PEDOMAN
ETIKA DAN PERILAKU
CODE OF CONDUCT SI

PT Wijaya Karya Beton Tbk.

SE.02.09/WB-0A.02.114/2012

Klasifikasi Keamanan: Proprietary

D A F T A R I S I

LEMBAR PENGESAHAN *CODE OF CONDUCT*
PT Wijaya Karya Beton Tbk

Direksi,

Rija Judaswara
Direktur Pemasaran dan Pengembangan

Manajer Divisi,

Fachrul Rozi
Manajer Divisi Sistem Informasi

Manajer Bidang,

Ade Maksum
Manajer Bidang Enterprise Resource Planning

Akhmat Sofanul Adi
Manajer Bidang Network, Infrastruktur dan Support

PEDOMAN
ETIKA DAN PERILAKU
CODE OF CONDUCT 2023

BAB I
Pendahuluan

BAB I. PENDAHULUAN

1.1. Latar Belakang, Sistematika Etika dan Tata Perilaku Sistem Informasi

(Code of Conduct IT)

Sebagai bagian dari manajemen perusahaan dalam komitmen untuk melaksanakan praktik-praktik *Good Corporate Governance* atau Tata Kelola perusahaan yang baik sebagai bagian dari usaha untuk pencapaian Visi dan Misi Perusahaan. *Code of Conduct* Sistem Informasi ini merupakan salah satu bentuk wujud komitmen tersebut dan menjabarkan Tata Nilai Unggulan PT Wijaya Karya Beton Tbk., yaitu *transparency, accountability, responsibility, indepedency* dan *fairness* ke dalam interpretasi prilaku yang terkait dengan etika dan tata perilaku sistem informasi.

Etika dan Tata Perilaku Sistem Informasi (*Code of Conduct IT*) ini disusun untuk menjadi acuan bagi Komisaris, Direksi Pegawai dan tenaga kerja yang terlibat dalam kegiatan usaha sebagai insan WIKA Beton dalam mengelola perusahaan guna mencapai Visi, Misi dan tujuan perusahaan.

1.2. Tujuan Etika dan Tata Perilaku Sistem Informasi

(Code of Conduct IT)

Penerapan Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT)* ini dimaksudkan untuk:

1.2.1. Mengidentifikasi nilai-nilai dan standar etika sistem informasi yang selaras dengan Visi dan Misi Perusahaan

1.2.2. Menjabarkan Tata Nilai sebagai landasan etika dan perilaku yang harus diikuti oleh *user* WIKA Beton dalam menggunakan fasilitas Sistem Informasi Perusahaan.

1.2.3. Menjelaskan secara rinci standar etika agar *user* WIKA Beton dapat menilai bentuk kegiatan yang dilakukan dan membantu memberikan pertimbangan dalam berinteraksi dengan Sistem Informasi perusahaan.

1.2.4. Mengatur keamanan informasi dan kerahasiaan data meliputi pengamanan terhadap infrastruktur.

1.2.5. Menghindarkan perusahaan dari tuntutan hukum dari pihak ketiga.

1.3. Ruang Lingkup

Pedoman Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT)* ini penerapannya meliputi seluruh Infrastruktur Sistem Informasi yang terdapat di lingkungan Perusahaan WIKA Beton.

1.4. Istilah Penting

Dalam Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT)* ini yang dimaksud dengan:

1.4.1. *Corporate Governance* adalah struktur dan proses yang digunakan oleh organ perusahaan untuk meningkatkan keberhasilan usaha dan akuntabilitas perusahaan guna mewujudkan nilai pemegang saham dalam jangka panjang dengan tetap memperhatikan kepentingan *stakeholders* lainnya, berlandaskan peraturan perundang-undangan dan nilai-nilai etika.

1.4.2. Etika adalah sekumpulan norma atau nilai yang tidak tertulis yang diyakini oleh suatu kelompok masyarakat sebagai suatu standar perilaku kelompok tersebut.

1.4.3. *Good Corporate Governance* adalah komitmen, aturan main dan praktik penyelenggaraan bisnis yang sehat dan beretika.

1.4.4. Insan WIKA Beton adalah Komisaris beserta perangkatnya, Direksi, Pegawai dan tenaga kerja yang terlibat dalam kegiatan usaha PT Wijaya Karya Beton Tbk.

1.4.5. *Steering Committee* adalah Komite yang dibentuk oleh Direksi untuk memantau efektivitas pelaksanaan Sistem Informasi perusahaan.

1.4.6. Pejabat yang Bertanggung Jawab atas penerapan Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT)* meliputi para Direktur, Manajer Divisi, Manajer unit kerja dan pejabat lain setingkat Manajer.

1.4.7. *User* adalah insan WIKA Beton yang secara langsung menggunakan perangkat Sistem Informasi Perusahaan.

1.4.8. Pegawai adalah orang yang bekerja dan terdaftar sebagai pegawai pada PT Wijaya Karya Beton Tbk. berdasarkan surat ketetapan / keputusan resmi dengan menerima gaji.

1.4.9. Perusahaan adalah PT Wijaya Karya Beton Tbk., kecuali dalam konteks kalimat tertentu mempunyai arti perusahaan yang umum.

1.4.10. *Hardware* adalah semua bagian fisik komputer, dan peralatan yang berfungsi untuk mendukung proses komputerisasi.

1.4.11. *Software* adalah istilah umum untuk data yang diformat dan disimpan secara digital, termasuk program komputer.

1.4.12. Aplikasi adalah suatu subkelas perangkat lunak komputer yang memanfaatkan kemampuan komputer langsung untuk melakukan suatu tugas yang diinginkan pengguna.

1.4.13. *Server* adalah sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer.

1.4.14. *VOIP (voice over internet protocol)* adalah teknologi yang memungkinkan percakapan suara jarak jauh melalui media internet.

1.4.15. *File* adalah identitas dari data yang disimpan di dalam sistem berkas yang dapat diakses dan diatur oleh pengguna.

1.4.16. *Password* adalah kumpulan karakter atau string dan numerik yang digunakan oleh *user* pada sebuah sistem operasi yang mendukung banyak pengguna *(multiuser)* untuk memverifikasi identitas dirinya.

1.4.17. *Account* adalah identitas seorang pengguna dalam mengakses suatu entitas sistem.

1.4.18. Infrastruktur adalah sumber daya teknologi bersama yang menyediakan platform untuk aplikasi sistem informasi perusahaan yang terperinci.

1.4.19. DSI adalah Divisi Sistem Informasi.

1.4.20. *VA (Vulnerability Assessment)* adalah merupakan proses untuk mengidentifikasi, mengevaluasi, dan mengklasifikasikan tingkat risiko pada kerentanan keamanan yang ada pada sebuah jaringan komputer, sistem, aplikasi, atau bagian lain yang ada di ekosistem IT.

1.4.21. *Pentest (Penetration Testing)* adalah serangkaian metode untuk menemukan celah keamanan.

1.4.22. *SLA* adalah kesepakatan secara formal antara Penyedia Layanan dengan pelanggan seputar komitmen pelayanan yang diterima dan diberikan, dengan sejumlah ukuran performansinya

1.4.23. *ITSC* adalah Information Technology Steering Committee

1.4.24. *CMDB (Configuration Management Data Base)* adalah untuk basis data yang menyimpan informasi di mana sebagian besar proses TI, incident, problem, *change* and *asset management* bergantung padanya untuk dapat beroperasi dengan baik

1.4.25. RPO (Recovery Point Objective) adalah jumlah data yang dapat ditoleransi untuk hilang setelah kejadian yang tidak terduga terjadi, seperti kegagalan sistem atau bencana alam

1.4.26. *NDA (Non-Disclosure Agreement*) adalah suatu kontrak dalam hubungan kerja profesional yang mengikat secara hukum dan bersifat konfidensial.

1.4.27. Commercial off the self (COTS) adalah produk-produk yang berupa suatu paket aplikasi, sub sistem ataupun modul-modul perangkat lunak yang telah dirancang sesuai dengan suatu standard proses bisnis tertentu dan tersedia secara luas di pasar untuk dapat dipergunakan dengan modifikasi seminimal mungkin. Contoh aplikasi: Ms. Word, Adobe Photoshop, dll.

Infrastruktur SI meliputi perangkat keras *(hardware)*, perangkat lunak *(software)*, dan jaringan komunikasi yang tersebar di seluruh perusahaan atau tersebar di seluruh unit kerja perusahaan.

PEDOMAN
ETIKA DAN PERILAKU
CODE OF CONDUCT 2023

BAB II
Etika Bisnis Perusahaan

BAB II. STANDAR ETIKA DAN TATA PERILAKU SISTEM INFORMASI

Sarana dan Fasilitas Sistem Informasi Perusahaan hanya digunakan dan dimanfaatkan oleh insan WIKA Beton dan dimanfaatkan sebagai sarana untuk pendukung pekerjaan dan kepentingan Perusahaan. Sarana dan Fasilitas Sistem Informasi Perusahaan meliputi seperti dibawah ini, tetapi tidak terbatas pada:

- *Software (Email, OS, Finance dan HRMS, SIM)*
- *Hardware* dan Jaringan Komunikasi (*server*, komputer, *notebook*, *printer, voip, router*, *firewall*, ruang *server*, *switch*)
- Internet
- Dan lain-lain.

Penggunaan dan Pemanfaatan Sarana dan Fasilitas Sistem Informasi Perusahaan diatur dengan ketentuan sebagai berikut:

2.1. Tata Kelola Sistem Informasi Perusahaan

2.1.1. Pengelolaan *Master Plan* TI

2.1.1.1. *Master Plan* TI terdiri dari *Master Plan* TI WIKA Beton.;

2.1.1.2. *Master Plan* TI WIKA Beton mencakup arsitektur TI dan *roadmap* untuk layanan TI Induk Perusahaan dan layanan TI bersifat *shared services* yang akan digunakan bersama-sama oleh seluruh anak perusahaan, dengan mekanisme pengelolaan sebagai berikut:

a. Unit Pengelola TI melakukan kajian dan mengusulkan kepada manajemen, berkonsultasi dengan Unit Kerja Pemilik Bisnis dan Direksi Anak Perusahaan;
b. *IT Steering Committee* melakukan review dan memberikan masukan perbaikan jika diperlukan;
c. Dewan Direksi WIKA Beton memutuskan melalui Keputusan Direksi;
d. Unit Pengelola TI melaksanakan Master Plan TI yang telah ditetapkan dalam Keputusan Direksi.

2.1.2. Pengelolaan Kebutuhan Bisnis akan Layanan TI

2.1.2.1. Kebutuhan bisnis untuk level WIKA Beton mencakup layanan TI yang digunakan di WIKA Beton dan layanan *shared services* yang akan digunakan oleh seluruh anak perusahaan. Pengelolaan kebutuhan bisnis untuk level WIKA Beton diatur sebagai berikut:

a. Kebutuhan bisnis untuk level WIKA Beton dianalisa setiap tahun, yang akan menjadi dasar dalam penentuan belanja TI tahunan WIKA Beton;
b. Unit Pengelola TI atau Unit Pemilik Proses Bisnis dapat mengusulkan kebutuhan bisnis akan layanan TI, dengan merujuk kepada *Master Plan* TI atau perkembangan bisnis kontemporer. Unit Pengelola TI mengkompilasi seluruh usulan kebutuhan bisnis akan Layanan TI;
c. Kebutuhan bisnis mempertimbangkan aspek pengamanan informasi dengan ketentuan sebagai berikut.
    1) *Business Requirement* mengidentifikasi informasi sensitif yang dikelola oleh sistem dan klasifikasi informasinya;
    2) *Business Requirement* mempertimbangkan persyaratan hukum, peraturan perundangan maupun persyaratan kontrak terkait manajemen pengamanan informasi;
    3) *Risk assessement* dilakukan untuk memastikan isu dalam *Business Requirement* dikelola sesuai dengan kriteria risiko yang telah ditetapkan.

d. *IT Steering Committee* melakukan review atas hasil kompilasi Kebutuhan Bisnis tahunan, untuk memastikan keselarasan dengan *Master Plan* TI atau dinamika bisnis;
e. Dewan Direksi WIKA Beton menyetujui Kebutuhan Bisnis TI tahunan sebagai dasar untuk penetapan anggaran TI tahunan.

