astragraphia
member of ASTRA

KEBIJAKAN KEAMANAN INFORMASI
(INFORMATION SECURITY POLICY)
PT Astra Graphia Tbk

www.astragraphia.co.id

1. Tujuan

1.1. Menyediakan kerangka kerja terkait pengelolaan keamanan informasi di Astragraphia.
1.2. Memahami tanggung jawab terkait upaya perlindungan aset informasi di Astragraphia.
1.3. Melindungi karyawan Astragraphia dalam hal terjadinya penyalahgunaan aset informasi, kerugian atau pengungkapan informasi yang tidak sah.
1.4. Meningkatkan kepedulian keamanan informasi di Astragraphia.

2. Ruang Lingkup

2.1. Kebijakan ini berlaku untuk seluruh karyawan Astragraphia dan semua orang yang memiliki akses atau mengelola informasi di Astragraphia.
2.2. Kebijakan keamanan informasi dan Teknologi Informasi mencakup semua sistem, otomatis dan manual, untuk tanggung jawab administrasi Astragraphia. Hal ini termasuk seluruh informasi, terlepas dari bentuk dan formatnya, yang dibuat atau digunakan untuk mendukung proses bisnis Astragraphia.
2.3. Menjelaskan kepada karyawan Astragraphia terkait pemahaman dan tanggung jawab mengenai masalah keamanan informasi dalam upaya melindungi aset informasi Astragraphia.
2.4. Pengguna/struktur organisasi yang diberikan tanggung jawab untuk mengelola kebijakan ini adalah Head of ITSS, Manajemen (Board of Directors and Chiefs), Astragraphia Managers, Information Owners, Information Security Manager, Manage Services, Karyawan Astragraphia dan pihak eksternal.
2.5. Kebijakan harus dikomunikasikan oleh manajer untuk seluruh karyawan Astragraphia dan semua orang lain yang memiliki akses dan mengelola terhadap informasi Astragraphia. Kebijakan keamanan ini adalah teknologi yang independen dan tidak termasuk standar pelaksanaan, proses dan prosedur.

3. Definisi

3.1. **ITSS** : Information Technology Shared Services
3.2. **Astragraphia** : PT Astra Graphia Tbk
3.3. **Information Security** : Upaya perlindungan terhadap keamanan aset informasi.
3.4. **Incident Management** : Pengelolaan cara penanganan terhadap insiden yang terjadi.

4. Penanggung Jawab

Dept. Head of ITSM bertanggung jawab untuk memastikan Kebijakan Information Security dilakukan dengan benar dan tepat sesuai dengan ketentuan dan prosedur yang berlaku.

5. Ketentuan

5.1. Persyaratan Kepatuhan

5.1.1. Persyaratan Kepatuhan

Kepatuhan terhadap kebijakan ini adalah wajib. Setiap karyawan harus memahami peran dan tanggung jawabnya terkait masalah keamanan informasi dan melindungi informasi Astragraphia. Kegagalan dalam mematuhi ini atau kebijakan keamanan lainnya yang mengakibatkan kompromi kerahasiaan, integritas, privasi, dan/atau ketersediaan Astragraphia dapat mengakibatkan tindakan disipliner atau tindakan lain yang sesuai dengan prosedur yang telah ditetapkan seperti yang ditetapkan dalam kebijakan ini, atau kebijakan lain atau kebijakan dan arahan Astragraphia lainnya yang relevan. Astragraphia akan mengambil setiap langkah yang diperlukan, termasuk tindakan hukum dan administratif, untuk melindungi asetnya dan telah membentuk posisi Manajer Keamanan Informasi untuk memantau kepatuhan terhadap masalah kebijakan.

5.1.1.1. Pengecualian terhadap Kebijakan

Kepala Manajemen Informasi harus terlebih dahulu menyetujui pengecualian terhadap kebijakan atau standar keamanan ini atau lainnya. Kasus bisnis yang menjelaskan alasan pengecualian harus didokumentasikan secara tertulis, dan diajukan untuk disetujui oleh Kepala Manajemen Informasi, dan juga harus disetujui dan disimpan oleh orang yang bertugas sebagai Manajer Keamanan Informasi. Orang atau organisasi yang dikecualikan pengecualian juga harus menerima secara tertulis semua risiko yang terkait dengan pengecualian.

5.1.1.2. Handling Penegakan dan Penanganan Pelanggaran

Setiap kompromi atau dugaan kompromi terhadap kebijakan ini harus dilaporkan ke manajemen yang tepat dan Manajer Keamanan Informasi. Semua pelanggaran terhadap kebijakan dan/atau standar keamanan patuh pada tindakan disipliner atau tindakan lain yang sesuai sesuai dengan kebijakan Astragraphia.

Laporan insiden keamanan yang menunjukkan tingkat risiko pelanggaran akan dilaporkan ke entitas yang bertanggung jawab. Hak akses untuk akun pengguna yang terlibat dalam kompromi dapat dicabut pada saat dugaan pelanggaran sedang dalam penyelidikan. Laporan pelanggaran otomatis yang dihasilkan oleh berbagai sistem keamanan akan diteruskan ke manajemen yang tepat dan Manager Keamanan Informasi untuk resolusi yang tepat waktu.

