S U R A T - K E P U T U S A N
Nomor: SKEP / 6 / P / BD / X / 2025

Tentang

KEBIJAKAN TEKNOLOGI INFORMASI

DIREKSI PT PINDAD

Menimbang :

1. Bahwa untuk mengatur kebijakan teknologi informasi Perusahaan, telah ditetapkan Surat Keputusan Direksi PT Pindad nomor: SKEP/10/P/BD/VII/2021 tanggal 12 Juli 2021 tentang Kebijakan Teknologi Informasi di Lingkungan Perusahaan.
2. Bahwa dalam rangka mendukung transformasi digital perusahaan yang terintegrasi dan berkelanjutan serta optimalisasi pemanfaatan teknologi informasi di lingkungan Perusahaan, maka dipandang perlu menetapkan kembali Surat Keputusan Direksi tentang Kebijakan Teknologi Informasi.

Mengingat :

1. Undang-Undang Nomor 40 tahun 2007 tanggal 2 November 2007 tentang Perseroan Terbatas sebagaimana telah diubah dengan Undang-Undang No. 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang;
2. Peraturan Menteri Badan Usaha Milik Negara nomor: PER-2/MBU/03/2023 tanggal 3 Maret 2023 tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik Negara;
3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tanggal 25 Desember 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tanggal 2 Januari 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
4. Undang-Undang Nomor 27 Tahun 2022 tanggal 17 Oktober 2024 tentang Perlindungan Data Pribadi;
5. Surat Keputusan Direksi PT Pindad Nomor: SKEP/1/P/BD/II/2025 tanggal 10 Februari 2025 beserta perubahannya nomor: SKEP/1a/P/BD/II/2025 tanggal 14 Juli 2025 tentang Organisasi dan Tata Kerja PT Pindad.

M E M U T U S K A N

Menetapkan : Keputusan Direksi PT Pindad tentang Kebijakan Teknologi Informasi sebagai berikut:

/**BAB I**.....

BAB I
PENDAHULUAN
Pasal 1
Pengertian

Dalam Keputusan ini yang dimaksud dengan:

1. Aset teknologi informasi adalah aset milik Perusahaan yang tercatat secara akuntansi dan memiliki nilai strategis maupun ekonomi baik dalam bentuk aset berwujud/aset tidak berwujud yang meliputi: perangkat keras, perangkat lunak, lisensi penggunaan sistem, basis data, konfigurasi sistem, kode sumber (*source code*), dokumentasi teknis, algoritma, serta hasil inovasi digital yang menjadi bagian dari infrastruktur teknologi informasi Perusahaan.
2. Aset tidak berwujud teknologi informasi adalah aset tidak berwujud milik Perusahaan yang berupa elemen non-fisik namun memiliki nilai strategis dan ekonomi, meliputi: perangkat lunak, lisensi penggunaan sistem, basis data, konfigurasi sistem, kode sumber (*source code*), dokumentasi teknis, algoritma, serta hasil inovasi digital yang menjadi bagian dari infrastruktur teknologi informasi perusahaan.
3. Data pribadi adalah setiap informasi tentang individu yang dapat diidentifikasi secara langsung maupun tidak langsung, sebagaimana dimaksud dalam Undang-Undang tentang Perlindungan Data Pribadi (UU PDP).
4. Keamanan Data adalah serangkaian kebijakan, pedoman, dan prosedur untuk melindungi data dari akses tidak sah, kebocoran, penyalahgunaan, atau kerusakan, termasuk data pribadi sesuai Undang-Undang Perlindungan Data Pribadi.
5. Holding Industri Pertahanan (Defend ID) adalah PT Len Industri (Persero).
6. *Information Technology Service Management* (ITSM) adalah tata kelola layanan teknologi informasi berdasarkan kerangka kerja terbaik (*best practices*) meliputi pengelolaan insiden, masalah, perubahan, aset, permintaan layanan, dan perbaikan berkelanjutan.
7. Perusahaan adalah PT Pindad.
8. *Seat Management* adalah metode pengelolaan layanan teknologi informasi di mana mitra layanan teknologi informasi bertanggung jawab terhadap penyediaan, pemeliharaan, dan pengelolaan perangkat teknologi informasi.
9. *Service Level Agreement* (SLA) adalah kesepakatan tingkat layanan yang wajib dipenuhi oleh Fungsi Teknologi Informasi atau mitra layanan teknologi informasi terhadap pengguna internal maupun eksternal.
10. Sistem *Enterprise Resource Planning* (Sistem ERP) adalah *platform* sistem informasi terintegrasi yang digunakan untuk mengelola seluruh proses inti bisnis Perusahaan.
11. Teknologi Informasi adalah keseluruhan infrastruktur dan teknologi yang meliputi perangkat keras (*hardware*), perangkat lunak (*software*), jaringan, basis data, serta aplikasi yang digunakan oleh Perusahaan untuk mendukung proses operasional, produksi, manajemen, dan pengendalian Perusahaan.

