KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI
DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN KEBUMEN

Dinas Komunikasi dan Informatika Kabupaten Kebumen menyadari bahwa informasi merupakan aset perusahaan yang harus dijaga. Oleh sebab itu, Dinas Komunikasi dan Informatika Kabupaten Kebumen berkomitmen untuk mengimplementasikan Sistem Manajemen Kemananan Informasi Berstandar Internasional yang bertujuan untuk memberikan perlindungan terhadap informasi sehingga terjamin ketersediaan, keutuhan serta kerahasiaannya. Untuk membuktikan komitmen dimaksud, kami menetapkan kebijakan ini untuk selalu memastikan hal-hal berikut dilaksanakan dalam kegiatan sehari-hari oleh manajemen, pekerja dan pihak ketiga yang berkerja dengan Dinas Komunikasi dan Informatika Kabupaten Kebumen, yaitu:

- ✓ Memenuhi harapan Stakeholder dengan mewujudkan Confidentiality, Integrity dan Availlability informasi melalui implementasi ISO/IEC 27001:2013 ISMS
- ✓ Selalu mentaati segala ketentuan dan peraturan terkait keamanan informasi yang berlaku di wilayah Republik Indonesia serta wilayah tempat dilakukannya pekerjaan
- ✓ Berjalannya perbaikan yang berkesinambungan terhadap kinerja Sistem Manajemen Keamananan Informasi.

Kebumen, 1 Agustus 2019

Kepala Dinas Komunikasi dan Informatika
Kabupaten Kebumen

PEMERINTAH KABUPATEN DISKOMINFO KEBUMEN

Sukro Aminoto, S.IP, M.Kes

PEMBERITAHUAN

Terkait dengan implementasi Sistem Manajemen Keamanan Informasi berbasis ISO 27001: 2013 di lingkungan Dinas Komunikasi dan Informatika Kabupaten Kebumen, berikut hal-hal yang harus dipatuhi dan diperhatikan:

1. Sistem Manajemen Keamanan Informasi merupakan sistem manajemen dalam suatu organisasi yang bertujuan untuk membangun, mengimplementasikan, mengoperasikan, memantau, memelihara dan meningkatkan keamanan informasi. Termasuk kerahasiaan, integritas dan ketersediaan dari suatu informasi.
2. Meja harus dalam keadaan bersih (tidak ada dokumen yang berserakan) apabila meninggalkan ruang kerja (misalnya: makan siang, ke toilet, dan sebagainya). Dokumen bisa disimpan dalam laci yang terkunci.
3. Layar komputer/laptop harus dalam kondisi terkunci apabila meninggalkan ruang kerja (misalnya: makan siang, ke toilet, dan sebagainya)
4. Tidak menshare password kepada orang lain dan tidak menuliskan password pada tempat-tempat yang bisa dibaca oleh orang lain. Misalnya menempelkan password pada meja kerja/layar komputer
5. Memastikan password yang digunakan sudah sesuai dengan ketentuan password yang baik, yaitu: password minimal panjang 8 karakter, kombinasi huruf besar/kecil, angka, dan simbol
6. Memastikan tidak ada dokumen yang tertinggal pada mesin foto copy dan/atau mesin scan
7. Memastikan antivirus pada PC/laptop yang digunakan dalam keadaan aktif, jika tidak dalam keadaan aktif, harap melaporkan kepada Pengelola Operasional dan Komunikasi
8. Tidak diperbolehkan untuk menginstall software bajakan dan/atau menyimpan file illegal pada PC/laptop
9. Pada saat menggunakan removable media (flashdisk, external hardisk) harus dipastikan removable media tersebut bebas dari virus.
10. Larangan melakukan update social media yang menampilkan data customer

Selain itu, terkait dengan hasil internal audit yang telah dilakukan pada 29 Agustus 2019, berikut ini beberapa hal yang perlu diperhatikan yaitu:

1. Sosialisasi terhadap Kebijakan Keamanan Informasi serta memastikan ketersediaan Kebijakan tersebut bagi pihak yang terkait harus dilakukan
2. Penilaian risiko harus dilakukan secara konsisten sesuai dengan ketentuan yang telah disusun
3. Pengelolaan terhadap dokumen, yang didalamnya termasuk juga pengesahan terhadap dokumen harus dilakukan
4. Pengelolaan akses harus dilakukan, termasuk juga pelaksanaan review terhadap akses yang dikelola
5. Rencana keberlangsungan harus ditentukan dan ditetapkan, termasuk menyiapkan redudansi dari perangkat pengelola informasi (DRC). Selain itu, rencana

keberlangsungan tersebut harus diuji dan hasil pengujiannya didokumentasikan untuk dilakukan Analisa

6. Peraturan/perundangan/kontrak yang terkait dengan proses bisnis yang dijalankan oleh organisasi harus diidentifikasi untuk dianalisa kepatuhannya
7. Analisa kebutuhan training harus dilakukan guna dapat disusun jadwal training bagi pekerja yang masih membutuhkan training
8. Maintenance terhadap perangkat pendukung harus dilakukan secara teratur sesuai dengan periode yang telah ditentukan guna memastikan perangkat pendukung tersebut tersedia saat dibutuhkan
9. Backup harus dilakukan terhadap data-data kritikal organisasi, untuk kemudian dilakukan pengujian dan pendokumentasian atas pengujian tersebut

Mohon pemberitahuan ini dapat dipatuhi dan diperhatikan agar implementasi Sistem Manajemen Keamanan Informasi berbasis ISO 27001: 2013 di lingkungan Diskominfo Kabupaten Kebumen dapat berjalan dengan baik.

Kebumen, 4 Oktober 2019

Mengetahui,

(Pengelola Pengamanan Human Resource)