5.2. Tanggung Jawab organisasi dan fungsional

Berikut ini adalah penjelasan singkat tentang struktur organisasi yang bertanggung jawab untuk mengelola kebijakan ini.

- **Kepala Manajemen Informasi:** Menyetujui semua perubahan terhadap kebijakan dan standar keamanan, dan menyelesaikan masalah keamanan saat terjadi konflik dengan persyaratan bisnis.
- **Manajemen Astragraphia (Board of Directors dan Chief)**: Akan menetapkan dan mendukung kebijakan Astragraphia, termasuk kebijakan keamanan dan mengkomunikasikan kebijakan ini ke karyawan Astragraphia.

- **Manajer Astragraphia:** akan bertanggung jawab atas pelaksanaan kebijakan dan kepatuhan staf mereka di bawah pengawasan mereka dalam pelaksanaannya, sebagaimana tercantum dalam pernyataan misi mereka. Manajer harus mendidik staf mereka berkaitan dengan masalah keamanan informasi. Manajer akan menjelaskan masalahnya, mengapa kebijakan tersebut telah ditetapkan, dan peran apa yang dimiliki staf dalam menjaga aset informasi. Konsekuensi dari ketidakpatuhan juga harus dijelaskan.
- **Pemilik Informasi:** Manajer yang ditunjuk akan menjadi pemilik informasi untuk data dan alat yang mereka gunakan. Pemilik informasi bertanggung jawab untuk menentukan siapa yang harus memiliki akses terhadap sumber daya yang dilindungi di dalam yurisdiksinya, dan hak akses yang seharusnya (baca, perbarui, dll.). Hak akses ini harus sesuai dengan tanggung jawab pekerjaan pengguna. Pemilik informasi juga berkomunikasi dengan Information Security Manager persyaratan untuk melindungi datanya.
- **Manajer Keamanan Informasi:** Manajer Keamanan Informasi bertanggung jawab penuh untuk memastikan pelaksanaan, peningkatan, pemantauan dan penegakan Kebijakan Informasi IT dan Keamanan Informasi. Manajer Keamanan Informasi bertanggung jawab untuk memberikan arahan dan kepemimpinan kepada Astragraphia melalui rekomendasi kebijakan, standar dan proses untuk memastikan tingkat pengamanan yang tepat diterapkan, dan untuk memastikan kepatuhan terhadap kebijakan, standar dan proses ini. Manajer Keamanan Informasi bertanggung jawab untuk menyelidiki semua dugaan pelanggaran keamanan. Manajer Keamanan Informasi biasanya akan mewakili Astragraphia dalam semua masalah keamanan informasi dan akan mengkoordinasikan dan mengawasi kegiatan program keamanan dan proses pelaporan untuk mendukung kebijakan ini.
- **Pengelola Layanan** memiliki infrastruktur pengolahan data dan jaringan komputasi yang mendukung pemilik informasi. Merupakan tanggung jawab organisasi-organisasi ini untuk mendukung Kebijakan Keamanan Informasi dan menyediakan sumber daya yang dibutuhkan untuk meningkatkan dan memelihara tingkat kontrol keamanan informasi yang sesuai dengan Kebijakan Informasi IT dan Informasi**.**

  Pengelola Layanan memiliki tanggung jawab berikut sehubungan dengan keamanan informasi:
  - memastikan proses, kebijakan dan persyaratan diidentifikasi dan diterapkan relatif terhadap persyaratan keamanan yang ditentukan oleh lini bisnis;
  - memastikan pengendalian informasi yang tepat diterapkan untuk lini bisnis;
  - telah menugaskan tanggung jawab kepemilikan, berdasarkan penunjukan klasifikasi Astragraphia;
  - memastikan keikutsertaan Manajer Keamanan Informasi dan staf teknis dalam mengidentifikasi dan memilih pengendalian dan prosedur keamanan yang sesuai dan hemat biaya, dan untuk melindungi aset informasi;

- memastikan bahwa persyaratan keamanan yang sesuai untuk akses pengguna ke informasi otomatis;
- mendefinisikan file, basis data, dan perangkat fisik yang ditugaskan ke area tanggung jawab mereka;
- memastikan bahwa data penting dan rencana pemulihan dicadangkan dan disimpan di tempat yang aman;
- fasilitas penyimpanan, dan pemulihan media cadangan akan bekerja jika dan bila diperlukan;
- memastikan kepatuhan terhadap Astragraphia yang tepat dan peraturan dan pernyataan misi lainnya.

Karyawan Astragraphia: Merupakan tanggung jawab semua karyawan untuk melindungi informasi dan sumber daya Astragraphia, termasuk password, untuk mencatat varians dari prosedur yang telah ditetapkan, dan melaporkan varians atau insiden keamanan yang dicurigai kepada manajer yang sesuai dan Manajer Keamanan Informasi.

Pihak Eksternal: personil mitra bisnis, kontraktor, konsultan, vendor dan pihaklain, sejauh akses mereka sekarang atau masa lalu terhadap aset informasi AGIT juga tercakup dalam kebijakan ini.