Pasal 2
Maksud & Tujuan

1. Kebijakan ini ditetapkan sebagai kerangka tata kelola teknologi informasi dan keamanan data yang mengikat seluruh unit kerja Perusahaan, guna menjamin pengelolaan sistem teknologi informasi yang aman, terintegrasi, dan patuh terhadap regulasi.
2. Tujuan kebijakan ini adalah:
   a. Menjamin keselarasan strategi teknologi informasi dengan tujuan dan strategi bisnis Perusahaan serta Holding Industri Pertahanan (Defend ID).

/b. Menetapkan.....

b. Melindungi kerahasiaan, integritas, dan ketersediaan informasi, termasuk data pribadi, sesuai prinsip perlindungan dan data.
c. Menetapkan prinsip kepemilikan, pengelolaan, dan akuntabilitas atas seluruh aset teknologi informasi, termasuk aset tidak berwujud teknologi informasi.
d. Memastikan bahwa Sistem ERP berfungsi sebagai sistem utama dalam pengelolaan data perusahaan, guna menjamin konsistensi, akurasi informasi lintas fungsi bisnis.
e. Menyediakan layanan teknologi informasi yang andal, responsif, dan terukur sesuai dengan kerangka kerja ITSM.
f. Menetapkan mekanisme manajemen risiko teknologi informasi, rencana pemulihan bencana (*Disaster Recovery Plan* – DRP), serta rencana keberlanjutan bisnis (*Business Continuity Plan* – BCP) guna menghadapi gangguan operasional dan ancaman siber secara proaktif.
g. Meningkatkan tingkat kepatuhan terhadap regulasi yang berlaku.

Pasal 3

Ruang Lingkup

1. Kebijakan ini berlaku untuk seluruh unit kerja, divisi, direktorat, dan pegawai Perusahaan.
2. Kebijakan ini mencakup seluruh Sistem Teknologi Informasi.
3. Kebijakan ini juga berlaku untuk pengelolaan data lintas Holding Industri Pertahanan (Defend ID), mitra layanan teknologi informasi, serta pihak eksternal yang memiliki akses ke Sistem Teknologi Informasi atau data Perusahaan.

BAB II
TATA KELOLA TEKNOLOGI INFORMASI
Pasal 4
Prinsip Tata Kelola Teknologi Informasi

Penerapan teknologi informasi yang dilaksanakan Perusahaan, harus memenuhi prinsip sebagai berikut:

1. Keselarasan Strategis: setiap pengembangan dan pemanfaatan teknologi informasi harus selaras dengan strategi bisnis Perusahaan dan Holding Industri Pertahanan (Defend ID).
2. Transparansi: Setiap aktivitas pengembangan teknologi informasi harus didokumentasikan dengan baik, dilaporkan secara transparan tanpa mengorbankan aspek kerahasiaan, serta tersedia untuk pemeriksaan oleh fungsi pengawasan internal maupun auditor independen dari luar perusahaan.
3. Nilai Tambah: penggunaan teknologi informasi harus memberikan manfaat nyata dalam meningkatkan efisiensi, efektivitas, keamanan, serta daya saing Perusahaan.
4. Pengendalian Internal: Seluruh transaksi, data, pertukaran data baik internal maupun eksternal dan laporan yang diproses melalui sistem informasi yang dikelola sesuai dengan prinsip-prinsip pengendalian internal dan ketentuan peraturan yang berlaku, guna menjamin akurasi, integritas, keterlacakan (*auditability*), dan kepatuhan (*compliance*) di seluruh fungsi bisnis.
5. Kepatuhan Regulasi: Pengelolaan teknologi informasi harus mematuhi seluruh ketentuan hukum dan peraturan yang berlaku, baik yang ditetapkan oleh pemerintah maupun lembaga terkait, serta mengacu pada praktik terbaik secara global
6. Akuntabilitas: Setiap pegawai yang menggunakan, mengakses, dan mengelola sistem teknologi informasi harus dapat mempertanggungjawabkan tindakan, keputusan, dan penggunaan sumber daya teknologi informasi sesuai kewenangan yang diberikan perusahaan.
7. Sentralisasi: Seluruh proses pengembangan, pemanfaatan, dan pengadaan sistem teknologi informasi wajib dilaksanakan secara terpusat dan dikoordinasikan sepenuhnya dengan Fungsi Teknologi Informasi. Sistem paralel atau *shadow systems* yang berjalan di luar kendali dan arsitektur resmi perusahaan tidak diperkenankan, guna menjaga keselarasan tata kelola, keamanan, efisiensi, dan integrasi sistem.

Pasal 5
Manfaat Penerapan Teknologi Informasi

Penerapan teknologi informasi yang dilaksanakan Perusahaan, harus memenuhi manfaat sebagai berikut:

1. Manfaat teknologi informasi di Perusahaan sebagai berikut:
   a. Sebagai alat untuk melakukan perubahan, sebagai akibat dari tuntutan kompetisi.
   b. Sarana perbaikan berkelanjutan dan membangun citra Perusahaan.
2. Untuk memenuhi manfaat teknologi informasi Perusahaan, maka harus terlaksananya:
   a. Pengembangan Aplikasi dan Infrastruktur yang tepat guna dan kesesuaian terhadap kebutuhan fungsi usaha.
   b. Pengembangan kompetensi Sumber Daya Manusia (SDM) dan kemampuan organisasi melalui program manajemen pengetahuan.
   c. Pembangun dan pemeliharaan lingkungan yang mendukung keakuratan, keaktualan dan keabsahan data/informasi, bersama dengan setiap unit manajemen.

