G. Ketentuan Pengamanan Fisik dan Informasi Arsip Dinamis

NO.	TINGKAT KLASIFIKASI KEAMANAN	MEDIA					
		ARSIP KONVENSIONAL			ARSIP ELEKTRONIK		
		Arsip	Pengguna	Prasarana & Sarana	Arsip	Pengguna	Prasarana & Sarana
1.	Biasa/ Terbuka	Tidak ada persyaratan dan prosedur khusus.	Pengguna yang berasal dari eksternal dan internal yang mempunyai hak akses	Tidak memerlukan prasarana dan sarana khusus	*Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autentisitas arsip	Pengguna yang berasal dari eksternal dan internal yang mempunyai hak akses	Tidak memerlukan prasarana dan sarana khusus
2.	Terbatas	Ada persyaratan dan prosedur dengan memberikan cap "TERBATAS" pada fisik arsip	Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum	Diperlukan tempat penyimpanan yang aman	1. *Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autentisitas arsip. 2. File-file elektronik (termasuk database) harus dilindungi terhadap penggunaan internal atau oleh pihak-pihak eksternal.	1. Autentikasi pengguna (nama pengguna/ *password* atau ID digital) 2. Penggunaan untuk *log in* pada tingkat individual	1. Autentikasi server 2. Langkah-langkah keamanan dengan *Operating System* khusus atau aplikasi khusus 3. *Firewall* dan sistem- sistem serta prosedur-prosedur deteksi terhadap intrusi

NO.	TINGKAT KLASIFIKASI KEAMANAN	MEDIA					
		ARSIP KONVENSIONAL			ARSIP ELEKTRONIK		
		Arsip	Pengguna	Prasarana & Sarana	Arsip	Pengguna	Prasarana & Sarana
3.	Rahasia	1. Ada persyaratan dan prosedur rahasia dengan memberikan cap "RAHASIA" pada fisik arsip 2. Tidak sembarangan meletakkan arsip/ dokumen yang bersifat rahasia	Dibatasi hanya untuk penentu kebijakan, pengawas internal dan eksternal serta penegak hukum	Lokasi aman dengan akses yang terbatas	1. *Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autentisitas arsip 2. File-file elektronik (termasuk database) harus dilindungi terhadap penggunaan internal atau oleh pihak-pihak eksternal	3. Hanya staf yang ditunjuk oleh kepala perangkat daerah yang dapat mengakses arsip tersebut 4. Autentikasi pengguna (nama pengguna/ *password* atau ID digital) 5. Penggunaan untuk *log in* pada tingkat individual	4. Langkah-langkah keamanan dengan *Operating System* khusus atau aplikasi khusus 5. *Firewall* serta sistem- sistem dan prosedur-prosedur deteksi terhadap intrusi. *Firewall* adalah sistem untuk melindungi komputer atau jaringan dari akses komputer lain yang tidak memiliki hak untuk

NO.	TINGKAT KLASIFIKASI KEAMANAN	MEDIA					
		ARSIP KONVENSIONAL			ARSIP ELEKTRONIK		
		Arsip	Pengguna	Prasarana & Sarana	Arsip	Pengguna	Prasarana & Sarana
4.	Sangat Rahasia	Ada persyaratan dan prosedur rahasia dengan memberikan cap “SANGAT RAHASIA” pada fisik arsip	Dibatasi hanya untuk Penentu Kebijakan, Pengawasan, dan Penegak Hukum	1. Disimpan dalam zona yang sangat aman, dengan penelusuran jejak akses 2. Penerapan kebijakan “Meja harus bersih”	1. *Back-up* secara teratur untuk tujuan pemulihan sistem dalam rangka menjamin autentisitas arsip 2. File-file elektronik (termasuk database) harus dilindungi terhadap penggunaan internal.	1. Autentikasi pengguna (nama pengguna/*pass word* atau ID digital) 2. Penggunaan untuk *log in* pada tingkat individual	1. Autentikasi server 2. Langkah-langkah keamanan dengan *Operating System* khusus atau aplikasi khusus 3. Firewall dan sistem- sistem dan prosedur-prosedur deteksi terhadap intrusi.

GUBERNUR JAWA TIMUR

Dr. H. SOEKARWO