5.3. **Rujukan Prosedur**

Prosedur merujuk pada ketentuan yang diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta perubahannnya ("UU ITE"), Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dan Transaksi Elektronik ("Permen Perlindungan Data Pribadi"), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ("PP PSTE").

5.4. **Kebijakan Teknologi Informasi dan Keamanan Informasi**

Semua informasi terlepas dari bentuk atau format yang dibuat, diperoleh atau digunakan untuk mendukung kegiatan bisnis Astragraphia, hanya boleh digunakan untuk bisnis Astragraphia. Informasi Astragraphia adalah aset dan harus dilindungi dari penciptaannya, melalui masa manfaatnya. Ini harus dijaga dengan aman, akurat, dan dapat diandalkan dan tersedia untuk penggunaan yang sah.

5.4.1. **Akuntabilitas Perorangan**

Akuntabilitas perorangan diperlukan saat mengakses semua sumber elektronik Astragraphia. Akses ke sistem komputer dan jaringan Astragraphia harus disediakan melalui penggunaan pengenal komputer unik yang ditetapkan secara individu, yang dikenal sebagai ID pengguna. Individu yang menggunakan sumber daya komputer Astragraphia hanya dapat mengakses sumber daya yang menjadi kewenangannya. Terkait dengan masing-masing user-ID adalah token otentikasi, seperti password, yang harus digunakan untuk mengotentikasi orang yang mengakses data, sistem atau jaringan. Kata sandi harus diperlakukan sebagai informasi rahasia, dan tidak boleh diungkapkan. Semua individu bertanggung jawab atas semua aktivitas yang dilakukan dengan ID pengguna mereka. Untuk perlindungan pengguna, dan untuk melindungi sumber daya

Astragraphia, ID pengguna tidak boleh dibagi.

5.4.2. **Kerahasiaan/Integritas/Ketersediaan**

- Semua informasi Astragraphia akan dilindungi dari akses yang tidak sah untuk membantu memastikan kerahasiaan informasi dan menjaga integritas.
- Informasi akan tersedia untuk penggunaan resmi bila diperlukan oleh pengguna dalam pelaksanaan tugasnya yang normal.
- Jadwal cadangan dan pemulihan akan ditetapkan pada sistem dan data tersebut untuk memastikan pemulihan tepat waktu jika terjadi pemadaman diperpanjang.

5.4.3. **Perlindungan Atas Data Pribadi**

Data Pribadi adalah data perseorangan tertentu yang disimpan, dirawat, dan dijaga kebenaran serta dilindungi kerahasiaannya. Astragraphia menghargai privasi setiap orang termasuk karyawan dan pelanggan dan Data Pribadi mereka, termasuk informasi digital tentang mereka yang disimpan oleh Astragraphia.
Astragraphia akan mengumpulkan dan menggunakan Data Pribadi sesuai dengan nilai-nilai Astragraphia, undang-undang yang berlaku dan menghargai privasi sebagai hak asasi manusia. Kebijakan pedoman ini menetapkan langkah apa saja yang harus diambil untuk memastikan Data Pribadi ditangani dengan tepat. Sosialisasi atas kebijakan perlindungan atas Data Pribadi akan dilakukan secara berkala kepada seluruh karyawan Astragraphia.
Ketika mengumpulkan, menggunakan atau menyimpan Data Pribadi, karyawan harus:

- Hanya mengumpulkan data yang memadai dan relevan dan menggunakannya semata-mata sesuai dengan tujuan pengumpulannya.
- Bersikap transparan dengan individu mengenai bagaimana Data Pribadi mereka digunakan sesuai dengan ketentuan perundangan-undangan yang berlaku.
- Mendapatkan izin dari individu sesuai dengan hukum yang berlaku.
- Tetap menjaga kemutakhiran Data Pribadi dengan memperbaiki informasi yang tidak akurat ketika diminta.
- Menjaga kerahasiaan dan keamanan Data Pribadi dengan membatasi akses atas Data Pribadi tersebut.
- Bertindak dengan penuh tanggung jawab dan beretika, menjunjung tinggi nilai-nilai Astragraphia, selalu mempertimbangkan resiko terhadap individu dalam menggunakan Data Pribadi mereka dan mengambil langkah untuk mengurangi resiko tersebut.

Ketika mengumpulkan, menggunakan atau menyimpan Data Pribadi, karyawan tidak boleh:

- Mentransfer Data Pribadi kepada siapapun di luar pihak-pihak yang berkepentingan di dalam Astragraphia.
- Mengumpulkan dan menggunakan Data Pribadi untuk tujuan yang tidak diharapkan oleh pelanggan atau karyawan Astragraphia.

5.5. Kebijakan Keamanan Personalia

Kebijakan Keamanan Personalia dimaksudkan untuk mengurangi risiko kesalahan manusia, pencurian atau penyalahgunaan informasi dan fasilitas Astragraphia. Tanggung jawab keamanan harus ditangani di tahap perekrutan karyawan dan dipantau selama pekerjaan individu. Individu potensial harus memiliki pemeriksaan latar belakang yang memadai, terutama jika mereka berada dalam posisi sensitif. Semua karyawan dan pengguna fasilitas pengolahan teknologi informasi pihak ketiga harus menandatangani perjanjian kerahasiaan (tidak diungkapkan) jika mereka memiliki akses terhadap informasi sensitif.