2.1.3. Pengelolaan Belanja TI

2.1.3.1. Pengelolaan belanja TI di level WIKA Beton diatur sebagai berikut:

a. Unit Pengelola TI WIKA Beton mengusulkan belanja TI tahunan berdasarkan hasil analisa kebutuhan bisnis akan layanan TI tahunan yang telah disetujui oleh Dewan Direksi, berkonsultasi dengan Unit Pemilik Proses Bisnis;
b. *IT Steering Committee* mereview usulan belanja tahunan TI, dan memberikan masukan perbaikan jika diperlukan;
c. Dewan Direksi WIKA Beton menyetujui dan menetapkan belanja TI tahunan WIKA Beton;
d. Unit Pengelola TI melaksanakan belanja TI yang telah disetujui Dewan Direksi berdasarkan ketentuan penganggaran dan keuangan yang berlaku.

2.1.4. Pengelolaan Standar dan Portofolio Arsitektur TI

2.1.4.1. Standar dan portofolio teknologi ditetapkan sebagai mekanisme kontrol untuk memastikan interoperabilitas dan keamanan seluruh teknologi yang diimplementasikan di WIKA Beton dan anak perusahaan;

2.1.4.2. Standar dan teknologi terkait layanan WIKA Beton atau shared services diusulkan oleh Unit Pengelola TI WIKA Beton dan disetujui oleh *IT Steering Committee*;

2.1.4.3. Standar dan teknologi terkait layanan spesifik anak perusahaan diusulkan oleh Unit Pengelola TI anak perusahaan dan disetujui oleh Unit Pengelola TI WIKA Beton.

2.1.5. Kebijakan dan SOP TI

2.1.5.1. Unit Pengelola TI di WIKA Beton dan anak perusahaan melaksanakan kebijakan dan Pedoman Tata Kelola dan Pengelolaan TI yang telah ditetapkan.

2.1.5.2. Unit Pengelola TI WIKA Beton mengusulkan SOP TI (baik baru atau perubahannya) yang akan digunakan seluruh lingkungan perusahaan, berkonsultasi dengan fungsi audit internal WIKA Beton;

2.1.6. Pengelolaan Risiko dan kesinambungan layanan Teknologi Informasi

2.1.6.1. Unit Pengelola TI bertanggung jawab untuk mengidentifikasi setiap kejadian (ancaman dan kerawanan) di lingkungan Teknologi Informasi yang memberikan dampak terhadap tujuan dan/atau operasional Perusahaan, termasuk aspek bisnis, regulasi, hukum, teknologi, mitra kerja, sumber daya manusia, dan aspek operasi;

2.1.6.2. Unit Pengelola TI bertanggung jawab untuk melaksanakan *Risk Assessment* berdasarkan kerangka kerja pengelolaan risiko yang telah ditetapkan oleh Perusahaan;

2.1.6.3. Unit Pengelola TI harus memberikan dukungan terhadap implementasi *Business Continuity Plan (BCP)* melalui layanan Teknologi Informasi yang berkesinambungan *(Continuous IT Services)* yang memungkinkan bisnis Perusahaan berjalan dalam standar minimum yang telah ditetapkan;

2.1.6.4. Pengaturan lebih detail terkait sekuriti Teknologi Informasi akan ditetapkan dalam *Standar Operational Procedure (SOP).*

2.1.7. Pengelolaan Sumber Daya dan Aset Teknologi Informasi

2.1.7.1. Pengadaan sumber daya Teknologi Informasi, mencakup perangkat keras, perangkat lunak, dan jasa Teknologi Informasi, harus mengacu kepada peraturan proses pengadaan yang berlaku di Perusahaan;

2.1.7.2. Unit Pengelola TI bersama unit pengelola Aset secara bersama melakukan pengelolaan aset sistem informasi Perusahaan sesuai tugas dan tanggung jawab yang ditetapkan termasuk didalamnya aset lisensi perangkat lunak *(software)* yang meliputi pembukuan, pemeliharaan dan penghapusan;

2.1.7.3. Unit Pengelola Teknologi Informasi bertanggung jawab terhadap legalitas lisensi perangkat lunak *(software)* termasuk didalamnya *operating system*, paket aplikasi, *database, network operating system,* pemenuhan jumlah lisensi sesuai kebutuhan serta peremajaan lisensi perangkat lunak yang digunakan.

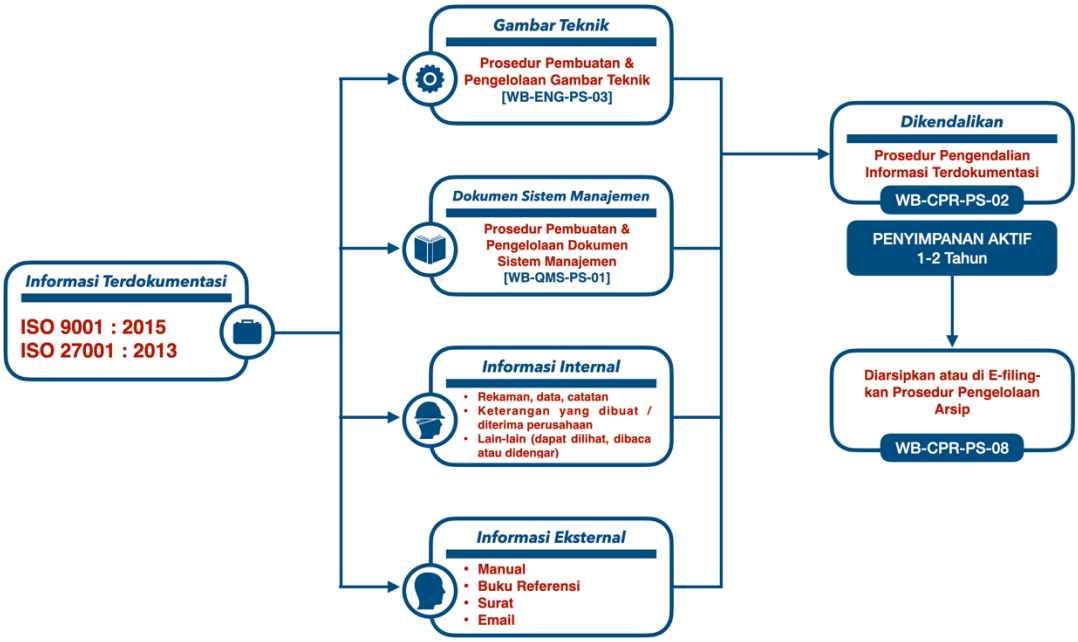
2.1.7.4. Unit Pengelola Teknologi Informasi bertanggung jawab terhadap legalitas lisensi perangkat lunak *(software)* termasuk didalamnya *operating system*, paket aplikasi, *database, network operating system,* pemenuhan jumlah lisensi sesuai kebutuhan serta peremajaan lisensi perangkat lunak yang digunakan.

2.1.7.5. Unit Pengelola Teknologi Informasi tidak bertanggung jawab bila pegawai mengunduh atau meng-*install* perangkat lunak *(software)* dan mendapatkan denda atau pinalti dari pemilik perangkat lunak *(software)* tersebut. Semua bentuk denda atau pinalti adalah tanggung jawab pegawai tersebut

2.1.7.6. Setiap aset diperlakukan sesuai dengan klasifikasi informasi pada aset tersebut. Berikut ini merupakan pedoman bagi perusahaan untuk menerapkan klasifikasi informasi perusahaan.

a. Seluruh aset informasi perusahaan dinilai dan diklasifikasikan sesuai dengan konten aset tersebut;
b. Kriteria utama dalam klasifikasi diantaranya adalah ketentuan hukum, nilai informasi terhadap perusahaan, kritikalitas informasi, dan sensitivitas terhadap modifikasi serta kebocoran informasi;
c. Pengklasifikasian ulang dilakukan secara berkala, mengingat sensitivitas aset bisa berubah dari waktu ke waktu.

2.1.7.7. Penanganan aset sesuai dengan klasifikasi sebagai berikut.



2.1.7.8. Setiap aset diberikan label sesuai dengan klasifikasi informasi aset tersebut. Terutama aset dengan klasifikasi informasi internal maupun rahasia. Berikut pedoman pelabelan informasi.

a. Dokumen Cetak
   1) Dokumen cetak diberi label dengan *watermark* pada setiap halaman sesuai dengan klasifikasi informasi;
   2) Jika tidak mungkin, diberi tulisan pada halaman depan dan *footer* setiap halaman sesuai dengan klasifikasinya.

b. Media Penyimpanan
   Pemberian label pada tempat penyimpanan sesuai dengan klasifikasi informasi;
c. Pesan Eletronik
   1) Pemberian pernyataan klasifikasi informasi pada pesan elektronik;
   2) Apabila informasi berupa *attachment* pesan elektronik maka label klasifikasi informasi dinyatakan pada header tiap halaman dokumen.

2.1.7.9. Aset bisa dilakukan *disposal* termasuk aset berupa media yang memuat informasi. Ketentuan disposal sebagai berikut.

a. Permintaan disposal media diajukan pada *IT Service desk*, disertai dengan pemilik, jenis media, nomer seri, serta klasifikasi informasi yang ada;
b. Apabila dibutuhkan, data yang tersimpan di-*backup* terlebih dahulu;
c. Apabila terdapat media yang telah dikumpulkan untuk dimusnahkan namun belum dimusnahkan, *IT Service desk* bertanggung jawab terhadap keamanan media tersebut.
d. Setelah media dikumpulkan, detail informasi tentang media di-*update* pada Aplikasi Inventory;
e. Perusahaan dapat memusnahkan media menggunakan *disk shredder* dengan ketentuan pemusnahan disaksikan lebih dari satu orang, atau menggunakan jasa dari pihak ketiga dengan ketentuan terdapat sertifikat *disposal*; dan
f. Setelah media dimusnahkan, detail informasi tentang media di-update pada Aplikasi Inventory.

