# SURAT - KEPUTUSAN

**Nomor : SKEP / 45 /P/BD/ III / 2017**

Tentang

## KEBIJAKAN MANAJEMEN KEAMANAN INFORMASI

---

**DIREKSI PT PINDAD (PERSERO)**

Menimbang :

1. Bahwa dalam rangka mendukung penerapan tata kelola teknologi informasi di lingkungan PT. Pindad (Persero);
2. Bahwa dalam rangka melindungi kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability) aset informasi Perusahaan dari ancaman (threat) dan kerentanan (vulnerability), baik dari dalam maupun dari luar lingkungan Perusahaan yang dapat mengganggu kelangsungan bisnis Perusahaan;
3. Bahwa berdasarkan pertimbangan sebagaimana dimaksud butir 1 dan 2 di atas, maka dipandang perlu menetapkan Keputusan Direksi tentang Kebijakan Manajemen Keamanan Informasi di Lingkungan PT. Pindad (Persero).

Mengingat

1. Surat Keputusan Direksi PT. Pindad (Persero) Nomor: Skep/35/P/BD/IX/2014 30 Juni 2014 tentang Pedoman Penerapan Good Corporate Governance (GCG) Di Lingkungan PT.pindad (Persero);
2. Surat Keputusan Direksi PT. Pindad (Persero) nomor : Skep/2/P/BD/II/2017 tanggal 10 Februari 2017 tentang Organisasi dan Tata Kerja PT. Pindad (Persero).
3. Surat Keputusan Direksi PT. Pindad (Persero) nomor : Skep/2/P/BD/IX/2011 tanggal 8 September 2011 tentang Kebijakan Teknologi Informasi PT. Pindad (Persero);
4. Surat Keputusan Direksi PT. Pindad (Persero) nomor : Skep/29/P/BD/XII/2015 tanggal 23 Desember 2015 tentang Kebijakan Penerapan Tata Kelola Teknologi Informasi PT. Pindad (Persero).

/**MEMUTUSKAN**.....

**Head Office**
Jl. GatotSubroto No. 517
Bandung 40284
Indonesia
P +62 22 7312073
F +62 22 7301222
E info@pindad.com

**Representative Office**
Jl. BatuCeper No. 28
Jakarta 10120
Indonesia
P +62 21 3806929
F +62 21 3814039
E pindadjkt@pindad.com

www.pindad.com

**MEMUTUSKAN**

Menetapkan : Keputusan Direksi PT Pindad (Persero) tentang Kebijakan Manajemen Keamanan Informasi di lingkungan PT. Pindad (Persero) sebagai berikut:

1. Penerapan manajemen keamanan informasi merupakan tanggungjawab operasional seluruh manajemen PT. Pindad (Persero) di semua tingkatan.

2. Manajemen keamanan informasi mencakup segala bentuk prosedur dan metoda untuk melindungi seluruh sumber daya informasi Perusahaan dari kerusakan, kerentanan dan ancaman yang dapat mengganggu proses bisnis Perusahaan, meliputi:
   a. Organisasi dan lokasi, yaitu seluruh unit kerja dan lokasi kerja yang digunakan untuk mengelola dan menyediakan layanan internal dan eksternal.
   b. Aset informasi, yaitu:
      1) Data/ Informasi, meliputi seluruh informasi yang disimpan dalam media simpan, ditulis, dicetak, dan dikomunikasikan langsung atau melalui teknologi komunikasi, antara lain; rencana strategis Perusahaan, data karyawan, data enjinering & data produk, dokumen teknis, dokumen manajemen, dokumen keuangan dan dokumen audit.
      2) *Software*, meliputi *software* aplikasi, *operating system*, *development tool*, dan *Software tool* (antivirus, *audit tool*).
      3) *Hardware*, meliputi Server, PC, Laptop, Media penyimpan data, perangkat jaringan komunikasi dan fasilitas pendukungnya.
      4) Sumber Daya Manusia; meliputi karyawan tetap, calon karyawan tetap, karyawan kontrak, mitra, vendor dan pihak ketiga lainnya yang menyediakan layanan, jasa, serta produk yang menunjang bisnis Perusahaan.

3. Penerapan manajemen keamanan informasi dimaksudkan untuk memenuhi prinsip-prinsip keamanan informasi sebagai berikut:
   a. Ketersediaan (*availability*), yaitu informasi dan layanan harus tersedia atau dapat diakses oleh pengguna yang berwenang saat diperlukan.
   b. Kerahasiaan (*confidentiality*), yaitu data hanya boleh diakses oleh orang yang berhak untuk melihat dan hanya dapat diubah oleh orang-orang yang diperbolehkan untuk mengubahnya.
   c. Keutuhan (*integrity*), yaitu data lengkap, akurat, terkini, jelas sumbernya dan relevan serta sistem beroperasi sesuai dengan spesifikasi yang ditetapkan.

/4. Manajemen.....

4. Manajemen keamanan informasi berdasarkan pada penilaian risiko yang dapat dilakukan pada setiap entitas dalam lingkungan perusahaan atau pada entitas luar yang telah menandatangani perjanjian secara tertulis dengan Perusahaan.
5. Entitas dalam lingkungan perusahaan atau pada entitas luar sebagaimana dimaksud ayat 4 di atas dapat dilakukan pada berbagai sistem informasi beserta setiap proses atau prosedur yang digunakan.
6. Kebijakan manajemen keamanan informasi harus dikomunikasikan ke seluruh karyawan dan pihak ketiga terkait, termasuk: *vendor*, konsultan & mitra melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi.
7. Seluruh Divisi atau lokasi kerja perlu meningkatkan kesadaran (awareness), kepedulian, pengetahuan dan keterampilan tentang keamanan informasi.
8. Seluruh kelemahan keamanan informasi yang berpotensi atau telah mengakibatkan gangguan bisnis (business interuption), harus segera dilaporkan ke penanggung jawab terkait.
9. Seluruh karyawan bertanggung jawab untuk menjaga dan melindungi keamanan aset informasi serta mematuhi kebijakan dan prosedur keamanan informasi yang telah ditetapkan.
10. Setiap pelanggaran terhadap kebijakan ini dapat dikenai sangsi atau tindakan disiplin sesuai peraturan yang berlaku.
11. Kebijakan teknis yang diperlukan dalam rangka penerapan manajemen keamanan informasi akan diatur lebih lanjut dalam bentuk pedoman dan/atau prosedur yang ditetapkan dalam Surat Keputusan Direksi tersendiri.

/12. Surat.....

12. Surat keputusan ini berlaku terhitung mulai tanggal ditetapkan.

Ditetapkan di : B a n d u n g
Pada tanggal : 31 Maret 2017

**PT PINDAD (PERSERO)**
**DIREKSI**

**ABRAHAM MOSE**
**DIREKTUR UTAMA**

Kepada Yth.:
1. Direksi
2. Para VP dan GM
3. Para Ahli Utama
4. Para PMO
5. Ka. SPI
6. Sekretaris Perusahaan