5.5.1. Personel Screening

Astragraphia mengikuti panduan SDM terkini berkenaan dengan skrining pra-kerja. Skrining tambahan untuk posisi sensitif dapat dilakukan.

5.5.2. Kesadaran Pengguna

Untuk memastikan bahwa semua karyawan Astragraphia mengetahui ancaman dan masalah keamanan informasi, dan dilengkapi untuk mendukung kebijakan keamanan Astragraphia, karyawan harus diberitahu mengenai prosedur keamanan dan penggunaan fasilitas pemrosesan informasi yang benar untuk meminimalkan kemungkinan risiko keamanan.

Semua karyawan Astragraphia dan bila diperlukan pihak ketiga harus menerima pembaruan reguler dalam kebijakan, standar dan prosedur keamanan Astragraphia. Ini termasuk persyaratan keamanan, tanggung jawab hukum dan kontrol bisnis, serta penggunaan fasilitas informasi yang benar, misalnya prosedur login dan penggunaan paket perangkat lunak, sebelum akses ke informasi diberikan.

Program kesadaran keamanan informasi harus dikembangkan, diterapkan dan dipelihara untuk memenuhi kebutuhan pendidikan keamanan semua karyawan. Program kesadaran keamanan Astragraphia akan diperkuat setidaknya setiap tahun.

5.5.3. Menanggapi Insiden dan Malfungsi Keamanan

Insiden yang mempengaruhi keamanan harus dilaporkan ke Information Security Manager melalui Help Desk (Customer Service Center/CSC) secepat mungkin. Semua karyawan dan kontraktor harus diberi tahu tentang prosedur untuk melaporkan berbagai jenis insiden (pelanggaran keamanan, ancaman, kelemahan atau kerusakan) yang mungkin berdampak pada keamanan aset Astragraphia.

5.5.4. Pelaporan Kelemahan Keamanan

Pengguna teknologi informasi harus diminta untuk mencatat dan melaporkan setiap kelemahan atau ancaman keamanan yang diamati atau yang dicurigai seperti intrusi dari luar wilayah Astragraphia kepada Manajer Keamanan Informasi. Mereka harus melaporkan kelemahan ini sesegera mungkin. Pengguna tidak boleh mencoba dalam keadaan apapun untuk membuktikan kelemahan yang dicurigai. Ini untuk perlindungan mereka sendiri karena

kelemahan pengujian dapat dianggap sebagai penyalahgunaan sistem yang potensial.

5.6. Kebijakan Keamanan Fisik dan Lingkungan

Fasilitas pengolahan informasi bisnis Astragraphia yang penting atau kritis harus ditempatkan di area yang aman, dilindungi oleh perimeter keamanan yang ditentukan, dengan penghalang keamanan dan kontrol masuk yang sesuai. Mereka harus dilindungi secara fisik dari akses, kerusakan dan interferensi yang tidak sah.

5.6.1. Perimeter Keamanan Fisik

Keamanan fisik bisa dicapai dengan menciptakan penghalang fisik seputar aset yang dilindungi. Setiap penghalang membentuk perimeter keamanan yang memerlukan metode kontrol akses untuk masuk. Perimeter ini bisa berupa pintu masuk dengan akses kunci kartu, area resepsionis atau penghalang fisik lainnya. Penilaian risiko akan menentukan jenis dan luas perimeter ini.

5.6.2. Keamanan Perlengkapan

Potensi kerentanan teknis harus diidentifikasi dan ditangani oleh tim IT. Teknis manajemen kerentanan harus membahas pemantauan kerentanan, penilaian risiko kerentanan, peletakan dan pelacakan aset. Garis waktu harus didefinisikan dalam menanggapi pemberitahuan kerentanan teknis. Prosedur harus ditetapkan untuk mengklasifikasikan tingkat tindakan yang diambil karena kerentanan teknis timbul terkait dengan prosedur penanganan perubahan atau prosedur penanganan insiden.

Risiko yang terkait dengan pemasangan Patch harus dinilai. Patch harus diuji sebelum dipasang. Jika Patch tidak tersedia maka kontrol lain harus dipertimbangkan:

a) Mengubah layanan yang terkait dengan kerentanan.
b) Menambah akses kontrol.
c) Menambah pemantauan untuk mendeteksi dan mencegah serangan.
d) Meningkatkan kesadaran akan kerentanan.

Log harus diambil untuk semua tindakan yang berkaitan dengan kerentanan memperbaiki dan/atau menambal, dan meninjau secara teratur. Teknologi yang tepat harus digunakan untuk menilai kerentanan teknis dan harus diaudit setahun sekali.

5.6.3. Keamanan Perlengkapan

Peralatan komputer harus dilindungi secara fisik dari ancaman keamanan dan bahaya lingkungan. Perlindungan peralatan diperlukan untuk mengurangi risiko akses data yang tidak sah dan untuk melindungi dari kehilangan atau kerusakan. Kontrol khusus mungkin juga diperlukan untuk melindungi fasilitas pendukung seperti pasokan listrik dan infrastruktur kabel.