2.1.8. Pengelolaan Sumber Daya Manusia Teknologi Informasi

2.1.8.1. Pegawai menandatangani kontrak yang memuat kepatuhan terhadap hukum yang berlaku dan aturan pengamanan informasi;

2.1.8.2. Unit Pengelola TI bertanggung jawab untuk meminimalkan ketergantungan kepada individu tertentu terhadap suatu proses atau pengetahuan aplikasi / sistem yang kritikal dengan terselenggaranya proses *knowledge sharing*, dokumentasi, *succession planning* dan penyediaan *backup staff;*

2.1.8.3. Unit Pengelola TI bertanggung jawab untuk mengusulkan kepada Unit *Human Resource* mengenai *job description* pengelolaan Teknologi Informasi Perusahaan beserta standar kompetensi yang dibutuhkan agar terjadi efisiensi dan efektivitas pengelolaan Teknologi Informasi, tidak terjadi tumpang tindih penugasan, dan terdapat *segregation of duties* yang jelas;

2.1.8.4. Kualitas staf profesional sistem informasi baik untuk bidang teknis maupun bidang pengelolaan sistem informasi harus dijamin telah melalui program pelatihan dan pengembangan keahlian dan kompetensi yang berkesinambungan, khususnya berdasarkan hasil evaluasi performansi dan kompetensi, serta pelaksanaan sertifikasi keahlian yang sesuai;

2.1.8.5. Pengelolaan Teknologi Informasi oleh jasa pihak ketiga dimungkinkan dalam rangka pencapaian sasaran bisnis Perusahaan dan efisiensi sumber daya manusia Teknologi Informasi pada bidang-bidang pekerjaan yang ditinjau dari segi proses bisnis, teknis, keahlian dan biaya layak untuk dilaksanakan dan tidak terjadi tumpang tindih dengan pengelolaan Teknologi Informasi secara swakelola.

2.2. *Software* Sistem Informasi Perusahaan

2.2.1. Pengembangan atau Implementasi *Software* Aplikasi

2.2.1.1. Pengembangan atau implementasi software aplikasi hanya dapat dilakukan oleh Unit Pengelola TI WIKA Beton dan Unit Pengelola TI Anak perusahaan, dengan lingkup software aplikasi merujuk kepada mekanisme pengelolaan kebutuhan bisnis akan layanan TI dan belanja TI;

2.2.1.2. Strategi pengembangan atau implementasi *software* aplikasi harus mempertimbangkan strategi sumberdaya yang panduan awalnya telah diberikan oleh Master Plan TI, yang mencakup:

a. Tipe solusi dapat bersifat *tailor-made* atau COTS;

b. Tipe pengembangan dapat bersifat *insourcing*, *co-sourcing* atau *outsourcing*;
c. Tipe pengoperasian layanan dapat bersifat insourcing atau outsourcing.

2.2.1.3. Dalam melakukan pengembangan atau implementasi *software* aplikasi, Unit Pengelola TI WIKA Beton atau anak perusahaan harus merujuk kepada SOP TI atau *good practices* terkait:

a. *System Development Life Cycle* terkait *software* aplikasi;
b. Manajemen Proyek;
c. Kecukupan *Application Control.*

2.2.1.4. Ketentuan pengamanan informasi dalam proses analisis dan desain sebagai berikut.

a. *Security architecture* disusun berdasarkan kebutuhan pengamanan informasi dan risk assessment yang sudah dilakukan;
b. Analisis dan Desain keamanan sistem meliputi:
   1) Kendali input;
   2) Kendali pemrosesan;
   3) Kendali output.

2.2.1.5. Ketentuan pengamanan informasi dalam proses development sebagai berikut.

a. Pengembangan dilakukan dalam *secure Development environment*;
b. Pengembangan mengikuti *secure coding*/*configuration guideline*;
c. Evalausi pengembangan dilakukan untuk memastikan berbagai ancaman dikelola dalam *risk assesment*;
d. Setiap pengembangan harus menggunakan source code atau program yang terakhir pada repositori source code atau source program yang ada.
e. Setiap programmer berkewajiban melakukan *back-up coding* selama masa pengembangan baik dalam bentuk softcopy maupun dalam media penyimpanan lainnya;
f. Setelah melewati pengujian dan telah dinyatakan dapat diimplementasikan ke lingkungan *production*, *source code* atau *source* program tersebut disimpan secara terpusat.

2.2.1.6. Ketentuan pengamanan informasi dalam proses *testing* sebagai berikut.

a. Pengujian kendali keamanan dilakukan berdasarkan persyaratan pengaman yang telah diidentifikasi;
b. Pengujian keamanan juga dilakukan oleh tim *Testing* yang terpisah dari tim pengembangan;
c. Pengendalian dilakukan untuk memproteksi data pengujian;
d. Data *sensitive* tidak digunakan sebagai data pengujian.

2.2.1.7. Ketentuan lingkungan pengembangan yang aman sebagai berikut.

a. Proses pengembangan, pengujian dan rilis ke lingkungan produksi dilakukan oleh personil yang berbeda;
b. *Environment* pengembangan, pengujian dan operasional dipisahkan;
c. Pengembang tidak memiliki akses ke lingkungan pengujian maupun operasional termasuk akses setelah *go-live*;
d. Kode, program dan komponen konfigurasi lainnya disimpan dalam repositori yang aman

2.2.2. Operasi dan Pemeliharaan Aplikasi

2.2.2.1. Unit Pengelola TI bertanggung jawab atas ketersediaan aplikasi yang dibutuhkan melalui aplikasi otomasi yang tepat dan selaras dengan kebutuhan bisnis;

2.2.2.2. Unit Pengelola TI harus memastikan adanya prosedur yang mengatur operasi dan pemeliharaan aplikasi;

2.2.2.3. Unit Pengelola TI bertanggung jawab atas pelaksanaan operasi dan pemeliharaan aplikasi;

2.2.2.4. Unit Pengelola TI bertanggung jawab atas penyusunan prosedur atas *End User Computing (EUC)* yang digunakan untuk proses laporan keuangan, performansi Perusahaan maupun input sistem aplikasi utama dengan mempertimbangkan keamanan, ketersediaan, dan integritas pada saat pemrosesan;

2.2.2.5. Dalam setiap implementasi aplikasi, perlu dilakukan *Post Implementation Review (PIR)* melalui suatu prosedur baku, untuk mengevaluasi efektivitas sistem aplikasi setelah implementasi dan menilai keberhasilan suatu implementasi aplikasi dalam hal fungsionalitas, performansi, keamanan, biaya versus keuntungan *(cost benefit)* termasuk proses pengembangannya;

2.2.2.6. Secara periodik Unit Pengelola TI bertanggung jawab untuk melakukan evaluasi performansi aplikasi terhadap target yang ditetapkan, melakukan *root cause analysis* dan melakukan inisiasi tindakan perbaikan terhadap kasus yang terjadi.

2.2.3. Implementasi Infrastruktur TI

2.2.3.1. Implementasi infrastruktur TI hanya dapat dilakukan oleh Unit Pengelola TI WIKA Beton dan Unit Pengelola TI Anak perusahaan, dengan lingkup infrastruktur merujuk kepada mekanisme pengelolaan kebutuhan bisnis akan layanan TI dan belanja TI;

2.2.3.2. Dalam melakukan implementasi infrastruktur TI, Unit Pengelola TI WIKA Beton atau anak perusahaan harus merujuk kepada SOP TI atau *good practices* terkait:

a. *System Development Life Cycle* terkait infrasruktur TI.

b. Manajemen Proyek.

2.2.4. Pengelolaan Perubahan

2.2.4.1. Unit Pengelola TI bertanggung jawab untuk memastikan bahwa setiap perubahan terhadap aset TI sudah melalui proses *assessment*, persetujuan, pengujian, implementasi dan review yang terkontrol;

2.2.4.2. Unit Pengelola TI harus mendefinisikan kriteria klasifikasi perubahan mulai dari minor sampai dengan mayor, ruang lingkup perubahan serta mekanisme perubahan darurat;

2.2.4.3. Setiap perubahan harus melalui mekanisme persetujuan dan pengujian sesuai prosedur yang berlaku serta dikomunikasikan kepada pelanggan layanan terkait ataupun pihak-pihak yang terkena dampak;

2.2.4.4. Unit Pengelola TI perlu menganalisis data perubahan sebagai referensi *Continual Improvement* serta harus melaporkan setiap perubahan yang terjadi pada layanan TI yang berlaku dalam rangka evaluasi pencapaian Tingkat Layanan (*Service Level*).

2.2.5. Pengelolaan Aset dan Konfigurasi TI

2.2.5.1. Unit Pengelola TI bertanggung jawab untuk mengelola aset-aset TI beserta konfigurasinya secara efektif melalui manajemen konfigurasi;

2.2.5.2. Aset TI terdiri dari aset utama (Proses bisnis dan aktivitas) dan aset pendukung (*Hardware, Software, Network, Personel, Site, Struktur Organisasi*)

2.2.5.3. Setiap Aset ataupun Configuration Item harus diidentifikasi secara unik dengan mendefinisikan segala atribut yang menunjukan karakteristik fungsional maupun fisik aset TI tersebut kemudian mencatat dan menyimpannya ke dalam CMDB;

2.2.5.4. Setiap perubahan konfigurasi baik itu berupa penambahan, modifikasi, pemindahan, penghapusan harus melalui proses Manajemen Perubahan;

2.2.5.5. Proses verifikasi terhadap CI harus dilakukan secara berkala untuk memastikan integritas data aset TI terkait.

2.2.5.6. Semua Aset TI dikelola dalam aplikasi *Inventory*

2.2.6. Hal-hal yang tidak diperkenankan:

2.2.6.1. Melakukan perbuatan secara sengaja yang menyebabkan kerusakan pada fasilitas *Software* Sistem Informasi milik Perusahaan.

2.2.6.2. Memanfaatkan fasilitas *Software* dan Data Sistem Informasi Perusahaan diluar kepentingan pekerjaan.

2.2.6.3. Memindahkan, memasang, menginstall *software* ke dalam perangkat Sistem Informasi Perusahaan, kecuali atas izin Manajer Sistem Informasi dan penanggung jawab Sistem Informasi yang ditunjuk di masing-masing unit kerja.

2.2.6.4. Menggunakan fasilitas *Software* Sistem Informasi Perusahaan yang melanggar norma agama, sosial dan kesusilaan.

2.2.6.5. Memperbaiki gangguan atau kerusakan pada fasilitas *software* sistem Informasi perusahaan kecuali oleh penanggung jawab Sistem Informasi yang ditunjuk di masing-masing unit kerja.

2.2.6.6. Menginstall *file games* / permainan pada semua fasilitas sistem informasi Perusahaan.

2.2.6.7. Memberikan *username* dan password kepada orang lain.

2.2.6.8. Menggunakan komputer yang sudah *login* dengan menggunakan *username* pengguna lain.

2.2.6.9. Menyalahgunakan, meng-*copy*, menjiplak, menggandakan *system* / pemrograman / data maupun informasi, diluar kepentingan Perusahaan.

2.2.6.10. Memanfaatkan fasilitas *email* bagi kepentingan pribadi diluar kepentingan perusahaan, seperti; Kepentingan komersial (MLM, undian, lowongan pekerjaan, jual beli, dll) Kepentingan umum yang dapat mengakibatkan rusaknya reputasi perusahaan di hadapan publik. Mengganggu atau mengintimidasi orang lain (informasi yang menyangkut SARA, pornografi, hasutan, pesan-pesan yang tidak berhubungan dengan pekerjaan, dll).

2.2.6.11. Membuka *email* atau pesan dari siapapun yang terlihat mencurigakan dapat merusak *system* keamanan Sistem Informasi Perusahaan.

2.2.6.12. Mengirim *email* atau *file attachment* apapun juga yang melebihi kapasitas yang sudah ditentukan tanpa persetujuan DSI.

2.2.6.13. Menyimpan *file* / data yang tidak berhubungan dengan kepentingan perusahaan ke dalam *fileserver*, dan apabila ditemukan oleh DSI maka *file* tersebut akan dihapus tanpa pemberitahuan terlebih dahulu.

