1. **Struktur dokumen IS/IT Policy**
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. Policy Statement, multiple with any type of :
7. Obligation statemement

* Semua perangkat dalam ruang lingkup akan mengaktifkan enkripsi disk lengkap.
* Kebijakan penggunaan PT Pasifik Satelit Nusantara yang dapat diterima (AUP) dan pelatihan kesadaran keamanan harus mengharuskan pengguna untuk memberi tahu jika mereka curiga mereka tidak mematuhi kebijakan ini sesuai AUP.
* Pelatihan AUP dan kesadaran keamanan harus mengharuskan pengguna untuk memberi tahu tentang perangkat apa pun yang hilang atau dicuri.
* Kebijakan enkripsi harus dikelola dan kepatuhan divalidasi dengan lengkap. Mesin perlu melaporkan ke infrastruktur manajemen pusat untuk memungkinkan catatan audit untuk menunjukkan kepatuhan sebagaimana diperlukan.
* Apabila manajemen tidak memungkinkan dan enkripsi mandiri dikonfigurasikan (hanya sekali disetujui oleh penilaian risiko), maka pengguna perangkat harus memberikan salinan kunci enkripsi aktif ke IT.
* Memiliki hak untuk mengakses perangkat terenkripsi apa pun untuk keperluan penyelidikan, pemeliharaan atau tidak adanya karyawan dengan akses sistem file primer. AUP dan pelatihan kesadaran keamanan akan memberi tahu pengguna tentang persyaratan ini. (Tergantung pada AUP Anda, atau perjanjian dengan karyawan Anda akan ingin mengubah sikap persyaratan kebijakan ini).
* Teknologi enkripsi harus dikonfigurasi sesuai dengan praktik terbaik industri untuk dikeraskan terhadap serangan.
* Semua peristiwa terkait keamanan akan dicatat dan diaudit dengan lengkap untuk mengidentifikasi akses yang tidak pantas di sistem atau penggunaan berbahaya lainnya.
* Help desk lengkap akan diizinkan untuk mengeluarkan tantangan / respons out-of-band untuk memungkinkan akses ke sistem jika terjadi kegagalan, kehilangan kredensial atau persyaratan pemblokiran bisnis lainnya. Tantangan / respons akan diberikan hanya jika identitas pengguna dapat ditetapkan menggunakan atribut tantangan dan respons didokumentasikan dalam kebijakan kata sandi.
* (Beberapa perusahaan mungkin memiliki persyaratan untuk mempraktikkan pendekatan berjenjang untuk keamanan data. Ini mungkin melibatkan serangkaian pengguna yang memiliki data yang sangat sensitif dan membutuhkan keamanan yang lebih besar. Anda dapat menghapus ini jika ini bukan persyaratan bisnis Anda). Sekelompok pengguna data / VIP yang sensitif akan diidentifikasi oleh kebijakan data yang dibatasi. Pengguna dalam grup ini akan memerlukan anggota dari (mis. Manajemen Senior atau TI) otorisasi untuk perubahan utama atau respons tantangan. Bantuan desk tidak akan diizinkan untuk mengakses sistem tersebut tanpa otorisasi. Sistem ini diidentifikasi memiliki akses ke sangat sensitif, data penggunaan terbatas dan memiliki persyaratan untuk pemisahan tugas. Di mana diidentifikasi oleh otentikasi dan kebijakan data terbatas, suatu sistem / pengguna akan diminta untuk menggunakan dua faktor otentikasi sesuai dengan standar yang ditentukan. Otentikasi akan terjadi di lingkungan pra-boot.
* Perubahan konfigurasi harus dilakukan melalui proses kontrol perubahan, mengidentifikasi risiko dan perubahan implementasi yang penting untuk manajemen keamanan

1. Prohobitive statement

* Karyawan tidak diperkenankan membawa dan menyambungkan peralatan dari luar kantor yang bukan milik perusahaan ke dalam jaringan perusahaan.
* Memindahkan data perusahaan ke pihak lain yang berpotensi merugikan perusahaan.
* Melakukan perubahan jaringan atau akses internet yang telah diteteapkan oleh perusahaan.

1. Restricted permissive statement

* Perusahaan melakukan penyebaran jaringan atau akses internet di beberapa wilayah dengan persetujuan daerah setempat dan sesuai dengan kesepakatan yang berlaku.

1. Necessity statement

* Perusahaan melakukan survei lapangan terhadap wilayah maupun daerah pelosok dengan melakukan pemasangan modem.

1. Impossibility statement

* Perusahaan dengan tanpa izin atau kesepakatan bersama melakukan pemutusan hak akses jaringan internet terhadap beberapa wilayah Indonesia.

1. Restricted possibility statement

* Perusahaan menerapkan secara detail mengenai penunjang akses jaringan yang telah bekerjasama dengan Telkomsel sesuai kesepakatan.