5.6.4. Clean Desk and Clear Screen

Informasi sensitif seperti yang didefinisikan oleh standar Klasifikasi Data Astragraphia harus dihapus dari pandangan dan dijamin secara fisik bila tidak digunakan. Komputer desktop dan laptop harus menggunakan screen saver

untuk memastikan informasi sensitif tidak ditampilkan setelah periode tidak aktif pengguna. Komputer desktop yang terhubung ke jaringan harus log off secara otomatis atau layar terkunci setelah periode tertentu tidak aktif.

5.7. Manajemen Komunikasi dan Operasi

5.7.1. Prosedur dan Operasi

Prosedur operasi untuk seluruh sistem dan aplikasi Astragraphia harus di dokumentasikan dan di rawat. Prosedur operasi harus diperlakukan sebagai dokumen formal dan perubahan harus diberi wewenang oleh manajemen. Prosedur terdokumentasi juga harus dipersiapkan untuk kegiatan rumah tangga yang terkait dengan fasilitas pemrosesan informasi dan komunikasi seperti startup komputer dan prosedur shut down, back-up, perawatan peralatan, pengelolaan dan keamanan data center.

5.7.2. Kontrol Perubahan Operasi

Perubahan pada fasilitas dan sistem pengolahan informasi Astragraphia harus diotorisasi dan dikendalikan melalui proses manajemen perubahan formal. Tanggung jawab dan prosedur pengelolaan formal harus ada untuk memastikan kontrol yang memuaskan atas semua perubahan pada peralatan, perangkat lunak atau dokumentasi prosedural.

5.7.3. Prosedur Manajemen Insiden

Tanggung jawab dan prosedur manajemen insiden harus didefinisikan dan didokumentasikan dengan jelas untuk memastikan respon yang cepat, efektif dan tertib terhadap insiden keamanan.

5.7.4. Pemisahan Tugas

Kapan pun layak, Astragraphia harus menerapkan pemisahan tugas untuk meminimalkan risiko penyalahgunaan atau kesalahan sistem Astragraphia secara disengaja atau tidak disengaja. Bila hal ini tidak memungkinkan, kontrol lain seperti pemantauan kegiatan, jalur audit, dan pengawasan manajemen harus dipertimbangkan.

5.7.5. Pemisahan Fasilitas Pengembangan dan Operasional

Sejauh mungkin, Astragraphia harus memisahkan pengembangan dari fasilitas operasional dan menetapkan proses formal untuk memindahkan perangkat lunak dan / atau perangkat keras dari satu lingkungan ke lingkungan lainnya (kedua arah). Lingkungan yang sama harus ada antara pengembangan dan pengujian. Lingkungan uji yang stabil harus ditetapkan untuk memastikan perubahan tidak dapat dilakukan pada versi uji perangkat lunak.

5.7.6. Perlindungan Terhadap Perangkat Lunak yang Berbahaya

Perangkat lunak dan kontrol terkait harus diterapkan di semua sistem Astragraphia untuk mencegah dan mendeteksi pengenalan perangkat lunak berbahaya. Pengenalan perangkat lunak berbahaya seperti virus komputer, program network worm dan trojan horse dapat menyebabkan kerusakan serius pada jaringan, workstation dan data bisnis. Pengguna harus waspada terhadap bahaya perangkat lunak yang tidak sah atau berbahaya. Astragraphia harus

menerapkan kontrol untuk mendeteksi dan mencegah virus komputer diperkenalkan ke lingkungan Astragraphia.

5.7.7. **Manajemen Jaringan**

Astragraphia harus menerapkan berbagai kontrol jaringan untuk menjaga keamanan di jaringan internal agar terpercaya, dan perlindungan layanan dan jaringan yang terhubung. Kontrol ini harus mencegah akses tidak sah dan penggunaan jaringan pribadi Astragraphia.

5.7.8. **Keamanan Internet & Penggunaan yang Dapat Diterima**

Saat karyawan terhubung ke Internet menggunakan "ag-it.com" atau sebutan Astragraphia lainnya, seharusnya untuk kegiatan bisnis Astragraphia. Peralatan, sistem, fasilitas dan perlengkapan Astragraphia harus digunakan hanya untuk menjalankan bisnis Astragraphia atau untuk tujuan yang disahkan oleh manajemen. Berikut ini belum keseluruhan daftar, dan hanya memberikan contoh perilaku yang dapat mengakibatkan tindakan disipliner. Secara khusus, internet tidak boleh digunakan