2.2.6.14. Tidak diperkenankan menggunakan *email* pribadi untuk kepentingan perusahaan. Kecuali jika tidak memiliki *email* perusahaan (contoh magang)

2.2.7. Hal-hal yang diwajibkan:

2.2.7.1. Melaporkan atau menginformasikan segala kelemahan atau kerusakan dari *software* sistem informasi Perusahaan kepada jajaran DSI.

2.2.7.2. Melaporkan atau menginformasikan setiap adanya kemungkinan penyalahgunaan atau pelanggaran norma susila, agama dan lainnya pada *software* sistem informasi Perusahaan kepada DSI.

2.2.7.3. Bertanggung jawab penuh untuk menjaga kerahasiaan *username* dan *password* yang diberikan oleh perusahaan.

2.2.7.4. Melakukan *logout* setelah selesai dalam suatu *session*/pekerjaan.

2.2.7.5. Bertanggung jawab atas akses kepemilikan *username* dan *password* selaku pemilik *account*.

2.2.7.6. Merawat dan memanfaatkan fasilitas *email account* yang diberikan Perusahaan secara maksimal dalam mendukung pekerjaan.

2.2.7.7. Mengamankan data informasi perusahaan sesuai dengan tingkat tanggung jawabnya masing-masing baik berupa data *master*, data transaksi maupun hasil proses, karena data tersebut pada dasarnya adalah milik WIKA Beton.

2.2.7.8. Mengakses materi, data dan dokumen pada perangkat sistem informasi bagi pegawai yang ditunjuk dan diberi wewenang sesuai dengan fungsi dan jabatan yang menjadi tanggung jawabnya.

2.2.7.9. Menjaga agar meja selalu bersih dan tidak terdapat dokumen yang bersifat rahasia berserakan *(clear desk)*

2.3. *Hardware* dan Jaringan Komunikasi Sistem Informasi Perusahaan.

2.3.1. Operasi dan Pemeliharaan Infrastruktur

2.3.1.1. Unit Pengelola TI bertanggung jawab untuk memastikan ketersediaan, kapasitas dan integritas infrastruktur untuk mendukung kelancaran aplikasi bisnis;

2.3.1.2. Penyediaan infrastruktur Teknologi Informasi dapat dilakukan oleh jasa pihak ketiga;

2.3.1.3. Pengelolaan sekuriti yang mencakup perlindungan fisik, pembatasan akses dan pengelolaan inventory dilakukan terhadap infrastruktur Teknologi Informasi, terutama yang kritikal bagi kelangsungan bisnis;

2.3.1.4. Pengelola infrastruktur harus memastikan adanya prosedur yang mengatur operasi dan pemeliharaan infrastruktur;

2.3.1.5. Unit Pengelola TI bertanggung jawab atas pelaksanaan operasi dan pemeliharaan infrastruktur Teknologi Informasi;

2.3.1.6. Secara periodik Pengelola Infrastruktur bertanggung jawab untuk melakukan evaluasi performansi infrastruktur terhadap target, melakukan *root cause analysis* dan melakukan inisiasi tindakan perbaikan terhadap kasus yang terjadi;

2.3.1.7. Sistem kritikal memiliki log yang merekam aktivitas pengguna atau sistem tersebut. Beberapa ketentuan log sebagai berikut.

a. Hal-hal yang tidak diizinkan pada *log*.
   1) Perubahan data yang direkam;
   2) File log dilakukan proses editing atau dihapus; dan
   3) Kapasitas penyimpanan dari media log file telah terlewati, yang berakibat pada kegagalan dalam merekam kejadian atau menimpa rekaman kejadian sebelumnya;

b. *Log* Administrator dan Operator
   Log aktivitas administrator sistem dan operator dikelola meliputi:
   1) Waktu kejadian (sukses atau gagal) terjadi;
   2) Informasi tentang kejadian atau kegagalan;
   3) Akun dan administrator atau operator yang terlibat; dan

2.3.1.8. Waktu pada sistem harus dilakukan sinkronisasi. Ketentuan sinkronisasi waktu sebagai berikut.

a. *Clock* semua sistem informasi didalam PT Wijaya Karya Beton Tbk. disinkronisasi dengan standar yang telah disepakati untuk memastikan akurasi dari log audit;
b. Format tanggal yang digunakan oleh PT Wijaya Karya Beton Tbk. adalah dd/mm/yyyy;
c. Format waktu yang digunakan oleh PT Wijaya Karya Beton Tbk. adalah hh:mm, yang memberlakukan sistem 24 jam; dan
d. Clock pada semua server dan perangkat pemrosesan informasi PT Wijaya Karya Beton Tbk. diperiksa secara reguler dan dikoreksi jika dibutuhkan.

2.3.2. Pengelolaan Fasilitas *Desktop* dan *Removable Media*

2.3.2.1. Pengelolaan fasilitas desktop mengikuti ketentuan berikut:

a. Unit Pengelola TI memberikan masukan terkait standarisasi perangkat lunak dan perangkat keras untuk kemudian ditetapkan Direktur Perusahaan menjadi Keputusan Direksi mengenai Hak Standar Fasilitas Desktop;

b. Pengadaan Desktop oleh *Unit Supply* mengacu kepada standarisaisi spesifikasi perangkat keras dan perangkat lunak yang telah ditetapkan dalam Keputusan Direksi;

c. Seluruh fasilitas desktop adalah milik perusahaan dan hanya diberikan kepada karyawan yang berhak menerima sesuai dengan jabatan, tanggung jawab dan keperluan untuk mendukung pekerjaan karyawan yang bersangkutan;
d. Kebutuhan yang tidak mengikuti standarisasi yang diberlakukan oleh Unit Pengelola TI dapat diberikan kepada karyawan dengan syarat mengajukan perubahan, penambahan atau pengecualian standarisasi yang telah disetujui oleh Pimpinan Unit Kerja bersangkutan;
e. Karyawan tidak diperkenankan menambah atau mengurangi perangkat keras/lunak yang telah disediakan perusahaan kecuali telah mendapatkan persetujuan Unit Pengelola TI. Unit Pengelola TI dapat menghapus perangkat lunak di PC atau laptop karyawan yang tidak terdapat dalam daftar perangkat lunak yang diijinkan;
f. Penggunaan perangkat keras/lunak di luar standarisasi yang telah ditetapkan perusahaan akan menjadi tanggung jawab karyawan sepenuhnya;
g. Pelatihan bagi karyawan baru untuk penggunaan PC dan Laptop, cara akses ke jaringan dan perangkat lunak/aplikasi lainnya akan diberikan oleh Unit Pengelola TI;
h. Setiap karyawan yang memiliki hak akses ke *working folder server* untuk menyimpan data. Setiap periode tertentu data yang ada di server akan dilakukan prosedur backup. Data dan aplikasi yang ada di PC/Laptop tidak di lakukan backup.
i. Perusahaan menggunakan *software server antivirus* yang akan melakukan *scanning* secara otomatis terhadap seluruh PC/Laptop yang terhubung di jaringan perusahaan.

2.3.2.2. Pemberian dukungan atas fasilitas desktop mengikuti ketentuan berikut:

a. Dukungan teknis terhadap perangkat lunak hanya disediakan pada jenis perangkat lunak yang masuk dalam standarisasi perusahaan;
b. Unit Pengelola TI akan melakukan pemeliharaan terhadap semua desktop perusahaan dimana dimungkinkan melalui metode *managed service*;

c. Pemeliharaan *peripheral* yang digunakan oleh suatu unit kerja merupakan tanggung jawab pimpinan unit atau *senior leader* unit tersebut;
d. Unit Pengelola TI bertanggung jawab terhadap semua instalasi perangkat keras desktop/laptop dan karyawan dilarang memodifikasi, memutuskan, menyambung atau memindahkan perangkat keras tanpa sepengetahuan Unit Pengelola TI;
e. Setiap karyawan diwajibkan memelihara dan menjaga dengan baik setiap perangkat keras dan perangkat lunak yang telah dipercayakan oleh perusahaan kepada karyawan untuk menunjang aktifitas kerjanya di perusahaan;
f. Jika mengalami masalah dengan Desktop, pengguna diwajibkan untuk menghubungi tim Helpdesk di Unit Pengelola TI dan kemudian tim *Helpdesk* akan mengarahkan ke bagian Desktop support perusahaan. Pengguna tidak di perkenankan menentukan sendiri penyedia jasa perbaikan/servis Desktop tanpa melalui persetujuan dari Unit Pengelola TI;
g. Karyawan atau Unit Kerja yang membutuhkan penggantian perangkat keras harus menyampaikan permintaan formal kepada Unit Pengelola TI, disertai dengan dokumen Berita Acara serah terima asset yang telah ditandatangani oleh karyawan tersebut, atasan langsung dan Unit Pengelola Aset (sebagai pemeriksa asset);
h. Perangkat pribadi yang dipergunakan untuk kepentingan perusahaan tidak akan mendapatkan support dari Unit Pengelola TI kecuali sebelumnya didaftarkan terlebih dahulu melalui permintaan dan persetujuan unitnya.

2.3.2.3. Pengamanan *removable media* sebagai berikut.

a. *Removable media* yang boleh digunakan hanya tipe *removable disk* yang telah ditentukan oleh perusahaan;
b. Perusahaan mencatat informasi mengenai *removable media* sebagai *Configuration Item* (CI) dalam CMDB;
c. *Removable media* yang digunakan dilengkapi dengan *password* yang diwajibkan sesuai dengan peraturan pengunaan *password*;
d. Pendistribusian dan pelabelan informasi pada *removable media* mengikuti klasifikasi informasi masing-masing.

2.3.2.4. Clear Desk & Clear Screen

a. Menyimpan dokumen *hardcopy* yang berisi informasi sensitif pada tempat yang terkunci pada saat tidak digunakan;
b. Tidak meninggalkan layar komputer dalam keadaan terbuka. Bila meninggalkan komputer, pengguna harus *log off* atau mengaktifkan *screen saver* berbatas waktu yang dilengkapi dengan autentikasi *password*;
c. Memindahkan dokumen yang mengandung informasi sensitif dengan segera dari mesin *printer*, *fax* dan *photocopy*.

2.3.3. Pengelolaan Data

2.3.3.1. Semua data dalam jaringan baik di server maupun client yang terkait dengan kegiatan perusahaan adalah milik perusahaan;

2.3.3.2. Unit Pengelola TI bertanggung jawab melakukan pengelolaan data sesuai prosedur yang ditetapkan dan mencakup:

a. pemrosesan data untuk menghasilkan output yang diperlukan oleh bisnis;
b. pengelolaan *storage*, media library, *backup*, *recovery* dan disposal untuk menjamin efektivitas pengelolaan data yang digunakan oleh seluruh aplikasi;
c. pengamanan data;
d. pengujian kualitas hasil *backup* dan proses *recovery* secara periodik.

2.3.3.3. Unit Kerja Pemilik data berkewajiban untuk memastikan tersedianya sumber data yang diperlukan oleh aplikasi dari aktivitas bisnis dan menentukan periode penyimpanan *(retention period)* yang mengacu pada kebutuhan bisnis dan/atau sesuai dengan aturan Perusahaan.

2.3.4. Hal-hal yang tidak diperkenankan:

2.3.4.1. Menggunakan *file sharing* pada sistem jaringan Perusahaan yang berkapasitas besar (≥ 500 *mb*) kecuali atas izin Manajer DSI.

