 PT Indonesian Tobacco Tbk.	STANDARD OPERATING PROCEDURE	Nomor : IT/IT/SOP/03
	KEAMANAN DAN KONTROL AKSES DATA	Revisi : 2
		Halaman : 1 dari 2
		Tanggal : 31/01/2020

1. TUJUAN

1.1 Sebagai pedoman dalam menjaga keamanan data yang terdapat pada perangkat IT di lingkungan PT Indonesian Tobacco Tbk.

2. RUANG LINGKUP

2.1 Prosedur ini berlaku mulai dari pembatasan akses (blocking) port USB pada komputer dan pemberian kontrol akses untuk melihat dan merubah data yang ada pada perangkat IT khususnya komputer;

2.2 PIC adalah Person In Charge atau orang yang ditunjuk untuk bertanggung jawab dalam departemen.

3. DEFINISI

- 3.1 Blocking : Pembatasan hak akses;
- 3.2 Port : Soket/ colokan;
- 3.3 USB : Universal Serial Bus;
- 3.4 Storage : Media penyimpanan;
- 3.5 User : Pengguna;
- 3.6 Password : Kata Kunci;
- 3.7 VPN : Virtual Private Network, aplikasi untuk mengakses jaringan lokal secara aman;
- 3.8 Autentifikasi : Hak akses.

4. TANGGUNG JAWAB

4.1 Spv. IT/ Staf IT bertanggung jawab untuk melakukan menonaktifkan port USB pada komputer yang tidak mempunyai autentifikasi penggunaan Flashdisk/ USB Storage;

4.2 Staf IT bertanggung jawab untuk membuat daftar pengguna yang diberikan autentifikasi dalam mengakses data menggunakan port USB atau jaringan komputer.

5. URAIAN

5.1 Penonaktifan Port USB

- 5.1.1 Staf IT membuat "Rekap Daftar USB Lock" (IT/IT/ITI/09) yang mempunyai autentifikasi penggunaan flashdisk/ USB storage di lingkungan PT Indonesian Tobacco Tbk. dan disetujui oleh Spv. IT;
- 5.1.2 Spv. IT/ Staf IT menonaktifkan port USB pada setiap komputer yang user-nya tidak mempunyai autentifikasi penggunaan flashdisk/ USB storage;
- 5.1.3 Penonaktifan port USB hanya sebatas melakukan pembatasan hak akses (blocking) penggunaan flashdisk/ USB storage lainnya, namun masih bisa berfungsi untuk hal selain itu.

5.2 Akses Data


- 5.2.1 Spv. IT/ Staf IT membuat daftar PIC komputer pada setiap departemen, serta pembuatan user dan password untuk setiap PIC tersebut;
- 5.2.2 Data pada setiap komputer menjadi tanggung jawab setiap PIC departemen terkait, selain PIC terkait atau Spv. IT / Staff IT tidak diperkenankan mengakses data disetiap komputer, kecuali mendapat persetujuan dari PIC terkait atau Spv IT / Staff IT;

Disiapkan oleh :	Disetujui oleh :
Jabatan : Staf IT	Jabatan : Supervisor IT

Rahasia

Terkendali



 PT Indonesian Tobacco Tbk.	STANDARD OPERATING PROCEDURE	Nomor : IT/IT/SOP/03
	KEAMANAN DAN KONTROL AKSES DATA	Revisi : 2
		Halaman : 2 dari 2
		Tanggal : 31/01/2020

- 5.2.3 Akses data meliputi akses langsung di komputer terkait atau mengakses data lewat jaringan internal (file shared) / eksternal (VPN);
- 5.2.4 PIC terkait tidak diperkenankan mengcopy data perusahaan yang berada di komputer ke Flashdisk / USB storage pribadi, kecuali mendapat persetujuan dari manajemen;
- 5.2.5 Tamu atau orang diluar karyawan PT Indonesian Tobacco Tbk. tidak diperkenankan untuk menancapkan Flashdisk / USB storage lainnya ke komputer dalam lingkungan PT Indonesian Tobacco Tbk., kecuali mendapat persetujuan dari manajemen dan harus melalui Dept. IT terlebih dahulu;
- 5.2.6 Tamu atau orang diluar karyawan PT Indonesian Tobacco Tbk. jika ingin mendapatkan akses jaringan/ wifi harus melalui Dept. IT untuk diberikan password;
- 5.2.7 Tamu atau orang diluar karyawan PT Indonesian Tobacco Tbk. tidak diperkenankan untuk membuka file shared network, jika ingin mengcopy data hanya diperbolehkan melalui media flashdisk yang berasal dari Dept. IT, untuk selanjutnya Dept. IT yang melakukan proses pengcopyan.

6. INFORMASI TERDOKUMENTASI TERKAIT

6.1 Rekap Daftar USB Lock

IT/IT/IT/09

Disiapkan oleh :	Disetujui oleh :
Jabatan : Staf IT	Jabatan : Supervisor IT

Rahasia

Terkendali