/d. Mengkomunikasikan.....

d. Mengkomunikasikan dan mengevaluasi setiap kebijakan, pedoman, ketentuan dan prosedur secara berkala untuk dipahami dan menjadi komitmen bersama seluruh manajemen dan seluruh pegawai.

Pasal 6

Fokus Utama Tata Kelola Teknologi Informasi

1. Proses Penyelarasan Strategi Teknologi Informasi (*Strategic Alignment*)

   Penyusunan strategi teknologi informasi Perusahaan, dilakukan dengan mempertimbangkan aspek:

   a. Keselarasannya dengan tujuan Perusahaan, baik dalam jangka pendek dan jangka panjang,
   b. Kondisi teknologi informasi saat ini dan masa mendatang, biaya dan risiko yang ditimbulkan karena penggunaan teknologi informasi, serta manfaatnya bagi Perusahaan,
   c. Kapasitas dan kapabilitas organisasi teknologi informasi untuk memberikan layanan kepada bisnis Perusahaan serta investasi yang diperlukan untuk meningkatkan kapasitas dan kapabilitas organisasi tersebut.

2. Proses Dukungan Teknologi Informasi (*Value Delivery*)

   Proses teknologi informasi Perusahaan harus memberikan dukungan atau nilai tambah kepada bisnis Perusahaan, sehingga:

   a. Perusahaan memiliki keunggulan kompetitif dalam industri,
   b. Proses bisnis dan pengambilan keputusan dapat dilakukan oleh Perusahaan secara cepat,
   c. Teknologi Informasi dapat memberikan dukungan yang optimal untuk penyediaan data dan informasi Perusahaan secara akurat dan cepat,
   d. Seluruh Pegawai dapat memaksimalkan penggunaan teknologi informasi dalam pelaksanaan tugas-tugasnya,
   e. Produktivitas dan efisiensi Pegawai meningkat.

3. Proses Pengelolaan Sumber Daya Teknologi Informasi (*Resource Management*)

   Agar perencanaan Perusahaan dalam penggunaan teknologi informasi dapat memberikan manfaat yang optimal, maka harus dipastikan bahwa alokasi sumber daya manusia (*people, skill, and knowledge*), pembelian dan penggunaan aplikasi teknologi informasi, pembelian dan penggunaan fasilitas teknologi informasi, penggunaan informasi dan data teknologi informasi telah dilakukan dengan tepat sesuai dengan kebutuhan Perusahaan.

4. Proses Penilaian Kinerja Teknologi Informasi (*Performance Measurement*)

   Penilaian kinerja teknologi informasi dilakukan dengan mempertimbangkan aspek:

   a. Kontribusi pemanfaatan informasi terhadap bisnis Perusahaan,
   b. Kepuasan pengguna teknologi informasi,
   c. Efektivitas dan efisiensi dalam penggunaan teknologi informasi, orientasi teknologi informasi terhadap masa depan bisnis Perusahaan,
   d. Keberhasilan implementasi program transformasi di bidang teknologi informasi,
   e. Kepatuhan terhadap peraturan perundang-undangan

/**Pasal 7**.....

Pasal 7

Kerangka Tanggung Jawab Tata Kelola Teknologi Informasi

Dalam rangka mendukung tata kelola teknologi informasi yang terintegrasi, aman, dan sesuai dengan prinsip akuntabilitas serta kepatuhan regulasi, Direksi menetapkan kerangka tanggung jawab seluruh fungsi terkait di Perusahaan sebagai berikut:

1. Fungsi Teknologi Informasi

   Sebagai pengelola utama tata kelola teknologi informasi, Fungsi Teknologi Informasi memiliki tanggung jawab strategis atas perencanaan, pengembangan, pemeliharaan, dan pengendalian sistem teknologi informasi serta memastikan tersedianya layanan teknologi informasi yang aman, andal, terintegrasi, serta selaras dengan kebutuhan bisnis.

2. Fungsi Pengawasan

   Bertanggung jawab melaksanakan audit atas transaksi, pengendalian, dan kepatuhan sistem teknologi informasi guna memastikan integritas proses, efektivitas kontrol, serta kesesuaian terhadap kebijakan dan regulasi yang berlaku.

3. Fungsi Sumber Daya Manusia (SDM)

   Bertanggung jawab memastikan ketersediaan SDM teknologi informasi yang kompeten, merancang kebutuhan talenta digital, mengembangkan kapabilitas dan kompetensi SDM, serta berkolaborasi aktif dengan Fungsi Teknologi Informasi dalam membangun budaya digital.

