


STANDARD OPERATION PROCEDURE (PROSEDUR)

Controlled Document

	Segmen : <i>Supporting Directorate</i> Proses Bisnis : <i>Information Technology</i> Sub. Proses : Prosedur Keamanan Informasi	No. Dokumen : SOP-IT-008 Tgl. Efektif : 29/07/2022 Rev. : 00
---	--	--

1. TUJUAN

Prosedur Keamanan Informasi disusun sebagai panduan untuk melindungi informasi perusahaan yang bersifat sensitif seperti : informasi pembayaran customer/ pelanggan, data karyawan atau informasi strategis lainnya sehingga terhindar dari bahaya kebocoran maupun pembobolan (*hacker*).

2. RUANG LINGKUP

- 2.1. Prosedur keamanan informasi mencakup penyusunan penanganan keamanan informasi, software yang aman, penggunaan *password* dan meningkatkan kesadaran keamanan di lingkungan kerja;
- 2.2. Prosedur ini berlaku di seluruh area PT Sefas Keliantama.

3. TANGGUNG JAWAB

- 3.1. Tim IT bertanggung jawab dalam penyusunan penanganan keamanan informasi, pemilihan software, pembuatan *password* dan sosialisasi pentingnya keamanan informasi.

4. DEFINISI

- 4.1. Informasi sensitif terbagi atas informasi sangat sensitif dan informasi cukup sensitif;
- 4.2. Informasi sangat sensitif adalah data yang dapat menyebabkan kerusakan parah dan membutuhkan keamanan tertinggi serta akses hanya diperbolehkan atas kebutuhan khusus;
- 4.3. Informasi cukup sensitif adalah data yang dapat menimbulkan risiko relative rendah dan membutuhkan sedikit kontrol keamanan serta hak akses internal;
- 4.4. Informasi non sensitif adalah data yang tidak menimbulkan risiko bagi perusahaan dan hanya membutuhkan keamanan yang sedikit atau tidak ada pembatasan akses;