2.3.4.2. Menggunakan sistem jaringan komputer Perusahaan untuk penggunaan Perangkat *hardware* pribadi (menghubungkan perangkat milik pribadi ke jaringan perusahaan) kecuali ada izin dari Manajer DSI seperti: Komputer; *Notebook*; Printer; *Modem Internet* (*3G, GPRS, Wireless*).

2.3.4.3. Memperbaiki gangguan atau kerusakan pada sarana dan fasilitas *hardware* sistem Informasi perusahaan kecuali oleh penanggung jawab Sistem Informasi yang ditunjuk di masing-masing unit kerja.

2.3.4.4. Memanfaatkan peralatan dan *hardware* sistem informasi Perusahaan untuk kepentingan pribadi yang bersifat komersial.

2.3.4.5. Melakukan Sabotase pada peralatan *hardware* Sistem Informasi Perusahaan.

2.3.5. Hal-hal yang diwajibkan:

2.3.5.1. Melaporkan atau menginformasikan segala kelemahan atau kerusakan dari *hardware* dan jaringan komunikasi sistem informasi Perusahaan kepada jajaran DSI.

2.3.5.2. Menggunakan *flash drive* sebagai media penyimpanan / data storage cadangan yang penggunaannya hanya untuk kepentingan pekerjaan.

2.3.5.3. Setiap perangkat kerja (inventaris laptop dan komputer) wajib diinstalkan antivirus perusahaan, kecuali perangkat Mac OS.

2.4. Fasilitas Internet Sistem Informasi Perusahaan.

2.4.1. Penggunaan akses internet dikelola sebagai berikut:

2.4.1.1. Hak akses penggunaan internet di lingkungan perusahaan merupakan fasilitas kerja yang diberikan kepada karyawan secara otomatis sedangkan untuk tamu perusahaan tidak diberikan secara otomatis tetapi berdasarkan permintaan dan rekomendasi unit yang bersangkutan.

2.4.1.2. Setiap karyawan bertanggung jawab terhadap hak akses yang telah diberikan dan pemanfaatannya.

2.4.1.3. Penggunaan internet hanya digunakan untuk kepentingan perusahaan.

2.4.1.4. Perusahaan melakukan kontrol akses terhadap beberapa sumber daya dan situs-situs internet *(website)*. Konten yang diakses oleh karyawan menjadi tanggung jawab karyawan bersangkutan sesuai aturan perusahaan dan hukum yang berlaku di Indonesia.

2.4.1.5. Setiap perangkat lunak atau *file* yang diunduh melalui internet ke jaringan perusahaan menjadi milik perusahaan. *File* tersebut atau perangkat lunak hanya dapat digunakan dengan cara-cara yang sesuai dengan ketentuan perusahaan lisensi dan hak cipta.

2.4.1.6. Perusahaan dapat melakukan *blocking* atas *website* atau sumberdaya yang akan berpotensi merugikan perusahaan.

2.4.1.7. Unit Pengelola TI dapat memberikan akses kepada pihak eksternal dengan mempertimbangkan aspek pengamanan informasi dan bersifat temporer.

2.4.1.8. Menjaga nama baik perusahaan melalui penggunaan fasilitas internet Perusahaan.

2.4.1.9. Memanfaatkan akses internet guna menunjang pekerjaan dan kebutuhan Perusahaan.

2.4.1.10. Bila terjadi kendala internet perusahaan, pegawai dapat menggunakan jaringan internet pribadi *(tethering)* dari perangkat masing-masing

2.4.1.11. Akun akses akan secara otomatis berubah sesuai dengan pengelompokan peran pada aplikasi di WIKA Beton berdasarkan data yang diperoleh dari data kepegawaian *(Human Capital).*

2.4.2. Hal-hal yang tidak diperkenankan:

2.4.2.1. Membawa data / informasi internal Perusahaan, ke luar Perusahaan kecuali untuk kepentingan Perusahaan.

2.4.2.2. Memasukkan *file* atau data / *download file* (*video*, gambar, tulisan, musik dll) yang tidak berhubungan dengan kepentingan pekerjaan kedalam perangkat sistem informasi perusahaan.

2.4.2.3. Mengakses, mengunggah, mengunduh, atau mendistribusikan pornografi, materi yang bermuatan seksual, ilegal, propaganda, politis, fitnah, pelecehan seksual, penghinaan, pencemaran nama baik, diskriminasi gender dan berbau SARA, serta berjudi.

2.4.2.4. Menggunakan fasilitas *file sharing* / *file storage* melalui media internet, demi keamanan data perusahaan.

2.4.2.5. Membuat dan memiliki *website* sendiri yang mengatasnamakan perusahaan, tanpa ijin dari Manajer DSI.

2.4.2.6. Melanggar peraturan atau undang-undang yang berlaku di indonesia;

2.4.2.7. Melakukan vandalisme atau pengrusakan properti individu lain atau organisasi lain.

2.4.2.8. Menyerang atau penyalahgunaan privasi orang lain.

2.4.2.9. Melanggar hak cipta atau penggunaan materi tanpa izin intelektual;

2.4.2.10. Menggunakan jaringan untuk keuntungan finansial atau komersial pribadi.

2.4.2.11. Mengganggu performa jaringan *(internet bandwidth abuse)*.

2.4.2.12. Mendownload atau mendistribusikan *software* ilegal;

2.4.2.13. Dengan sengaja menyebarkan *virus*, *worm, trojan horse* atau *tools* yang dilarang *(trap-door tools code)*. Jika ada kesengajaan maka akan mendapatkan sanksi sesuai peraturan perusahaan.

2.4.2.14. Bermain *Game online* pada waktu jam kerja.

2.5. Kebijakan dan Etika Tata Perilaku Personil DSI.

Setiap personil DSI bertanggung jawab dan bersikap profesional terhadap Pengelolaan Sistem Informasi Perusahaan.

2.5.1. Pengelolaan Akun Akses

2.5.1.1. Perusahaan memberikan data akun akses yang terdiri dari username dan password kepada karyawan yang berhak untuk mengakses sistem informasi perusahaan.

2.5.1.2. Setiap karyawan yang memperoleh password wajib menjaga kerahasian dan keamanan password;

2.5.1.3. Setiap pengajuan pembuatan akun akses untuk Sistem Informasi harus mendapatkan persetujuan dari atasan langsung minimal setingkat manager atau dari unit Human Resource. Unit Pengelola TI akan memberikan default password yang harus segera diganti oleh karyawan yang menerimanya saat pertama kali mempergunakan default password tersebut.

2.5.1.4. PT Wijaya Karya Beton mengendalikan pemberian password awal kepada pengguna dengan ketentuan sebagai berikut.

a. Password awal harus diganti saat login pertama kali;
b. Password awal diberikan secara aman;
c. Password awal yang diberikan kepada pengguna bersifat unik dan tidak mudah ditebak;
d. Password standar (default password) yang dimiliki oleh sistem operasi, sistem aplikasi, database management system dan perangkat jaringan harus diganti sebelum diimplementasikan;
e. PT Wijaya Karya Beton mewajibkan pengguna untuk:
    1) Menjaga kerahasiaan password;
    2) Menghindari penulisan password di kertas dan di tempat lain tanpa pengamanan yang memadai.
    3) Memilih *password* yang berkualitas:
        - Panjang Minimum : 8;
        - Panjang Maximum : 16;
        - Tidak bisa sama dengan sebelumnya (3 *password*);
        - Karakter yang diisi sekurang – kurangnya satu huruf kapital, setidaknya satu simbol dan satu nomor;
    4) Perubahan dilakukan setidaknya 90 hari sekali;
    5) Kriptografi minimal menggunakan *md5 + SALT* untuk pengembangan aplikasi internal maupun dengan vendor.
    6) *Password* dapat menggunakan *OTP (One Time-Password)*

2.5.1.5. Pengelolaan Priviledge Access

a. *Priviledge Access* hanya diberikan kepada personil yang bewenang sesuai dengan tugas pokok dan fungsi masing-masing;
b. *Priviledge Access* hanya diberikan oleh Manager Sistem Informasi dalam jangka waktu yang ditentukan;
c. *Priviledge Access* dilakukan logging, monitoring dan review berkala.

2.5.1.6. Unit Pengelola TI akan menghapus/menonaktifkan akun akses karyawan yang mengundurkan diri atau tidak tercatat lagi sebagai karyawan seperti pensiun, atas permintaan dan pemberitahuan dari unit Unit Pengelola SDM.

2.5.2. Mobile Computing & Teleworking

2.5.2.1. Pengelolaan mobile computing sebagai berikut.

a. Perangkat yang terkategori sebagai perangkat mobile terdiri namun tidak terbatas dari laptop, tablet, smartphone, PDA;
b. Perangkat mobile yang digunakan untuk menjalankan aktivitas bisnis adalah perangkat milik perusahaan dan perangkat milik pegawai yang telah teregistrasi;
c. Pengguna perangkat memastikan perangkatnya hanya digunakan oleh dirinya sendiri, dan tidak digunakan oleh orang lain yang tidak berhak;
d. Pengguna perangkat memastikan perangkat mobile yang berada pada lokasi yang aman;
e. Pengguna perangkat memastikan fitur keamanan seperti screen lock, password, dan sebagainya, dalam keadaan aktif;
f. Pengguna perangkat memastikan antivirus terpasang dan terupdate pada perangkatnya;
g. Pengguna bertanggung jawab atas segala informasi yang ada pada perangkat mobile yang dimilikinya;
h. Apabila terjadi kerusakan atau kehilangan pada perangkat mobile, pengguna melaporkannya pada *IT Service desk*;
i. Pengguna dapat sewaktu-waktu diminta untuk menyerahkan perangkat *mobile*-nya kepada perusahaan untuk keperluan pemeriksaan atau audit.

2.5.2.2. Pengelolaan *teleworking* sebagai berikut.

a. Pedoman *Teleworking* adalah pedoman untuk mengatur personel perusahaan yang bekerja di tempat lain diluar lokasi perusahaan, misalnya bekerja dari rumah;
b. Perusahaan melakukan penilaian risiko sebelum teleworking diterapkan, meliputi karakteristik pekerjaan yang akan dikerjakan secara teleworking, keamanan fisik, dan lain sebagainya;
c. Fasilitas yang digunakan untuk teleworking, meliputi jaringan komunikasi, mekanisme backup, serta dukungan teknis lainnya, diatur sesuai dengan ketentuan yang berlaku di perusahaan. Sementara itu, perangkat yang digunakan untuk teleworking menggunakan perangkat milik organisasi dan milik pegawai yang telah teregistrasi; dan
d. Apabila perjanjian *teleworking* telah selesai, seluruh akses *teleworking* diberhentikan.

2.5.3. Kriptografi

2.5.3.1. Kriptografi minimal menggunakan *md5 + SALT* untuk pengembangan aplikasi internal maupun dengan vendor.

2.5.3.2. Kriptografi di *network* minimal menggunakan 2 enkripsi *3DES SHA1 dan AES128 SHA1*

2.5.3.3. *Key Management* Kripto adalah Manajer Divisi Sistem Informasi.

2.5.4. Backup Data

2.5.4.1. *Backup Data* dilakukan sesuai dengan persyaratan *RPO* layanan

2.5.4.2. Mekanisme *Backup Data* yang diimplementasikan adalah *backup Disk-to-Disk*, yang dapat menggunakan solusi terotomatisasi pada *level database* atau *storage*.