- Untuk keperluan atau keuntungan pribadi,
- Untuk mewakili dirimu sebagai orang lain (yaitu, "spoofing"),
- Untuk meminta karyawan Astragraphia melakukan sesuatu untuk kepentingan selain bisnis,
- Untuk menyalin atau mengirim informasi pihak ketiga tanpa izin,
- Untuk mengekspresikan pendapat pribadi mengenai vendor, pemasok, dan sebagainya,
- Memberikan informasi tentang, atau daftar, karyawan Astragaphia kepada orang lain,
- Untuk permohonan komersial kegiatan bisnis non-Astragraphia,
- Bila hal tersebut mengganggu pekerjaan anggota karyawan atau pekerjaan anggota karyawan lainnya,
- Bila mengganggu pengoperasian gateway Internet,
- Untuk usaha yang tidak sah untuk masuk ke sistem komputasi apakah termasuk Astragraphia atau organisasi lain (yaitu, *cracking* atau *hacking*),
- Untuk mengirim pesan yang mengancam atau dengan cara apapun melecehkan orang lain,
- Untuk pencurian atau penyalinan tidak sah atas file elektronik,
- Untuk memposting informasi Astragraphia yang sensitif kepada personil yang tidak berwenang,
- Untuk mendownload atau mengunggah informasi yang isinya dapat menimbulkan konsekuensi hukum atau mencerminkan secara negatif reputasi Astragraphia - termasuk materi yang berkaitan dengan pernyataan ras, seksual, atau agama; materi dengan bahasa, grafis, atau gambar yang menyinggung; atau materi yang dilarang oleh hukum,
- Untuk "sniffing" (yaitu, memantau lalu lintas jaringan), kecuali yang berwenang melakukannya sebagai bagian dari tanggung jawab pekerjaan mereka.

5.7.9. **Koneksi Internet Eksternal**

Akses dial-up ke Internet dilarang dari perangkat yang terhubung ke bagian jaringan Astragraphia manapun. Ini mencakup akun dengan penyedia layanan Internet pihak ketiga. Pengguna tidak akan menggunakan akun Astragraphia Internet untuk menjalin koneksi dengan layanan pihak ketiga ini, kecuali jika diberi wewenang untuk melakukannya oleh manajemen Astragraphia dan Manajer Keamanan Informasi.

Mencoba untuk terhubung ke Internet dari firewall menggunakan jenis remote log-in atau layanan dial up dapat membahayakan integritas dan keamanan firewall.

5.7.10. **Koneksi ke Jaringan Pihak Ketiga**

Sambungan jaringan pribadi Astragraphia ke jaringan pribadi pihak ketiga harus memiliki dokumen bisnis yang didokumentasikan dan disetujui oleh Dept. Head ITSS dan Manajer Keamanan Informasi. Analisis risiko harus dilakukan untuk memastikan bahwa koneksi ke jaringan pihak ketiga tidak akan membahayakan jaringan pribadi Astragraphia.

5.7.11. **Keamanan Surat Elektronik**

Sistem surat elektronik biasanya digunakan untuk kegiatan bisnis Astragraphia. Astragraphia mengelola sistem surat elektronik (*e-mail*) untuk penggunaan bisnis oleh karyawan dan orang-orang yang berwenang lainnya. Penggunaan sistem ini harus sesuai dengan kebijakan ini dan standar dan prosedur Astragraphia lainnya mengenai penggunaan, distribusi, dan pengungkapan Astragraphia dan informasi kepemilikan pihak ketiga lainnya. Penggunaan sistem surat elektronok Astragraphia dapat dipantau secara acak agar sesuai dengan kebijakan ini.

Dalam keadaan normal, surat elektronik/data dianggap rahasia antara pengirim dan penerima. Baik pengirim atau penerima dapat mengungkapkan surat elektronik/data ke pihak ketiga atas kebijaksanaannya sendiri. Informasi kepemilikan pihak ketiga Astragraphia tidak boleh diungkapkan kepada individu atau organisasi yang bukan Astragraphia tanpa sepengetahuan dan persetujuan dari Pemilik Informasi. Dalam beberapa keadaan, menurut arahan manajemen, mungkin perlu bagi Manajer Keamanan Informasi untuk mengakses surat elektronik/data individu dalam penyelidikan dugaan insiden keamanan, atau keadaan khusus lainnya. Karyawan seharusnya tidak mengharapkan privasi saat menggunakan sistem surat elektronik Astragraphia.

5.8. **Kontrol Akses**

Integritas, kerahasiaan dan ketersediaan aset informasi Astragraphia akan dilindungi oleh mekanisme kontrol akses logis dan fisik yang sepadan dengan nilai, sensitivitas, risiko kehilangan atau kompromi dan kemudahan pemulihan aset-aset ini.

Pemilik Informasi bertanggung jawab untuk menentukan siapa yang harus memiliki akses terhadap sumber daya yang dilindungi di dalam yurisdiksinya, dan hak istimewa akses apa yang akan mereka dapatkan (baca, perbarui, dll.). Hak akses ini harus diberikan sesuai dengan tanggung jawab pekerjaan pengguna.

5.8.1. **Registrasi Pengguna dan Manajemen Akses**

Proses registrasi pengguna dan de-registrasi (penghentian) secara formal harus dibuat dan didokumentasikan untuk semua sistem dan layanan multi-user Astragraphia. Proses ini untuk mencegah akses tidak sah ke informasi Astragraphia.