4. Fungsi Hukum

   Bertanggung jawab mendukung penerapan perlindungan hukum, pengelolaan perjanjian lisensi, serta administrasi dan pengawasan dokumen *Non-Disclosure Agreement* (NDA) dengan vendor dan mitra layanan teknologi informasi, guna memastikan kepatuhan, transparansi, dan keamanan kerja sama.

5. Fungsi Akuntansi dan Keuangan

   Bertanggung jawab memastikan bahwa integrasi sistem ERP mendukung proses pencatatan, pelaporan, dan pengendalian internal keuangan sesuai dengan prinsip akuntansi dan tata kelola yang berlaku.

6. Fungsi Produksi

   Bertanggung jawab atas akurasi input data produksi, mendukung penerapan integrasi data produksi ke dalam ERP sebagai *single source of truth*, validasi sistem digital, dan kesiapan pemulihan proses produksi yang bersifat kritis.

7. Fungsi Mutu

   Bertanggung jawab memastikan bahwa pemanfaatan teknologi informasi secara optimal mendukung penerapan sistem mutu, K3LH, serta validasi data mutu melalui integrasi sistem ERP yang andal dan terkontrol.

8. Fungsi Pendukung Lainnya

   Bertanggung jawab atas keakuratan data, integritas proses bisnis, serta kesiapan operasional dalam pemanfaatan sistem. Tanggung jawab ini mencakup pemberian persetujuan atas perubahan sistem, validasi kebutuhan fungsional, pengawasan akses berbasis peran, serta dukungan terhadap audit dan pemulihan sistem saat terjadi gangguan.

Pasal 8

***Enterprise Resource Planning* (ERP) sebagai Sistem Utama**

1. ERP merupakan sistem utama yang wajib digunakan untuk seluruh transaksi dan pelaporan di bidang keuangan, produksi, rantai pasok, SDM, dan manajemen aset.

/2. Semua.....

2. Semua transaksi di luar ERP tidak diakui secara resmi, kecuali dalam keadaan darurat atau pengecualian yang ditetapkan oleh Direksi.
3. Integrasi modul ERP antar divisi harus dipelihara agar data tetap konsisten, akurat, dan dapat diaudit.
4. Fungsi Teknologi Informasi wajib menjamin ketersediaan, keamanan, dan keandalan ERP sesuai dengan SLA yang telah disepakati.

/**BAB III**….

BAB III
PERLINDUNGAN DATA DAN KEAMANAN INFORMASI
Pasal 9
Prinsip Perlindungan Data

Penerapan perlindungan data di lingkungan Perusahaan, harus memenuhi prinsip sebagai berikut:

1. Kepatuhan Regulasi: perlindungan data harus dilaksanakan sejalan dengan ketentuan hukum dan peraturan yang berlaku, baik yang ditetapkan oleh pemerintah maupun lembaga terkait.
2. Keamanan Data: menjaga keamanan data melalui penerapan mekanisme pencegahan terhadap akses tidak sah dan penyebaran informasi yang tidak semestinya
3. Pengendalian Akses: mengimplementasikan prinsip *least privilege* dalam pengelolaan hak akses, memastikan bahwa setiap pengguna hanya memiliki akses sesuai dengan peran dan tanggung jawabnya
4. Kedaulatan Data: menyimpan data perusahaan di pusat data yang berlokasi di wilayah Republik Indonesia, sesuai dengan prinsip kedaulatan data dan kebijakan nasional
5. Enkripsi Data: menggunakan teknologi dan mekanisme pengamanan yang memadai untuk menjaga kerahasiaan, integritas, dan keandalan data, sesuai dengan praktik terbaik dan standar yang berlaku

Pasal 10
Klasifikasi Data & Informasi

Data perusahaan diklasifikasikan dalam empat kategori:

1. Rahasia

   Data yang bersifat strategis dan memiliki dampak tinggi terhadap keberlangsungan perusahaan, termasuk data pertahanan, inovasi, kode sumber, data keuangan, serta informasi yang dilindungi oleh perjanjian kerahasiaan (*Non-Disclosure Agreement*/NDA). Akses terhadap data ini dibatasi secara ketat dan hanya diberikan kepada pihak yang berwenang.
2. Terbatas

   Data operasional internal yang hanya dapat diakses oleh unit kerja tertentu sesuai dengan fungsi dan tanggung jawabnya. Pengelolaan akses dilakukan berdasarkan prinsip pengendalian berbasis peran.
3. Internal

   Data yang dapat diakses oleh seluruh karyawan tanpa memerlukan perjanjian khusus, namun tetap dikelola sesuai dengan kebijakan internal dan prinsip keamanan informasi.
4. Publik

   Data yang dapat diumumkan kepada pihak eksternal, termasuk mitra, pemangku kepentingan, atau masyarakat umum sesuai dengan persetujuan dan ketetapan resmi dari Direksi.

Pasal 11
Perlindungan Data Pribadi

Perlindungan data pribadi di lingkungan Perusahaan mencakup hal-hal berikut:

1. Pengumpulan data pribadi dilakukan jika individu telah memberikan persetujuan secara jelas dan sadar, sebagai bentuk penghormatan terhadap hak privasi dan transparansi.
2. Pemrosesan data sesuai tujuan yang sah dan jelas.