2.5.4.3. Mempertimbangkan tingkat kritikalitas layanan, berikut ini adalah kriteria *backup* yang dilakukan:

- *Backup Data* terkait layanan yang bersifat *HOT* minimal adalah tiap 1 jam
- *Backup Data* terkait layanan yang bersifat *WARM* minimal adalah tiap 6 jam
- *Backup Data* terkait layanan yang bersifat *COLD* minimal adalah tiap 24 jam

2.5.4.4. Minimal setiap bulan sekali dilakukan evaluasi bahwa data hasil *backup* memungkinkan untuk di-*recovery* jika dibutuhkan.

2.5.4.5. Backup dapat menggunakan beberapa media, seperti: Media disk, *VM*, aplikasi, *External Storage*, dll

2.5.5. Hal-hal yang tidak diperkenankan:

2.5.5.1. Memberikan, memperjual belikan informasi, data atau aplikasi milik perusahaan kepada pihak siapapun tanpa seijin Direksi.

2.5.5.2. Membocorkan, merubah, menghapus data operasional perusahaan tanpa seijin Manajer DSI dan atau pejabat yang diberi wewenang.

2.5.6. Hal-hal yang diwajibkan:

2.5.6.1. Mengamankan dan merawat seluruh aset IT berupa *hardware*, jaringan, *software* beserta data milik Perusahaan terhadap ancaman baik dari pihak dalam maupun luar perusahaan.

2.5.6.2. Menjamin keberlangsungan operasional perusahaan yang terkait dengan penggunaan sarana IT.

2.5.6.3. Memastikan terhadap jalannya backup data operasi perusahaan dengan aman dan benar, serta melakukan uji *disaster recovery* minimal enam bulan sekali.

2.5.6.4. Menjaga kerahasiaan terhadap *password* yang dimiliki oleh masing masing personil DSI sesuai dengan tingkat tugas dan tanggung jawabnya.

2.5.6.5. Dalam keadaan *emergency* atau *trouble shooting* personil DSI wajib lebih mengutamakan kepentingan perusahaan dari pada kepentingan pribadi, dan siap dihubungi dalam waktu 24 jam.

2.5.6.6. Melakukan kontrol secara kontinyu terhadap:

Patching software, *firmware device* pada *server*.

- *Free space memory* dan *storage*.
- Lisensi, update lisensi, update versi untuk *software* dan antivirus.
- Daftar *User* aktif.

2.5.6.7. Melakukan pembatasan akses kepada *user* tanpa pemberitahuan terlebih dahulu jika terdapat penyalahgunaan hak akses yang diberikan kepada *user*.

2.5.7. Pihak Ketiga

2.5.7.1. Manajemen Pihak Ketiga

a. Proses pemilihan Pihak Ketiga merujuk kepada prosedur pengadaan yang sudah ada sebelumnya di WIKA Beton.
b. Dalam konteks manajemen layanan, Pihak Ketiga akan menyediakan layanan kepada WIKA Beton. Karena itu, layanan oleh Pihak Ketiga harus mengikuti ketentuan Manajemen Tingkat Layanan, yang dituangkan dalam persyaratan *SLA*.
c. Khusus untuk layanan Pihak Ketiga yang bersifat kritikal terhadap operasional TI dan pembayaran jasanya dilakukan secara reguler, maka dipersyaratkan keberadaan restitusi. Restitusi adalah pembayaran kembali atas durasi layanan yang tidak sesuai dengan target *SLA* yang telah disepakati di kontrak.
d. Manajer DSI dapat mengusulkan keikutsertaan klausul restitusi pada kontrak dengan pihak ketiga, sebagai input kepada unit kerja yang bertanggungjawab dalam pengelolaan kontrak dengan Pihak Ketiga.
e. *SLA* layanan Pihak Ketiga selalu dimonitoring dan dievaluasi reguler ketercapaiannya. Jika tidak mencapai target *SLA*, maka Pihak Ketiga harus memperbaiki layanannya, sekaligus membayarkan restitusi (jika ada dalam klausul kontrak).
f. Pihak ketiga harus menandatangani *NDA* saat melakukan kontrak dengan WIKA Beton

2.5.7.2. Minimal setiap dua tahun sekali dilakukan *VA-Pentest* oleh Pihak Ketiga yang independen.

2.5.7.3. *VA-Pentest* oleh Pihak Ketiga independen harus disupervisi oleh fungsi terkait di DSI

2.5.7.4. Pengelolaan akun akses Pihak Ketiga

a. Permintaan hak akses untuk Pihak Ketiga hanya dapat dilakukan oleh Manajer Divisi yang relevan.
b. Hak akses untuk Pihak Ketiga dibatasi hanya untuk kegiatan yang relevan dengan lingkup pekerjaan dalam kontrak.
c. Penggunaan hak akses oleh Pihak Ketiga diawasi dan dicatat secara otomatis oleh sistem.
d. Jika terdapat pelanggaran Hak Akses, Akun Pihak Ketiga akan dinonaktifkan dan dilakukan eskalasi kepada Divisi terkait. Tahapan selanjutnya akan merujuk kepada aturan hubungan dengan pihak ketiga yang ada di perusahaan.
e. Hak Akses Pihak Ketiga akan otomatis berakhir sesuai dengan tanggal perikatan dalam kontrak.

2.5.7.5. Pemberian Hak Akses Fisikal kepada Pihak Ketiga

a. Persetujuan hanya dapat diberikan oleh Manajer DSI, dengan rekomendasi dari fungsi terkait, setelah sebelumnya melengkapi data personil yang akan masuk ke fasilitas *Data Center/Disaster Recovery Center.*
b. Kunjungan Pihak Ketiga ke lokasi *Data Center/Disaster Recovery Center* harus disupervisi langsung oleh minimal satu staf internal perusahaan.
c. Jika aplikasi dikembangkan oleh pihak ketiga, kontrak pekerjaan dengan pihak ketiga harus memuat lingkup pemeliharaan aplikasi minimal setahun setelah serah terima *software* aplikasi.
d. Jika infrastruktur disediakan oleh pihak ketiga, kontrak pekerjaan dengan pihak ketiga harus memuat lingkup pemeliharaan minimal setahun setelah serah terima infrastruktur.

2.5.8. Prosedur penghapusan akses

2.5.8.1. Unit Pengelola TI akan menghapus/menonaktifkan akun akses karyawan yang mengundurkan diri atau tidak tercatat lagi sebagai karyawan seperti pensiun, atas permintaan dan pemberitahuan dari unit Unit Pengelola SDM.

2.5.9. Prosedur operasional

2.5.9.1. Seluruh prosedur operasional terlampir dan didistribusikan melalui Aplikasi *Knowledge Management*

2.5.10. Manajemen Perubahan TI

2.5.10.1. DSI bertanggung jawab untuk memastikan bahwa setiap perubahan terhadap layanan TI sudah melalui proses *assessment*, persetujuan, pengujian, implementasi dan *review* yang terkontrol.

2.5.10.2. DSI harus mendefinisikan kriteria klasifikasi perubahan mulai dari minor sampai dengan mayor, ruang lingkup perubahan serta mekanisme perubahan darurat.

2.5.10.3. Setiap perubahan harus melalui mekanisme persetujuan dan pengujian sesuai prosedur yang berlaku serta dikomunikasikan kepada pelanggan layanan terkait ataupun pihak-pihak yang terkena dampak.

2.5.10.4. DSI perlu menganalisis data perubahan sebagai referensi *Continual Improvement* serta harus melaporkan setiap perubahan yang terjadi pada layanan TI yang berlaku dalam rangka evaluasi pencapaian Tingkat Layanan *(Service Level).*

2.5.10.5. Terdapat tiga tipe perubahan yang memiliki proses berbeda *(versioning):*

a. *Standard Change* yaitu perubahan yang bersifat *pre-authorized* karena memiliki risiko kecil.
   - Pengambilan keputusan atas *standard change* dilakukan langsung oleh fungsi terkait di DSI. Hasil perubahan diinformasikan kepada Manajer DSI
   - Perbaikan *bug* tanpa membuat versi lama tidak bisa digunakan.
   - v1.1.1, v1.1.2, v1.1.3, dst.

b. *Emergency Change* yaitu perubahan yang harus dilakukan secepat mungkin karena terkait dengan keberlangsungan layanan. Misalnya adalah langkah resolusi atas insiden bersifat *major* atau *patch* keamanan.
   - Pengambilan keputusan tentang *emergency change* dilakukan oleh Manajer DSI menggunakan media komunikasi yang paling cepat dan mudah saat insiden terjadi.

- Berdasarkan keputusan oleh Manajer DSI, fungsi terkait langsung melakukan perubahan.
- Dokumentasi atas perubahan dilakukan setelah perubahan telah berhasil dilakukan.

c. *Normal Change* yaitu perubahan yang bukan bersifat standar dan mendesak dan memiliki risiko medium-besar.
   - Pengambilan keputusan atas *standard change* dilakukan langsung oleh fungsi terkait di DSI.
   - Hasil perubahan diinformasikan kepada Manajer DSI
   - Terdapat dua tipe *Normal Change* yaitu *Major Change* dan *Non-Major Change*

d. *Major Change* yaitu perubahan yang memiliki risiko besar dan harus mengikuti mekanisme pengembangan atau akusisi *software* aplikasi atau implementasi infrastruktur baru.
   - Pengambilan keputusan dilakukan secara bersama oleh DSI dengan Divisi terkait atau level manajemen yang lebih tinggi pada pertemuan *ITSC*, merujuk lingkup perubahan yang akan dilakukan.
   - Hasil perubahan diinformasikan kepada Manajer DSI dan Manajer Divisi terkait.
   - V1.x.x; v2.x.x; v3.x.x dst.

e. *Non-Major Change* yaitu perubahan yang memiliki risiko medium dan tidak diperlukan mengikuti prosedur pengembangan atau akuisisi *software* aplikasi.
   - Lingkup *Normal Change (Non-Major Change)* di antaranya tetapi tidak terbatas pada:
     - *Patching* sistem operasi
     - *Patching firmware* pada infrastruktur
     - Perubahan pada *software* aplikasi yang terbatas pada sebagian fitur di modul-modul aplikasi
     - Perubahan konfigurasi *CMDB*
     - Perubahan Katalog Layanan
   - Pengambilan keputusan oleh Manajer DSI.
   - Hasil perubahan diinformasikan kepada Manajer DSI.
   - V1.2.x; v1.3.x; v1.4.x dst.