5.8.2. **Manajemen Password Pengguna**

Password/kata sandi yang gigih adalah sarana umum untuk mengautentikasi identitas pengguna untuk mengakses sistem informasi atau layanan. Standar sandi harus dikembangkan dan diterapkan untuk memastikan semua orang yang berwenang mengakses sumber daya Astragraphia mengikuti praktik pengelolaan kata sandi yang terbukti. Aturan sandi ini harus diamanatkan oleh kontrol sistem bila memungkinkan. Praktik terbaik kata sandi ini termasuk namun tidak terbatas pada:

- Jangan tulis kata sandi,
- Gunakan kata sandi yang tidak mudah ditebak atau dikenai pengungkapan melalui serangan kamus,
- Jaga kerahasiaan kata sandi - jangan berbagi kata kunci individual dengan pengguna lain,
- Ubah kata sandi secara berkala,
- Ubah kata sandi sementara pada logon pertama,
- Jangan sertakan kata sandi dalam proses logon otomatis apapun, misalnya disimpan dalam makro atau tombol fungsi, atau dalam kode Aplikasi.

5.8.3. **Kontrol Akses Jaringan**

Akses ke jaringan internal Astragraphia yang terpercaya harus mewajibkan semua pengguna yang berwenang untuk mengautentikasi diri mereka sendiri melalui penggunaan ID pengguna individual dan mekanisme otentikasi, misalnya, kata sandi, token atau smart card, atau sertifikat digital. Kontrol jaringan harus dikembangkan dan diimplementasikan yang memastikan bahwa pengguna yang berwenang hanya dapat mengakses sumber daya jaringan dan layanan yang diperlukan untuk melakukan tanggung jawab pekerjaan mereka.

5.8.4. **Otentikasi Pengguna untuk Koneksi Eksternal (*Remote Access Control*)**

Akuntabilitas perorangan harus dipertahankan saat sumber daya Astragraphia diakses dari jarak jauh. Untuk mempertahankan standar keamanan informasi tertinggi, Astragraphia mengharuskan agar pertanggungjawaban individu dipertahankan setiap saat, termasuk selama akses jarak jauh. Untuk tujuan kebijakan ini, "akses jarak jauh" didefinisikan sebagai akses yang masuk ke jaringan Astragraphia dari luar jaringan pribadi Astragraphia dan terpercaya. Ini termasuk, namun tidak terbatas pada:

- Memanggil dari lokasi lain melalui jalur umum oleh anggota karyawan atau orang yang berwenang lainnya;
- Menghubungkan jaringan pihak ketiga melalui dial atau teknologi akses sementara lainnya ke jaringan Astragraphia.

5.8.5. **Pemisahan Jaringan**

Ketika jaringan Astragraphia terhubung ke jaringan lain, kontrol harus dilakukan untuk mencegah pengguna dari jaringan lain yang terhubung mengakses area sensitif yaitu jaringan pribadi Astragraphia. Daftar kontrol akses router atau teknologi lainnya harus diimplementasikan untuk mengendalikan akses ke sumber daya yang aman pada jaringan Astragraphia yang terpercaya.

5.8.6. **Kontrol Akses Sistem Operasi**

Akses ke kode sistem operasi, layanan dan perintah harus dibatasi hanya untuk orang-orang yang diperlukan dalam kinerja normal dari tanggung jawab pekerjaan mereka. Semua individu (pemrogram sistem, administrator database, administrator jaringan, dsb.) harus memiliki ID pengguna unik untuk penggunaan pribadi dan satu-satunya sehingga aktivitas dapat dilacak ke orang yang bertanggung jawab. ID pengguna seharusnya tidak memberikan indikasi tingkat hak istimewa pengguna, misalnya supervisor, manajer, administrator.
Dalam keadaan tertentu, di mana ada keuntungan bisnis yang jelas, penggunaan ID pengguna bersama untuk sekelompok pengguna atau pekerjaan tertentu dapat digunakan. Persetujuan Dept. Head ITSS harus didokumentasikan dalam kasus-kasus ini. Kontrol tambahan dapat diimplementasikan untuk memastikan akuntabilitas.

5.8.7. **Kontrol Akses Aplikasi**

Akses ke sistem dan bisnis aplikasi harus dibatasi pada orang-orang yang memiliki kebutuhan bisnis untuk mengakses aplikasi atau sistem dan pekerjaan tersebut merupakan bagian dari tanggung jawab pekerjaan mereka. Akses ke source code pada sistem dan aplikasi harus dibatasi untuk karyawan yang memiliki tugas sebagai support saja, dan akses tersebut harus dibatasi sehingga karyawan support hanya dapat mengakses sistem dan aplikasi yang merupakan kewenangan dan tanggung jawab mereka.

5.9. **Pengembangan dan Pemeliharaan Sistem**

Aplikasi perangkat lunak dikembangkan atau diperoleh untuk memberikan solusi ekonomi bagi masalah bisnis. Untuk memastikan keamanan dibangun ke dalam sistem informasi, semua persyaratan keamanan harus diidentifikasi pada tahap persyaratan proyek dan dibenarkan, disetujui dan didokumentasikan sebagai bagian dari keseluruhan kasus bisnis untuk sistem informasi.
Persyaratan dan pengendalian keamanan harus mencerminkan nilai bisnis aset informasi yang terlibat, dan potensi kerusakan bisnis yang mungkin diakibatkan oleh kegagalan atau ketiadaan tindakan pengamanan. Kerangka untuk menganalisis persyaratan keamanan dan mengidentifikasi kontrol untuk menghadapinya dikaitkan dengan penilaian ancaman dan manajemen risiko.

