Kebijakan Tata Kelola Teknologi Informasi

Seiring dengan pesatnya teknologi perbankan yang semakin berkembang, Perseroan memerlukan suatu Pedoman Tata Kelola Teknologi Informasi. Pedoman Tata Kelola Teknologi Informasi Perseroan meliputi beberapa kebijakan diantaranya pedoman terkait risiko teknologi informasi, pengelolaan perubahan teknologi informasi, pengelolaan problem teknologi informasi, pengendalian mutu teknologi informasi, pengelolaan kapasitas teknologi informasi, pengelolaan jaringan komunikasi teknologi informasi dan keamanan fisik *data center*. Pedoman-pedoman tersebut meliputi antara lain terkait kebijakan, proses penanganan, dan mitigasi risiko. Pengukuran tingkat kematangan teknologi informasi juga telah dilakukan oleh Perseroan. Perseroan telah melakukan implementasi kebijakan teknologi informasi secara efektif.

Berikut beberapa hal terkait pengelolaan Tata Kelola Teknologi Informasi pada Perseroan:

Kemananan Maya (*Cyber Security*) dan Gangguan (*Disruption*)

Perseroan telah memiliki beberapa kebijakan terkait keamanan dan gangguan cyber yang bertujuan untuk menghindari serangan cyber ataupun mengamankan Perseroan sendiri.

No.	Daftar Kebijakan
1	Kebijakan Dasar Manajemen Risiko Penggunaan TI
2	Kebijakan Pengamanan Informasi Kanwil dan Cabang
3	Kebijakan Pengamanan Informasi KP
4	Panduan Pengamanan Informasi Kanwil dan Cabang
5	Panduan Pengelolaan User ID dan *Password*
6	Panduan Sekuriti RACF
7	Pedoman Sekuriti Key Management System
8	Pedoman Sekuriti Network KP
9	Pedoman Sekuriti Network Kanwil/Cabang
10	Pedoman Sekuriti Tandem
11	Pedoman Sekuriti UNIX (Solaris)
12	Pedoman Sekuriti Linux
13	Pedoman Sekuriti User ID dan Password
14	Pedoman Sekuriti Windows
15	Manual Kerja Pengelolaan Sekuriti LAN
16	Manual Sekuriti Base24
17	Manual Sekuriti BDS IBS
18	Manual Sekuriti CardLink

19	Manual Key *Management Host to Host* ERP
20	Panduan Kerja Sistem Sekuriti Tandem
21	Pedoman Pemasangan Wireless Local Area Network (WLAN)
22	Pedoman Penggunaan Media Sosial, Internet dan Email
23	Pedoman Pengamanan ATM
24	Pedoman Sekuriti BYOD
25	Remote Access

Implementasi

Pelaksanaan tata kelola terkait *Cyber Security* pada Perseroan :

- Melakukan *awareness* ke segenap kantor Cabang/Kantor Wilayah berupa kunjungan ke Cabang/ Kantor Wilayah melalui Forum Diskusi atau Rapat Koordinasi Wilayah.
- Melakukan *awareness* ke segenap staf Kantor Pusat berupa COP (*Community of Practice)*
- Mewajibkan seluruh staf Kantor Pusat /Cabang/ Kantor Wilayah untuk mengikuti *e-learning*
- Pembuatan video *cyber security* untuk *awareness* yang diputarkan di media KP (TV media)
- Mengirimkan email-email *awareness* ke seluruh staf Kantor Pusat /Cabang/ Kantor Wilayah
- Melakukan *Phising test* ke seluruh staf yang memiliki hak akses bca.co.id
- Pembahasan dalam meeting BOD atau BOC terkait Teknologi Informasi selama tahun 2018.

Penilaian/*Assessment*

Berdasarkan *assessment* yang pernah dilakukan oleh Kominfo pada tahun 2018 penerapan Cyber Security Perseroan sudah dinyatakan sangat baik.

Pemulihan Bencana (*Disaster Recovery*)

Kebijakan Pemulihan Bencana dan Penanganan Keadaan Darurat diatur dalam Kebijakan *Business Continuity* Terintegrasi Konglomerasi Keuangan Perseroan berdasarkan Surat Keputusan Direksi No. 180/SK/DIR/2017 tanggal 11 Desember 2017. *Business Continuity* Terintegrasi Konglomerasi Keuangan Perseroan adalah penerapan *Business Continuity* untuk memastikan kelangsungan usaha Perseroan dan Anggota Konglomerasi Keuangan Perseroan pada saat terjadi gangguan. Hal-hal yang diatur dalam kebijakan dimaksud antara lain terkait kebijakan *business continuity plan*, protokol dari Perseroan ke anggota Konglomerasi Keuangan Perseroan dan sebaliknya serta urutan prioritas *Recovery*.

Latar Belakang	Kegiatan operasional Perseroan tidak dapat terhindar dari adanya gangguan/ kerusakan yang disebabkan oleh alam maupun manusia. Kerusakan yang terjadi tidak hanya berdampak pada kemampuan teknologi Perseroan, tetapi juga berdampak pada kegiatan operasional bisnis Perseroan terutama pelayanan kepada nasabah.
Terkait BCM	Untuk meminimalisasi risiko tersebut di atas, Perseroan memiliki *Business Continuity Management* (BCM). BCM adalah proses manajemen terpadu dan menyeluruh mengenai dampak potensi apabila kritikal bisnis dari Perseroan tidak dapat berfungsi karena adanya gangguan/bencana, guna melindungi kepentingan para stakeholder. BCM merupakan bagian yang terintegrasi dengan Kebijakan Manajemen Risiko Perseroan secara keseluruhan.
Pendukung	Agar BCM dapat berjalan efektif, maka BCM Perseroan didukung dengan: • Keterlibatan aktif manajemen. • Dilakukannya *Risk Assessment* dan *Business Impact Analysis*. • Penyusunan *Business Continuity Plan* (BCP) yang memadai. • Dilakukannya pengujian BCP. • Dilakukannya pemeriksaan oleh Divisi Audit Internal.