5. PROSEDUR

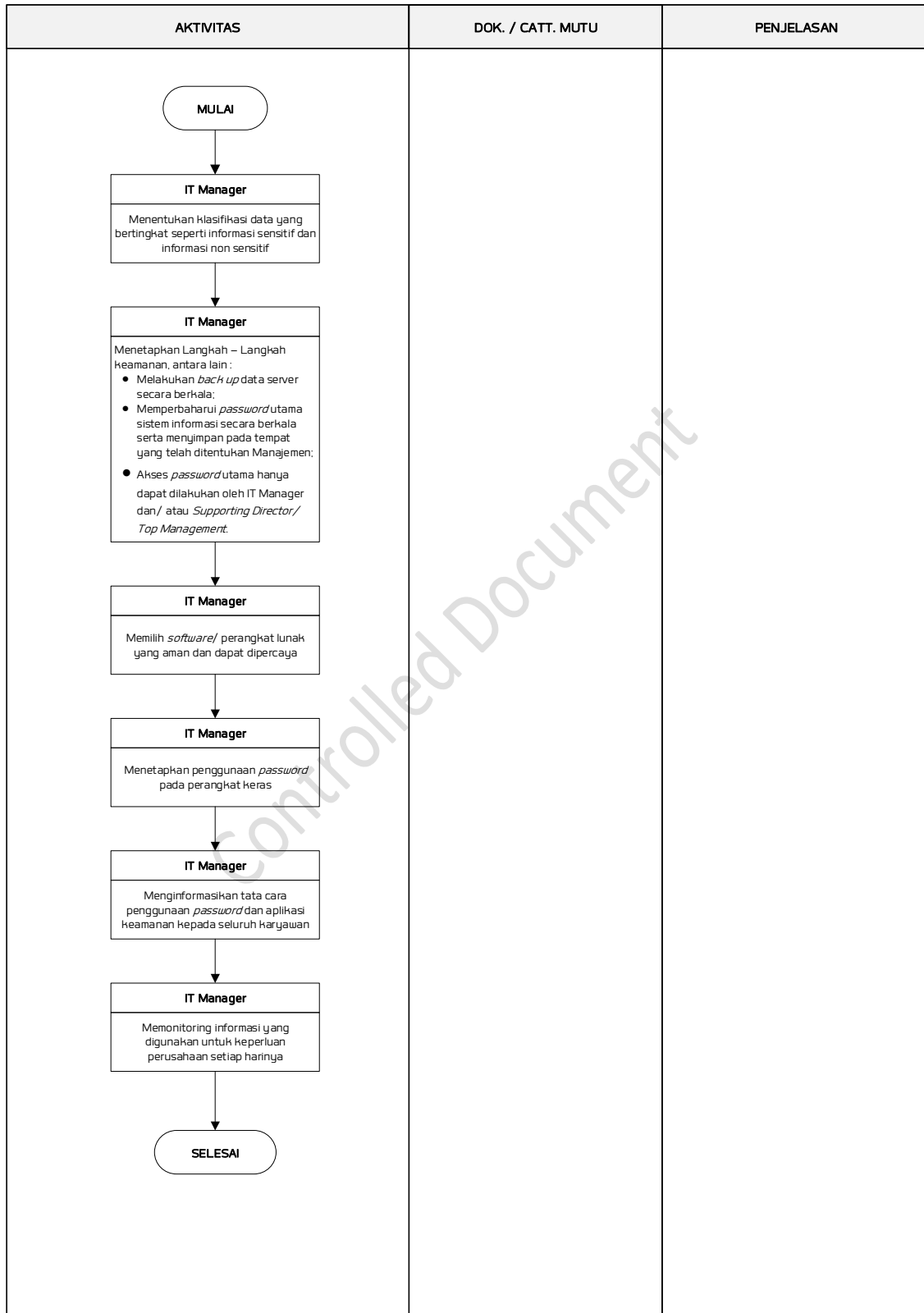
- 5.1. Penanganan keamanan informasi, sebagai berikut :
 - a. IT Manager menentukan klasifikasi data yang bertingkat seperti informasi sensitif dan informasi non sensitif;
 - b. IT Manager menetapkan Langkah – Langkah keamanan, antara lain :
 - Melakukan *back up* data server secara berkala;
 - Memperbaharui *password* utama sistem informasi secara berkala serta menyimpan pada tempat yang telah ditentukan Manajemen;
 - Akses *password* utama hanya dapat dilakukan oleh IT Manager dan/ atau *Supporting Director/ Top Management*.
 - c. IT Manager memilih *software/* perangkat lunak yang aman dan dapat dipercaya;
 - d. IT Manager menetapkan penggunaan *password* pada perangkat keras;
 - e. IT Manager menginformasikan tata cara penggunaan *password* dan aplikasi keamanan kepada seluruh karyawan;
 - f. IT Manager memonitoring informasi yang digunakan untuk keperluan perusahaan setiap harinya.




Segmen : *Supporting Directorate*
 Proses Bisnis : *Information Technology*
 Sub. Proses : Prosedur Keamanan Informasi

No. Dokumen : SOP-IT-008
 Tgl. Efektif : 29/07/2022
 Rev. : 00

6. FLOWCHART



	Segmen : <i>Supporting Directorate</i>	No. Dokumen : SOP-IT-008
	Proses Bisnis : <i>Information Technology</i>	Tgl. Efektif : 29/07/2022
	Sub. Proses : <i>Prosedur Keamanan Informasi</i>	Rev. : 00

7. REFERENSI

7.1. ISO 9001:2015 Klausul 7.1.3 Infrastruktur




8. DOKUMEN TERKAIT

8.1. *Password* utama sistem informasi

9. RIWAYAT DOKUMEN

Revisi No.	Uraian perubahan	Tanggal Efektif

10. PENGESAHAN

Disiapkan Oleh	Diperiksa Oleh	Disetujui Oleh
		
Nama : Gideon B. Sirapanji Jabatan : <i>IT Manager</i> Tgl. Pengesahan : 29/07/2022	Nama : Yoga Samudra Dewa Jabatan : MR & HRGA GM Tgl. Pengesahan : 29/07/2022	Nama : Kezia Roesli Jabatan : Direktur Tgl. Pengesahan : 29/07/2022