5.9.1. **Prosedur Pengendalian Perubahan**

Untuk meminimalisir kemungkinan terjadinya korupsi sistem informasi, pengawasan ketat terhadap perubahan sistem informasi harus dilaksanakan. Prosedur pengendalian perubahan formal harus diberlakukan. Mereka harus memastikan bahwa prosedur keamanan dan pengendalian tidak terganggu, bahwa karyawan pendukung diberi akses hanya pada bagian-bagian sistem

yang diperlukan untuk melakukan pekerjaan mereka, dan bahwa persetujuan formal dan proses persetujuan untuk perubahan diterapkan. Prosedur pengendalian perubahan ini harus diterapkan pada aplikasi bisnis serta perangkat lunak sistem yang digunakan untuk memelihara sistem operasi, perangkat lunak jaringan, perubahan perangkat keras, dan sebagainya.

5.9.2. **Kerentanan Manajemen**

Potensi kerentanan teknis harus diidentifikasi dan ditangani oleh tim IT. Teknis manajemen kerentanan harus membahas pemantauan kerentanan, penilaian risiko kerentanan, peletakan dan pelacakan aset. Garis waktu harus didefinisikan dalam menanggapi pemberitahuan kerentanan teknis. Prosedur harus ditetapkan untuk mengklasifikasikan tingkat tindakan yang diambil karena kerentanan teknis timbul terkait dengan prosedur penanganan perubahan atau prosedur penanganan insiden.

Risiko yang terkait dengan pemasangan Patch harus dinilai. Patch harus diuji sebelum dipasang. Jika Patch tidak tersedia maka kontrol lain harus dipertimbangkan:

a. Mengubah layanan yang terkait dengan kerentanan.
b. Menambah akses kontrol.
c. Menambah pemantauan untuk mendeteksi dan mencegah serangan.
d. Meningkatkan kesadaran akan kerentanan.

Log harus diambil untuk semua tindakan yang berkaitan dengan kerentanan memperbaiki dan / atau menambal, dan meninjau secara teratur. Teknologi yang tepat harus digunakan untuk menilai kerentanan teknis dan harus diaudit setahun sekali.

5.10. **Perencanaan Pemulihan Bencana**

Fungsi pemulihan bencana untuk komponen teknologi informasi (TI) harus dilakukan oleh organisasi Manajemen Layanan. Pihak yang bertanggung jawab di dalam area ini harus mencari masukan dari proses bisnis dan pemilik informasi mengenai persyaratan pemulihan mereka untuk teknologi informasi dalam jalur bisnis untuk memastikan gangguan terhadap operasi bisnis normal diminimalkan.

5.11. **Kepatuhan**

5.11.1. **Hak Kekayaan Intelektual**

Prosedur yang tepat harus diterapkan untuk memastikan kepatuhan terhadap pembatasan hukum penggunaan materi berhak cipta, atau materi yang mungkin memiliki hak desain atau merek dagang. Produk perangkat lunak berpemilik umumnya diberikan dengan perjanjian lisensi yang membatasi penggunaan produk ke mesin atau jumlah pengguna tertentu. Pengendalian harus dilaksanakan untuk memastikan semua aspek dari perjanjian lisensi terpenuhi dan dapat diaudit. Pelanggaran hak cipta dapat menyebabkan tindakan hukum yang mungkin melibatkan proses pidana.

5.11.2. **Pencegahan Penyalahgunaan Sumber Daya Teknologi Informasi**

Sumber teknologi informasi dan data yang diproses oleh sumber daya ini disediakan untuk tujuan bisnis Astragraphia. Manajemen harus mengizinkan penggunaannya. Setiap penggunaan fasilitas TI untuk tujuan non-bisnis atau

tidak sah, tanpa persetujuan manajemen, harus dianggap sebagai penyalahgunaan fasilitas Astragraphia.

5.11.3. **Kepatuhan Terhadap Kebijakan Keamanan**
Manajer harus memastikan bahwa semua proses dan prosedur keamanan di dalam area tanggung jawab mereka diikuti. Selain itu, semua unit bisnis di Astragraphia harus dipertimbangkan untuk tinjauan reguler guna memastikan kepatuhan terhadap kebijakan dan standar keamanan.

5.12. **Sosialisasi**
Kebijakan ini disosialisasikan secara berkala kepada seluruh karyawan Astragraphia dan Pihak Eksternal.

5.13. **Penutup**
Kebijakan ini akan disesuaikan apabila dianggap perlu dengan memperhatikan ketentuan hukum dan peraturan perundang-undangan yang berlaku di Indonesia.

6. Referensi

6.1. NIST
6.2. ISO 27001
6.3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta perubahannnya ("UU ITE");
6.4. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dan Transaksi Elektronik ("Permen Perlindungan Data Pribadi").
6.5. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik ("PP PSTE").

7. Dokumen Terkait

Tidak Ada