/3. Data…..

3. Data pribadi hanya disimpan selama jangka waktu yang diperlukan untuk memenuhi tujuan pemrosesan, sesuai dengan ketentuan hukum dan kebijakan internal.
4. Subjek data memiliki hak atas akses, koreksi, penghapusan, serta penarikan persetujuan atas penggunaan data pribadinya, sebagaimana diatur dalam peraturan perundang-undangan.
5. Setiap insiden kebocoran data pribadi wajib dilaporkan kepada otoritas yang berwenang sesuai dengan ketentuan hukum yang berlaku, sebagai bagian dari tanggung jawab dan akuntabilitas perusahaan
6. Fungsi Teknologi Informasi wajib mengintegrasikan mekanisme perlindungan data pribadi ke dalam sistem ERP dan seluruh aplikasi pendukung lainnya yang memproses atau menyimpan data pribadi
7. Mitra layanan teknologi informasi yang mengelola data pribadi wajib memenuhi ketentuan yang diatur dalam Undang-Undang Perlindungan Data Pribadi (UU PDP). Dalam kontrak kerja sama wajib memuat klausul perlindungan data pribadi guna menjamin kepatuhan terhadap regulasi

Pasal 12

Pengendalian Akses & Enkripsi Data

1. Perusahaan menerapkan pengendalian akses yang disesuaikan dengan peran dan tanggung jawab masing-masing pengguna.
2. Fungsi Teknologi Informasi wajib memastikan bahwa seluruh aktivitas pengguna dalam sistem tercatat secara menyeluruh melalui mekanisme audit trail yang andal.
3. Fungsi Teknologi Informasi bertanggung jawab atas pengelolaan, pemantauan, dan tinjauan berkala terhadap hak akses pengguna sebagai bagian dari pengendalian internal yang efektif.
4. Perlindungan data dilakukan secara proporsional terhadap tingkat klasifikasi data, dengan enkripsi diterapkan sebagai salah satu mekanisme utama untuk menjaga kerahasiaan dan integritas informasi.

Pasal 13

Manajemen Insiden Keamanan Informasi

1. Perusahaan menerapkan manajemen insiden keamanan informasi sebagai bagian integral dari tata kelola teknologi informasi dan pengelolaan risiko perusahaan.
2. Setiap insiden keamanan informasi wajib dilaporkan, dicatat, dan ditangani secara sistematis untuk meminimalkan dampak terhadap operasional, data, dan reputasi perusahaan
3. Insiden keamanan informasi diklasifikasikan berdasarkan tingkat kritikalitasnya guna menentukan prioritas penanganan dan mekanisme eskalasi yang tepat, dengan klasifikasi sebagai berikut:
    a. Kritis: Insiden yang berdampak besar terhadap keberlangsungan operasional dan keamanan sistem, seperti: kebocoran data, peretasan sistem ERP, serangan *malware* pada *server* utama.
    b. Sedang: Insiden yang mengganggu sebagian fungsi sistem namun tidak menyebabkan gangguan total, seperti: gangguan aplikasi non-kritis atau percobaan akses tidak sah yang terdeteksi.
    c. Ringan: Insiden minor yang tidak memengaruhi operasional perusahaan secara signifikan, seperti kesalahan konfigurasi kecil atau gangguan teknis yang dapat segera diatasi.

/4. Insiden…..

4. Insiden yang signifikan, terutama yang melibatkan kebocoran data pribadi, wajib segera dilaporkan kepada Direksi, Fungsi Pengawasan, dan otoritas terkait sesuai ketentuan peraturan perundang-undangan, termasuk UU Perlindungan Data Pribadi.
5. Fungsi Teknologi Informasi bertanggung jawab menyediakan kapabilitas deteksi ancaman secara proaktif, termasuk pemanfaatan teknologi dan proses yang mendukung identifikasi dini terhadap potensi insiden keamanan siber.

BAB IV
ASET TEKNOLOGI INFORMASI
Pasal 14
Pengendalian Aset Teknologi Informasi

1. Seluruh aset teknologi informasi merupakan aset milik Perusahaan dan berada di bawah tanggung jawab Fungsi Teknologi Informasi sebagai pengelola utama.
2. Aset teknologi informasi wajib dikelola secara tertib, transparan, dan dapat diaudit, serta dicatat dalam sistem ERP sesuai prinsip akuntansi yang berlaku.
3. Pengelolaan ketersediaan aset teknologi informasi melalui skema *seat management* berada dalam tanggung jawab mitra layanan teknologi informasi dan tunduk pada kontrol layanan teknologi informasi.
4. Kemitraan dengan pihak eksternal yang melibatkan pengembangan aset tidak berwujud wajib dilindungi melalui perjanjian tertulis. Perjanjian tersebut harus mencakup ketentuan kerahasiaan (*Non-Disclosure Agreement*/NDA) serta klausul perlindungan hak kekayaan intelektual, guna memastikan keamanan informasi dan kepemilikan hasil inovasi.