2.5.11. Rekaman

2.5.11.1. Rekaman/Bukti Kerja dibuat oleh masing-masing fungsi, sesuai dengan tugas masing-masing

2.5.11.2. Identifikasi Rekaman

a. Petugas Pengendalian Rekaman di masing – masing fungsi bertanggung jawab dalam hal identifikasi rekaman yang dilaksanakan dalam kurun waktu maksimal 1 minggu.

b. Petugas Pengendalian Rekaman di masing – masing fungsi perlu memperhatikan ketentuan-ketentuan identifikasi rekaman. Adapun ketentuan identifikasi rekaman adalah sebagai berikut:

i. Jenis rekaman dalam Sistem Manajemen Keamanan Informasi bermacam-macam sesuai dengan proses yang terkait dengannya, misalnya:

1. Insiden keamanan
2. Perubahan
3. Item konfigurasi
4. *Log* kejadian keamanan

ii. Untuk rekaman yang bersifat lintas proses, misalnya: risalah rapat. Untuk memudahkan identifikasi, *tool* yang dipergunakan dalam suatu proses dapat menerbitkan penomoran yang bersifat unik, sebagai contoh: INC000001 untuk insiden keamanan; CHG000001 untuk perubahan.

iii. Sedangkan untuk rekaman yang dibuat secara manual, aturan yang diberlakukan adalah:

1. Rekaman yang berupa Risalah Rapat diberi nama sesuai dengan agenda dan tanggal pelaksanaan rapat.
2. Rekaman yang berupa Laporan diberi nama sesuai dengan jenis laporan dan periode pelaporannya.
3. Rekaman yang berupa *Log* diberi nama sesuai dengan judul log dan tanggal/waktu periode *log* tersebut.

iv. Apabila ada jenis-jenis rekaman yang lain, penamaannya dilakukan sedemikian hingga nama yang diberikan memudahkan proses identifikasi rekaman tersebut.

2.5.11.3. Penyimpanan Rekaman

a. Petugas Pengendalian Rekaman di masing–masing fungsi perlu memperhatikan ketentuan ketentuan penyimpanan rekaman. Adapun ketentuan penyimpanan rekaman adalah sebagai berikut:

1. Seluruh rekaman disimpan di lokasi yang sesuai dengan jenis dan tujuan pembuatan rekaman. Sebagian rekaman dalam Sistem Manajemen Keamanan Informasi disimpan dalam *database* yang dibuat khusus, misalnya: database insiden keamanan.
2. Rekaman yang tidak berupa database disimpan sesuai dengan area yang relevan dalam Sistem Manajemen Keamanan Informasi.
3. Jika memungkinkan, seluruh rekaman disimpan dalam format elektronik. Rekaman dalam bentuk kertas sebaiknya dipindai dan disimpan di lokasi yang sesuai.
4. Petugas Pengendalian Rekaman di masing – masing fungsi bertanggung jawab dalam menentukan periode penyimpanan rekaman dalam Sistem Manajemen Keamanan Informasi sesuai dengan penilaian tingkat manfaat.
5. Petugas Pengendalian Rekaman di masing – masing fungsi bertanggung jawab dalam hal penyimpanan rekaman yang dilakukan dalam kurun waktu sesuai masa simpan.

2.5.11.4. Perlindungan Rekaman

a. Petugas Pengendalian Rekaman di masing – masing fungsi perlu memperhatikan ketentuan – ketentuan perlindungan rekaman. Adapun ketentuan perlindungan rekaman adalah sebagai berikut:
   1. Rekaman yang disimpan dalam *database* aplikasi harus di-*backup* sesuai dengan Prosedur Keberlanjutan Layanan TI. Lokasi penyimpanan *file* juga di-*backup* secara reguler. Keseluruhan backup yang terakhir dilakukan disimpan di lokasi *offsite*.
   2. Akses terhadap rekaman dibatasi hanya untuk individu yang memiliki hak akses dan dilakukan dengan mengikuti Kebijakan Keamanan Informasi organisasi.

2.5.11.5. Pengambilan Rekaman

a. Petugas Pengendalian Rekaman di masing – masing fungsi perlu memperhatikan ketentuan ketentuan pengambilan rekaman. Adapun ketentuan pengambilan rekaman adalah sebagai berikut:
   1. Rekaman dalam bentuk *file* elektronik diambil menggunakan aplikasi yang digunakan untuk membuatnya, misalnya: sistem *helpdesk* untuk insiden, permasalahan, dll.
   2. *Tool* pelaporan sebaiknya digunakan untuk memproses dan mengonsolidasikan data-data dalam rekaman menjadi informasi yang bermanfaat.

2.5.11.6. Pemusnahan Rekaman

a. Petugas Pengendalian Rekaman di masing – masing fungsi bertanggung jawab dalam hal pemusnahan Rekaman yang dilakukan dalam kurun waktu maksimal 1 minggu. Pemusnahan rekaman berdasarkan persetujuan unit kerja yang terkait atau telah melewati masa simpan.
b. Petugas Pengendalian Rekaman di masing – masing fungsi perlu memperhatikan ketentuan ketentuan pemusnahan rekaman. Adapun ketentuan pemusnahan rekaman adalah sebagai berikut:
   1. Apabila rekaman diputuskan untuk dihapus, maka rekaman tersebut harus dihapus dengan mengikuti prosedur disposal yang berlaku di organisasi.
   2. Rekaman dalam format elektronik (misalnya: *database*) dihapus dengan menggunakan *software* yang sesuai misalnya *helpdesk* biasanya memiliki fungsi dan fitur untuk menghapus rekaman insiden.
   3. Jika rekaman tersebut disimpan pada perangkat yang juga akan dibuang, maka perangkat tersebut harus dihancurkan oleh vendor yang ditetapkan.
   4. Rekaman berbentuk kertas yang akan dibuang harus dihancurkan sesuai dengan kebijakan keamanan informasi Pusdatin.

2.5.12. Penggunaan *Email* dan Nota Dinas

2.5.12.1. Penggunaan fasilitas *email* dan nota dinas diatur sebagai berikut:

a. Perusahaan menyediakan sarana sistem elektronik berupa *email* dan notadinas yang terdapat pada aplikasi portal kepada seluruh karyawan untuk mendukung efektifitas kerja karyawan dan tentunya akan meningkatkan produktivitas perusahaan;
b. *Email* dan Nota Dinas sepenuhnya milik perusahaan. Seluruh sarana yang digunakan termasuk semua pesan dan nota yang disimpan, dibuat, dikirimkan atau yang diterima oleh karyawan atau non karyawan adalah milik perusahaan dan BUKAN milik pribadi karyawan;
c. Perusahaan berhak untuk melakukan *blocking*, *monitor*, mengkaji dan mengungkapkan setiap/semua pesan yang dikirimkan atau diterima. Jika diperlukan dan sesuai persetujuan atasan atau pihak yang berwenang (jajaran *BOD* atau *Head of Internal Auditor*) audit pesan elektronik dapat dilakukan.

d. Pertukaran data internal dan eksternal terkait keperluan dinas harus menggunakan fasilitas *email* atau nota dinas perusahaan *(exchange agreement)*.
e. Setiap karyawan yang berhak akan mendapatkan alamat *Email* yang akan digunakan untuk pengiriman dan penerimaan *Email* hanya untuk kepentingan perusahaan.
f. Penggunaan *tools Email client* akan ditentukan oleh Unit Pengelola TI melalui daftar *software* atau perangkat lunak.
g. Jika ada pengakhiran hubungan kerja antara karyawan dan perusahaan maka perusahaan akan menutup *email* dan nota dinas karyawan dan penutupan akses terhadap seluruh sarana pada aplikasi portal perusahaan. Termasuk hak akses, hak melakukan download, mencetak, mengambil pesan yang tersimpan dalam sistem terhitung sejak tanggal terminasi hubungan kerja ditetapkan;
h. Perusahaan menyediakan *software antivirus* sebagai sarana pemeriksaan terhadap sarana pesan elektronik (*email*) dan nota dinas. Karyawan dilarang menonaktifkan *software* antivirus tersebut.

2.5.12.2. Fasilitas *email* dan nota dinas dilarang untuk kegiatan berikut:

a. Diskriminasi terhadap usia, ras, gender, orientasi seksual, agama atau politik dalam penggunaan sarana pesan elektronik *(email)* dan nota dinas.
b. Penggunaan pesan elektronik *(email)* dan nota dinas untuk kegiatan politik, kegiatan illegal/kriminal, mengandung isi pornografi, pesan/lampiran illegal, hal tidak senonoh, memfitnah atau menghina.
c. Promosi atau publikasi seseorang, pandangan yang bersifat ajakan ke golongan/politik tertentu atau paham agama yang menyesatkan, pengoperasian bisnis atau apapun kegiatan untuk kepentingan pribadi.
d. Kepesertaan dalam *mailing list public* atau kegiatan *social networking*.
e. Mengirim pesan elektronik *(email)* dan nota dinas yang tidak sah, mengungkapkan rahasia perusahaan atau informasi perusahaan yang bersifat rahasia.
f. Penyalinan dan distribusi terhadap materi yang dilindungi sebagai hak cipta perusahaan kecuali untuk tujuan program perusahaan.

2.6. Kebijakan dan Etika Tata Perilaku Insan WIKA Beton.

2.6.1. Kebijakan *Mobile Device Policy*

2.6.1.1. Perangkat yang terkategori sebagai perangkat *mobile* terdiri namun tidak terbatas dari *laptop, tablet, smartphone, PDA*.

2.6.1.2. Perangkat *mobile* yang digunakan untuk menjalankan aktivitas bisnis adalah perangkat milik perusahaan dan perangkat milik pegawai yang telah terverifikasi.

2.6.1.3. Pengguna perangkat memastikan perangkatnya hanya digunakan oleh dirinya sendiri, dan tidak digunakan oleh orang lain yang tidak berhak.

2.6.1.4. Pengguna perangkat memastikan perangkat *mobile* yang berada pada lokasi yang aman.

2.6.1.5. Pengguna perangkat memastikan fitur keamanan seperti *screen lock, password*, dan sebagainya, dalam keadaan aktif.

2.6.1.6. Perangkat dapat menggunakan *password*, fingerprint atau face id.

2.6.1.7. Pengguna perangkat memastikan *antivirus* terpasang dan terupdate pada perangkatnya.

2.6.1.8. Pengguna bertanggung jawab atas segala informasi yang ada pada perangkat *mobile* yang dimilikinya.

2.6.1.9. Apabila terjadi kerusakan atau kehilangan pada perangkat *mobile*, pengguna melaporkannya pada *IT Service desk*.

2.6.1.10. Pengguna dapat sewaktu-waktu diminta untuk menyerahkan perangkat *mobile*-nya kepada perusahaan untuk keperluan pemeriksaan atau audit.

2.6.1.11. Pengaturan laptop / desktop untuk waktu siaga *(standby / idle)* adalah 3 menit

2.6.2. Pelaksanaan peminjaman aset, untuk dibawa keluar kantor.

2.6.2.1. Permohonan izin membawa aset keluar lokasi disampaikan pada *IT Service Desk*.

2.6.2.2. Permohonan tersebut diverifikasi keakuratan dan kelengkapannya, serta dimintakan izin pada pemilik aset.

2.6.2.3. Ketika pengambilan aset, dilakukan pengecekan untuk memastikan kondisi aset yang akan dibawa keluar lokasi.

2.6.2.4. Aset yang sedang dibawa keluar lokasi dicatat dalam *CMDB* untuk menjelaskan bahwa aset tidak ada di dalam lokasi.

2.6.2.5. Pengembalian aset dilakukan pada jadwal yang telah disepakati, dan jika membutuhkan tambahan waktu, diinformasikan pada IT Service desk dengan persetujuan pemilik aset; dan

2.6.2.6. Ketika pengembalian aset, dilakukan pengecekan untuk memastikan kondisi aset yang dikembalikan.

2.6.3. Kebijakan dan Implementasi *removable media*

2.6.3.1. *Removable media* yang boleh digunakan hanya tipe *removable disk* yang telah ditentukan oleh perusahaan;

2.6.3.2. Perusahaan mencatat informasi mengenai removable media sebagai *Configuration Item (CI)* dalam *CMDB*.

2.6.3.3. Pendistribusian dan pelabelan informasi pada *removable media* mengikuti klasifikasi informasi masing-masing.

2.6.4. Disposal Media

2.6.4.1. Permintaan *disposal media* diajukan pada *IT Service desk*, disertai dengan pemilik, jenis media, nomor seri, serta klasifikasi informasi yang ada.

