat, meja bantuan bisa otentikasi pengguna dan kemudian berikan kata sandi untuk BIOS. Tujuannya adalah untuk menghindari penyerang booting dingin dan menyerang sistem.

1. End condition

Lingkungan pra-booting akan digunakan untuk otentikasi. Kredensial akan digunakan untuk mengotentikasi pengguna sesuai dengan lengkap sesuai kebutuhan kebijakan keamanan kata sandi. (Beberapa perusahaan memiliki persyaratan untuk menggunakan dua faktor, dan ini seharusnya tercermin di sini sesuai kebutuhan).