Pasal 15
Pemanfaatan Aset Tidak Berwujud oleh Pihak Eksternal

1. Aset tidak berwujud milik Perusahaan hanya dapat digunakan oleh pihak eksternal berdasarkan perjanjian tertulis yang telah disetujui dan ditandatangani oleh Direksi.
2. Setiap pemanfaatan aset tidak berwujud oleh pihak eksternal wajib memenuhi ketentuan berikut:
   a. Mendapatkan persetujuan dari Fungsi Teknologi Informasi, Fungsi Hukum, dan Direksi;
   b. Didukung oleh dokumen hukum yang sah, seperti perjanjian lisensi, *Non-Disclosure Agreement* (NDA), atau kontrak kerja sama yang secara eksplisit melindungi kepentingan Perusahaan;
   c. Mematuhi ketentuan perlindungan data pribadi dan keamanan informasi sesuai dengan regulasi nasional yang berlaku.
3. Pihak eksternal yang melanggar ketentuan ini akan dikenakan sanksi hukum sesuai dengan perjanjian dan peraturan perundang-undangan yang berlaku.

/BAB V…..

BAB V
MANAJEMEN RISIKO TEKNOLOGI INFORMASI

Pasal 16
Prinsip Manajemen Risiko Teknologi Informasi

1. Manajemen risiko teknologi informasi Perusahaan merupakan bagian integral dari sistem manajemen risiko perusahaan.
2. Prinsip manajemen risiko TI yang diterapkan mencakup:
   a. Pencegahan terhadap insiden dan gangguan operasional;
   b. Keberlanjutan layanan melalui kesiapan sistem dan infrastruktur teknologi informasi dalam menghadapi gangguan;
   c. Integrasi dengan tata kelola perusahaan dan sinergi dengan ekosistem Holding Industri Pertahanan (Defend ID);
   d. Transparansi dan akuntabilitas dalam pelaporan dan mitigasi risiko;
   e. Kepatuhan terhadap regulasi nasional dan standar internasional.

Pasal 17
Business Continuity Plan (BCP) dan *Disaster Recovery Plan* (DRP)

1. Perusahaan wajib memiliki rencana keberlanjutan operasional (*Business Continuity Plan*/BCP) untuk memastikan layanan tetap berjalan saat terjadi gangguan signifikan pada sistem informasi.
2. Rencana pemulihan bencana (*Disaster Recovery Plan*/DRP) disusun untuk menjamin pemulihan sistem, aplikasi, dan data penting dalam jangka waktu yang telah ditetapkan, termasuk dalam situasi bencana alam, gangguan teknis, atau serangan siber.

Pasal 18
Pelaporan Risiko dan Eskalasi

1. Setiap insiden atau potensi risiko teknologi informasi wajib segera dilaporkan kepada Fungsi Teknologi Informasi dan Fungsi Manajemen Risiko sesuai dengan mekanisme yang berlaku.
2. Risiko kritis wajib segera diekskalasi ke Direksi dan Fungsi Pengawasan untuk mendapat keputusan penanganan.

/**BAB VI**.....

BAB VI
KERANGKA KEAMANAN SIBER
Pasal 19
Prinsip Keamanan Siber

1. Perusahaan mengadopsi kerangka kerja keamanan siber yang selaras dengan standar internasional dan regulasi nasional.
2. Prinsip keamanan siber yang diterapkan meliputi:
   a. Kerahasiaan (*Confidentiality*): melindungi data dari akses tidak sah;
   b. Integritas (*Integrity*): menjaga keutuhan data dari perubahan tidak sah;
   c. Ketersediaan (*Availability*): menjamin ketersediaan sistem, data, dan layanan teknologi informasi;
   d. Keandalan (*Accountability*): setiap aktivitas pengguna harus tercatat dan dapat ditelusuri;
   e. Kepatuhan (*Compliance*): Mematuhi ketentuan hukum dan standar yang berlaku, termasuk regulasi nasional di bidang perlindungan data, keamanan siber, serta pedoman tata kelola yang ditetapkan oleh instansi terkait.

Pasal 20
Kerangka, Standar, dan Evaluasi Keamanan Informasi

1. Kerangka kerja keamanan siber mengacu pada standar yang ditetapkan oleh otoritas terkait, mencakup identifikasi risiko dan aset penting, penerapan kontrol perlindungan, pemantauan terhadap potensi gangguan, respons terhadap insiden, serta pemulihan sistem dan layanan secara terencana.
2. Perusahaan berkomitmen untuk menerapkan standar dan kerangka kerja yang diakui secara internasional maupun yang sesuai dengan standar yang ditetapkan oleh otoritas terkait dalam pengelolaan keamanan informasi.
3. Evaluasi kepatuhan terhadap standar pengelolaan keamanan informasi dilakukan secara berkala 1 (satu) kali setahun untuk menilai tingkat pengelolaan keamanan informasi.