2.6.4.2. Apabila dibutuhkan, data yang tersimpan di-*backup* terlebih dahulu.

2.6.4.3. Apabila terdapat media yang telah dikumpulkan untuk dimusnahkan namun belum dimusnahkan, IT Service desk bertanggung jawab terhadap keamanan media tersebut.

2.6.4.4. Setelah media dikumpulkan, detail informasi tentang media di-*update* pada *CMDB*.

2.6.4.5. Perusahaan dapat memusnahkan media menggunakan *disk shredder* dengan ketentuan pemusnahan disaksikan lebih dari satu orang, atau menggunakan jasa dari pihak ketiga dengan ketentuan terdapat sertifikat disposal; dan

2.6.4.6. Setelah media dimusnahkan, detail informasi tentang media di-*update* pada *CMDB*.

2.6.5. Penggunaan Instant Messaging

2.6.5.1. Penggunaan instant messaging dikelola sebagai berikut:

a. Pengguna menggunakan instant messaging untuk keperluan pekerjaan hanya instant messaging yang sudah ditentukan oleh Perusahaan;
b. Pengguna dilarang menggunakan media instant messaging dalam pengiriman informasi rahasia perusahaan dan segala hal yang dapat merusak reputasi perusahaan baik dalam bentuk apapun;
c. Pengguna dilarang mengirimkan material yang melanggar hak cipta atau hak atas kekayaan intelektual;
d. Pengguna dilarang menggunakan instant messaging untuk hal-hal yang dapat mengganggu atau merusak data maupun pekerjaan pengguna lain.
e. Pengguna dilarang mendistribusikan material yang mengganggu keharmonisan lingkungan internal maupun eksternal (misalnya: fitnah, isu rasial, pornografi, bullying, rahasia personal, dll).

2.6.6. Akses *user* jaringan dan *ERP*

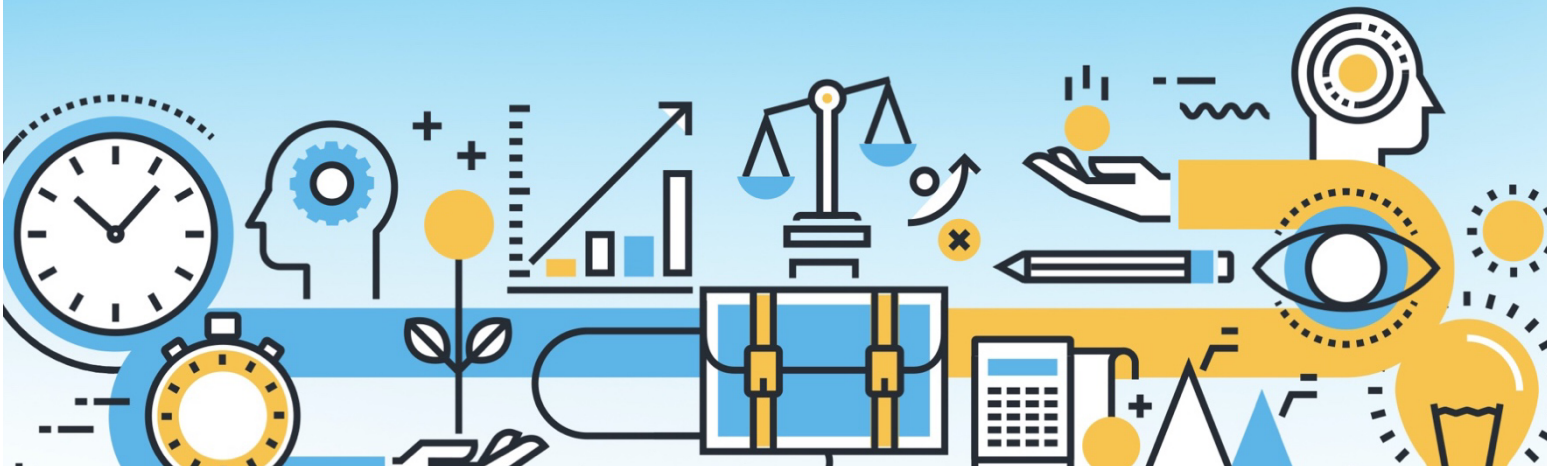
2.6.6.1. Pengguna hanya dapat mengakses atau menggunakan sumberdaya atau fasilitas TI perusahaan jika memiliki Akun Akses. Setiap pegawai hanya diperbolehkan memiliki satu Akun Akses, merujuk kepada *ID* Kepegawaian yang ada.

2.6.6.2. Akun Akses dikelola pada sistem terpusat dan digunakan sebagai referensi untuk melakukan otentikasi pada layanan *email*, akses internet, akses berbagai sistem informasi atau sumber daya TI lain.

2.6.6.3. Pengelolaan akun akses untuk internal

a. Permintaan hak akses (atau perubahannya) hanya dapat dilakukan oleh Manajer Divisi dimana staff berada.
b. Pemetaan Akun Akses ke sistem informasi yang relevan dilakukan pada level administrasi sistem informasi terkait.
c. Setiap perubahan posisi staff (misalkan: mutasi, promosi atau pemberhentian) yang akan berdampak terhadap akses ke sistem informasi atau sumberdaya TI terkait lainnya, harus disampaikan oleh Manajer Divisi terkait kepada DSI. Pemberitahuan ini akan digunakan untuk penyesuaian Hak Akses.
d. Penggunaan Hak Akses akan selalu dimonitoring. Jika terdapat pelanggaran, maka akan dieskalasikan ke Manajer Divisi terkait untuk diproses sesuai dengan ketentuan yang berlaku di perusahaan.

BAB III
Etika dan Perilaku Perusahaan



BAB III. PENGORGANISASIAN, PENERAPAN, PENEGAKAN DAN KOMUNIKASI

3.1. ORGANISASI

3.1.1. Direksi bertanggung jawab atas dipatuhinya, diterapkannya Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT)* di lingkungan Perusahaan dibantu oleh *Steering Committee* dan SPI.

3.1.2. Manajer PPU, Kasi KP, dan setingkat bertanggung jawab atas penerapan Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT)* di lingkungan unit kerjanya masing-masing.

3.1.3. Direksi menunjuk *Steering Committee* yang bertanggung jawab untuk melaporkan pelanggaran terhadap pelaksanaan Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT).*

3.1.4. Setiap insan WIKA Beton menerima satu salinan Etika Usaha dan Tata Perilaku *(Code of Conduct)* dan menandatangani formulir pernyataan bahwa yang bersangkutan telah menerima, memahami dan setuju untuk mematuhi Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT)* yang didokumentasikan oleh fungsi SDM di masing-masing unit kerja.

3.2. PENEGAKAN ETIKA DAN TATA PERILAKU SISTEM INFORMASI (*CODE OF CONDUCT IT*)

3.2.1. Setiap insan WIKA Beton harus melaporkan setiap fakta penyimpangan Etika Usaha dan Tata Perilaku *(Code of Conduct)* kepada DSI dan identitas pelapor dilindungi.

3.2.2. DSI menindaklanjuti setiap laporan dan menyampaikan rekomendasi tindak lanjut atas temuan tersebut kepada *Steering Committee* untuk memutuskan pemberian tindakan pembinaan, sanksi disiplin dan/atau tindakan perbaikan serta pencegahan yang harus dilaksanakan.

3.2.3. Insan WIKA Beton yang melakukan penyimpangan Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT)* memiliki hak untuk didengar penjelasannya di hadapan atasan langsung sebelum pemberian tindakan pembinaan atau hukuman disiplin.

3.3. SOSIALISASI DAN INTERNALISASI

3.3.1. DSI atau fungsi yang ditunjuk bertugas untuk melaksanakan sosialisasi dan internalisasi Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT)* kepada seluruh insan WIKA Beton.

3.3.2. Setiap insan WIKA BETON dapat meminta penjelasan atau menyampaikan pertanyaan terkait dengan Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT)* kepada atasan langsung atau kepada DSI.

3.4. PEMBARUAN/REVISI ETIKA USAHA DAN TATA PERILAKU (*CODE OF CONDUCT*)

3.4.1. Setiap insan WIKA BETON dapat memberikan masukan untuk penyempurnaan *Code of Conduct* kepada DSI.

3.4.2. DSI mengusulkan pembaruan/revisi Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT)* kepada *Steering Committee*.

3.4.3. *Steering Committee* mengajukan pembaruan/revisi Etika dan Tata Perilaku Sistem Informasi *(Code of Conduct IT)* untuk ditetapkan oleh Direksi.

3.5. KOMUNIKASI

3.5.1. Temuan-temuan / penyalahgunaan dikomunikasikan ke M. DSI melalui support@wika-beton.co.id

3.5.2. Audit *Code of Conduct* dilakukan oleh DSI bersama SPI

PEDOMAN
ETIKA DAN PERILAKU
CODE OF CONDUCT 2023

Pernyataan **Komitmen**

LAMPIRAN-1

SURAT PERNYATAAN INSAN WIKA Beton

Dengan ini saya menyatakan telah menerima, membaca dan memahami Etika dan Tata Perilaku Sistem Informasi (*Code of Conduct IT*) PT Wijaya Karya Beton Tbk. tanggal (efektif) ..... dan bersedia untuk mematuhi semua ketentuan yang tercantum di dalamnya dan menerima sanksi atas pelanggaran (jika ada) yang saya lakukan.

(Tempat) (Tanggal, bulan, tahun)
....., ...

....
(Nama , Tanda Tangan dan Jabatan)

LAMPIRAN 2

SURAT PERNYATAAN PEJABAT YANG BERTANGGUNG JAWAB
ATAS PENERAPAN ETIKA DAN TATA PERILAKU SISTEM INFORMASI
(*CODE OF CONDUCT IT*)

Sehubungan dengan pemberlakuan Etika Usaha dan Tata Perilaku Sistem Informasi (*Code of Conduct IT*) PT Wijaya Karya Beton Tbk. tanggal (efektif) ....., yang telah saya terima dan pahami sepenuhnya, saya menyatakan bahwa pada tahun ..... :

1. Telah mendistribusikan Etika dan Tata Perilaku Sistem Informasi (*Code of Conduct IT*), telah diterima dan ditandatangani oleh seluruh insan WIKA Beton di unit kerja yang menjadi tanggung jawab saya.
2. Telah mengkoordinasikan pelaksanaan sosialisasi dan internalisasi dengan *Steering Committee*.
3. Telah melakukan upaya-upaya untuk menjamin kepatuhan terhadap Etika dan Tata Perilaku Sistem Informasi (*Code of Conduct IT*) di unit kerja yang menjadi tanggung jawab saya.
4. Telah melaporkan semua pelanggaran secara lengkap kepada *Steering Committee.*
5. Telah melaksanakan semua pemberian sanksi disiplin dan tindakan pembinaan/perbaikan yang harus dilakukan di lingkungan unit kerja yang menjadi tanggung jawab saya.

(Tempat) (Tanggal. Bulan, Tahun)
....., ...
Nama/NIP : .....
Jabatan : .....

Tanda tangan : .....

PEDOMAN

ETIKA DAN PERILAKU

CODE OF CONDUCT 2023