SIPEF

PT Tolan Tiga Indonesia IT Security Policy

PT Tolan Tiga Indonesia is committed to protecting data and its network from misuse, corruption or damage. All employees should fully implement the following policy.

PT Tolan Tiga Indonesia berkomitmen dalam menjaga data dan jaringannya dari penyalahgunaan, manipulasi atau kerusakan. Seluruh pekerja wajib untuk mengimplementasikan kebijakan ini.

1.	This policy applies to data processing equipment, hardware, software and the network physically housed in PT Tolan Tiga Indonesia or stored remotely under the management of PT Tolan Tiga Indonesia.	Kebijakan ini berlaku untuk segala peralatan pengolah data, perangkat keras, perangkat lunak yang secara fisik disimpan oleh PT Tolan Indonesia atau disimpan di luar lokasi yang masih di bawah manajemen PT Tolan Tiga Indonesia.
2.	**Use of the Network and IT systems** External equipment/private hardware (PC, laptop and other equipment) connected to the network must be authorised by the IT department (ITD). It must be ensured that devices conform to security policies and requirements before connecting to any IT services. It is prohibited to download, install or run software (freeware, demo, trial) on the Company's computers/network other than software authorised by the IT department.	**Penggunaan Jaringan dan sistem IT** Perangkat external/private hardware (PC, Laptop, Perangkat jaringan) yang terkoneksi ke jaringan harus memperoleh otorisasi oleh ITD. Untuk memastikan perangkat mematuhi kebijakan keamanan dan persyaratan sebelum koneksi ke layanan TI apa pun. Dilarang keras untuk mengunduh, memasang atau menggunakan perangkat lunak (freeware, demo, trial) di computer / jaringan perusahaan selain dari perangkat lunak yang diotorisasi oleh departemen IT.
3.	**User Access (Accounts & Passwords)** The ITD provides access to a variety of programs /software utilised by the Company via user accounts and passwords. These accounts and passwords are for individual use only. **It is strictly forbidden to share accounts and passwords.** The ITD will periodically terminate the access privilege of users who change roles or leave the Company, and will check for unnecessary accounts. The ITD is also authorised to terminate the user access privilege if a user violates the terms mentioned above.	**Akses Pengguna (Akun & Kata sandi)** ITD menyediakan akses ke berbagai program / perangkat lunak yang digunakan oleh perusahaan melalui akun pengguna dan kata sandi. Akun dan kata sandi ini hanya untuk penggunaan individu. **Dilarang keras untuk berbagi akun dan kata sandi.** ITD akan menonaktifkan hak akses pengguna yang berganti role atau keluar dari perusahaan secara berkala akan diperiksa dan dihapus untuk akun yang tidak diperlukan. ITD juga berhak untuk menonaktifkan hak akses pengguna yang melanggar poin-poin kebijakan yang tercantum diatas.

SIPEF

PT Tolan Tiga Indonesia IT Security Policy

4.	**Data Safety:** Company-related files and documents should be saved, not only in the assigned computer but also on the Company server and/or other media as backups, when available. Any loss or damage to the files is the responsibility of the user. Confidential files and Company-owned files must not be copied, printed and/or distributed outside of the Company, without authorisation of the department head or manager. If this policy is violated, disciplinary action will be taken against the concerned employee or user. Staff are required to immediately notify the ITD in the event of the loss of a device containing Company data, regardless of the storage medium (e.g., disk drive, electronic tape, cartridge, disk, CD, DVD, external drive, paper, fiche, etc.) and regardless of the form (e.g., text, graphic, video, audio, etc.). Any data being uploaded to the Company's server must be scanned for any viruses/ malware using the Company's licensed antivirus software. Deleting and corrupting Company files and/or programs with the intent of disrupting Company operations can result in disciplinary action (termination of employment) of the employee/user.	**Keamanan Data:** Data dan dokumen perusahaan harus disimpan tidak hanya pada computer masing-masing akan tetapi harus di simpan di dalam server perusahaan dan/atau media penyimpanan lainnya sebagai cadangan. Data yang hilang atau rusak merupakan tanggung jawab pengguna. File milik perusahaan yang bersifat Confidential tidak boleh dicopy, dicetak dan atau didistribusikan ke luar perusahaan tanpa otorisasi dari Pimpinan. Jika hal ini dilanggar, tindakan disiplin akan dikenakan kepada pegawai atau user yang bersangkutan. Data perusahaan yang hilang terlepas dari media penyimpanan (misalnya, disk drive, pita elektronik, kartrid, disk, CD, DVD, drive eksternal, kertas, fiche, dll.) Dan terlepas dari bentuknya (mis., Teks, grafik, video, audio , dll.). Staf diwajibkan untuk segera memberitahu ITD jika perangkat yang berisi data dalam ruang lingkup hilang. Data yang diunggah ke dalam server perusahaan harus diperiksa untuk menghindari virus / malware dengan menggunakan antivirus yang terlisensi kepada perusahaan. Tindakan disiplin (hingga sampai PHK) akan dikenakan kepada pegawai atau user yang menghapus atau merusak program atau file milik perusahaan dengan sengaja untuk mengacaukan pekerjaan atau opera-sional perusahaan.
6	Special requests outside of ITD standards shall have prior approval from the ITD Head of Department (HOD) or Board of Directors (BOD).	Permintaan khusus di luar standar ITD membutuhkan persetujuan dari Head of Department ITD atau BOD bila diperlukan.

Commited by,

ADAM CHRISTIAN QUENTIN JAMES
President Director

Date: 21 AUG 2018