Pasal 21
Koordinasi Keamanan Siber

1. Fungsi Teknologi Informasi wajib membentuk *Computer Security Incident Response Team* (CSIRT) yang bertugas menangani insiden keamanan siber.
2. CSIRT wajib berkoordinasi dengan BSSN, CSIRT Sektoral, dan lembaga terkait apabila terjadi insiden siber yang berdampak strategis pada pertahanan negara.
3. CSIRT bekerja sama dengan Fungsi Hukum untuk memastikan seluruh insiden siber yang berdampak hukum ditindaklanjuti sesuai peraturan perundang-undangan.

/**BAB VII**.....

BAB VII
SERVICE LEVEL AGREEMENT (SLA)

Pasal 22
Prinsip *Service Level Agreement* (SLA)

1. Perusahaan menetapkan *Service Level Agreement* (SLA) sebagai standar kinerja layanan teknologi informasi yang wajib dipenuhi oleh Fungsi Teknologi Informasi maupun mitra layanan teknologi informasi.
2. Mitra layanan teknologi informasi yang tidak memenuhi standar keamanan atau ketentuan dalam SLA dapat dikenakan sanksi sesuai perjanjian.
3. Seluruh SLA wajib dituangkan dalam dokumen formal dan menjadi bagian dari akuntabilitas kinerja Fungsi Teknologi Informasi serta penyedia layanan.
4. SLA bertujuan untuk menjamin bahwa layanan teknologi informasi memberikan nilai tambah, bersifat terukur, transparan, dan dapat dievaluasi secara objektif.
5. SLA berlaku bagi seluruh layanan teknologi informasi.

Pasal 23
Review *Service Level Agreement* (SLA)

1. Fungsi Teknologi Informasi wajib menyediakan mekanisme pemantauan, evaluasi dan pelaporan kinerja SLA secara berkala, baik *real-time* maupun periodik, dengan menggunakan sistem yang andal.
2. SLA wajib ditinjau ulang secara berkala sekurang-kurangnya 1 (satu) kali dalam setahun, untuk menyesuaikan dengan perkembangan teknologi, kebutuhan bisnis, dan perubahan regulasi.

/BAB VIII…..

BAB VIII
MANAJEMEN PROYEK SISTEM INFORMASI

Pasal 24
Kepemilikan Proyek Sistem Informasi

1. Seluruh proyek pengembangan, implementasi, dan pemeliharaan sistem informasi merupakan aset strategis milik Perusahaan, dan berada di bawah tanggung jawab Fungsi Teknologi Informasi sebagai pengelola utama.
2. Kepemilikan mencakup seluruh hasil proyek, meliputi:
   a. Perangkat keras dan lunak
   b. Aset tidak berwujud seperti kode sumber, konfigurasi sistem, basis data, dan dokumentasi teknis
   c. Proses bisnis terotomasi dalam ERP dan aplikasi pendukung
   d. Hak kekayaan intelektual atas inovasi yang dihasilkan.
3. Dalam kerja sama dengan pihak ketiga, wajib dituangkan dalam perjanjian resmi dengan klausul yang menjamin bahwa hasil proyek tetap menjadi aset.

Pasal 25
Serah Terima & Pemeliharaan Hasil Proyek

1. Setiap proyek sistem informasi wajib ditutup dengan dokumen serah terima resmi yang menyatakan bahwa seluruh aset hasil proyek, baik fisik maupun non-fisik, telah menjadi milik Perusahaan dan berada di bawah pengelolaan Fungsi Teknologi Informasi
2. Seluruh hasil proyek wajib didokumentasikan dan disimpan dalam repositori resmi Perusahaan untuk menjamin ketersediaan dan keamanan informasi.
3. Fungsi Teknologi Informasi wajib menyusun rencana pemeliharaan (*maintenance plan*) untuk memastikan keandalan dan keamanan sistem pasca-implementasi.
4. Fungsi Pengawasan berhak melakukan audit atas hasil proyek untuk memastikan kesesuaian dengan dokumen proyek, kontrak, dan kebijakan perusahaan.

/BAB IX…..

BAB IX
AUDIT & KEPATUHAN
Pasal 26
Prinsip Audit Teknologi Informasi

1. Perusahaan wajib melaksanakan audit atas sistem teknologi informasi secara berkala sebagai bagian dari tata kelola perusahaan yang transparan dan akuntabel.
2. Audit dilakukan oleh auditor independen yang ditunjuk oleh Direksi atau Holding Industri Pertahanan (Defend ID) atau instansi pemerintah terkait, guna menilai efektivitas tata kelola teknologi informasi, kepatuhan regulasi, dan kualitas pengendalian internal.
3. Setiap mitra layanan teknologi informasi atau pihak lain yang memiliki hubungan kerjasama dalam penyediaan teknologi informasi kepada Perusahaan wajib tunduk pada prinsip audit dan kepatuhan.

