Information Security Management System Policy

The general policy of the Information Security Management System at PT Traze Andalan Futures is as follows:

1. Information is one of the primary assets in the business conducted by the Company. Therefore, the confidentiality, integrity, and availability of information must be managed so that its security is maintained.

2. The implementation of the Information Security Management System within the Company refers to the ISO/IEC 27001:2022 standard and applicable laws and regulations.

3. Top management of the Company continuously demonstrates leadership and commitment to implementing the Information Security Management System within the organization.

4. The information security policy must be communicated to all employees and relevant third parties through available communication media so that it is easily understood and complied with.

Kebijakan Sistem Manajemen Keamanan Informasi

Kebijakan umum sistem manajemen keamanan informasi di PT Traze Andalan Futures adalah sebagai berikut:

1. Informasi merupakan salah satu aset utama dalam bisnis yang diselenggarakan oleh Perusahaan. Oleh karena itu, kerahasiaan (confidentiality), kebenaran (integrity), dan ketersediaan (availability) informasi perlu dikelola sehingga keamanannya dapat terjaga.

2. Penerapan sistem manajemen keamanan informasi di Perusahaan mengacu pada standar ISO/IEC 27001:2022 dan peraturan perundang-undangan yang berlaku.

3. Manajemen puncak Perusahaan senantiasa menunjukkan kepemimpinan dan komitmen untuk menerapkan sistem manajemen keamanan informasi di organisasi.

4. Kebijakan keamanan informasi harus dikomunikasikan ke seluruh karyawan dan pihak ketiga terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi.

5. The Company will continuously strive to improve awareness, knowledge, and skills regarding information security for both internal employees and relevant external parties.

6. The Company conducts assessments and manages risks related to information security based on vulnerabilities and threats present in every asset and process.

7. If there are vulnerabilities and threats that have the potential to disrupt information security, all interested parties are required to report them to the Chief Information Security Officer (CISO) or members of the ISMS Team.

8. All leaders at all levels are responsible for monitoring and evaluating the effectiveness of the implementation of this policy across all work units/departments under their supervision.

9. All employees are responsible for maintaining and protecting the security of information assets and complying with established information security policies and procedures.

5. Perusahaan akan selalu berusaha meningkatkan kepedulian (awareness), pengetahuan, dan keterampilan tentang keamanan informasi bagi karyawan internal maupun pihak eksternal yang terkait.

6. Perusahaan melaksanakan kajian dan mengelola risiko-risiko terkait keamanan informasi berdasarkan kerentanan (vulnerability) dan ancaman (threat) yang ada pada setiap aset maupun proses.

7. Jika ada kerentanan dan ancaman yang berpotensi mengganggu keamanan informasi maka semua pihak yang berkepentingan wajib melaporkannya kepada Chief Information Security Officer (CISO) atau anggota Tim SMKI.

8. Seluruh pimpinan di semua tingkatan bertanggung jawab memantau dan mengevaluasi efektivitas penerapan kebijakan ini di seluruh unit kerja/bagian di bawah pengawasannya.

9. Seluruh karyawan bertanggung jawab untuk menjaga dan melindungi keamanan aset informasi serta mematuhi kebijakan dan prosedur keamanan informasi yang telah ditetapkan.

10. Any violation of this policy and other related policies will be subject to administrative sanctions, such as revocation of information system access rights and/or other disciplinary actions in accordance with applicable regulations.
11. The organization is committed to continual improvement of the Information Security Management System implementation.

More technical policies and procedures will be developed separately and established by referring to the principles set forth in this policy statement.

10. Setiap pelanggaran terhadap kebijakan ini dan kebijakan lain yang terkait akan dikenai sanksi administratif seperti pencabutan hak akses sistem informasi dan/atau tindakan pendisiplinan lain sesuai peraturan yang berlaku.
11. Organisasi berkomitmen untuk terus melakukan perbaikan berkelanjutan terhadap implementasi Sistem Manajemen Keamanan Informasi.

Kebijakan dan prosedur yang bersifat lebih teknis akan dibuat secara terpisah dan ditetapkan dengan merujuk prinsip-prinsip yang ditetapkan dalam pernyataan kebijakan ini.