Pasal 27
Pelaksanaan Audit Teknologi Informasi

1. Fungsi Pengawasan wajib melaksanakan audit internal teknologi informasi secara berkala, sekurang-kurangnya 1 (satu) kali setahun guna menilai kepatuhan terhadap Kebijakan Teknologi Informasi dan ketentuan keamanan data.
2. Fungsi Pengawasan berwenang melakukan audit insidentil jika terdapat indikasi pelanggaran atau insiden kritis.
3. Pelaksanaan audit eksternal atas tata kelola teknologi informasi dilakukan secara berkala sekurang-kurangnya 1 (satu) kali setahun sebagai bagian dari tata kelola perusahaan yang transparan dan akuntabel.
4. Laporan hasil audit wajib ditindaklanjuti dengan rencana aksi perbaikan yang terdokumentasi.

Pasal 28
Tindak Lanjut Audit Teknologi Informasi

Seluruh temuan audit wajib ditindaklanjuti dengan rencana aksi perbaikan (*Corrective Action Plan*/CAP) yang terdokumentasi dan diselesaikan dalam jangka waktu yang sesuai dengan rekomendasi.

/**BAB X**…..

BAB X
HAK & KEWAJIBAN PENGGUNA LAYANAN TEKNOLOGI INFORMASI

Pasal 29
Hak Pengguna

Setiap pengguna sistem teknologi informasi di Perusahaan memiliki hak atas hal-hal berikut:

1. Layanan teknologi informasi yang andal dan memenuhi standar kinerja yang ditetapkan dalam *Service Level Agreement* (SLA).
2. Fasilitas untuk mengajukan permintaan dukungan, perbaikan, atau pengembangan layanan melalui saluran resmi yang tersedia.
3. Edukasi dan pelatihan berkala terkait penggunaan sistem informasi.
4. Perlindungan atas data pribadi sesuai dengan ketentuan yang diatur dalam Undang-Undang Perlindungan Data Pribadi (UU PDP).
5. Penyediaan fasilitas pendukung kerja, meliputi akses, sistem, *hardware*, dan *software* harus sesuai dengan peran dan tanggung jawab pegawai serta mengikuti ketentuan/peraturan yang berlaku.

Pasal 30
Kewajiban Pengguna

Setiap pengguna sistem teknologi informasi di Perusahaan memiliki kewajiban sebagai berikut:

1. Menggunakan sistem secara bertanggung jawab hanya untuk kepentingan dinas dan mendukung tujuan bisnis perusahaan.
2. Menjaga kerahasiaan akun, kata sandi, serta perangkat autentikasi pribadi, dan tidak membagikannya kepada pihak lain.
3. Mematuhi prinsip pengendalian akses.
4. Tidak menginstal perangkat lunak, aplikasi, atau sistem tanpa persetujuan resmi dari Fungsi Teknologi Informasi.
5. Seluruh pegawai yang menggunakan perangkat pribadi dalam aktivitas kerja diwajibkan untuk melaporkan penggunaannya kepada Fungsi Teknologi Informasi.
6. Dalam hal rotasi, promosi, atau mutasi, pegawai diwajibkan mengembalikan atau melaporkan perangkat teknologi informasi kepada Fungsi Teknologi Informasi sebagai bagian dari kepatuhan terhadap kebijakan perusahaan.
7. Melaporkan secara segera setiap insiden, gangguan sistem, atau dugaan pelanggaran keamanan sesuai dengan regulasi yang berlaku.
8. Tidak menyalahgunakan data perusahaan, termasuk data pribadi, untuk kepentingan pribadi maupun pihak ketiga.

Pasal 31
Tanggung Jawab Hukum

1. Setiap pelanggaran terhadap kewajiban pengguna yang mengakibatkan kerugian perusahaan, gangguan operasional, atau kebocoran data dikenakan sanksi sesuai dengan peraturan internal dan ketentuan perundang-undangan yang berlaku
2. Pelanggaran yang melibatkan data pribadi dapat dikenakan sanksi administratif, perdata, atau pidana sebagaimana diatur dalam UU PDP.
3. Direksi berwenang menetapkan sanksi disiplin berdasarkan tingkat keparahan pelanggaran, yang dapat berupa teguran tertulis, penundaan promosi, hingga pemutusan hubungan kerja.

/**BAB XI**.....

BAB XI
PENUTUP
Pasal 32
Penutup

1. Surat Keputusan ini berlaku sejak tanggal ditetapkan, dengan ketentuan apabila dikemudian hari terdapat kekeliruan dan/atau perlu dilakukan perubahan di dalamnya maka akan diadakan perbaikan sebagaimana mestinya.
2. Dengan ditetapkan Surat Keputusan ini maka Surat Keputusan Direksi PT Pindad nomor: SKEP/10/P/BD/VII/2021 tanggal 12 Juli 2021 tentang Kebijakan Teknologi Informasi di Lingkungan Perusaaan dicabut dan dinyatakan tidak berlaku.

Ditetapkan di : Bandung
Pada tanggal : 9 Oktober 2025

PT PINDAD
DIREKSI

SIGIT PUJI SANTOSA
DIREKTUR UTAMA

Kepada Yth.:
1. Direksi
2. *Senior Vice President*
3. Sekretaris Perusahaan
4. Kepala SPI
5. Para *Vice President*
6. Para *General Manager*
7. *Senior Principal Expert*