# Rekayasa Pertahanan Ciber

Drs. Afrizal Zein M. Kom

# Rekayasa Pertahanan Ciber


## Drs. Afrizal Zein M.Kom


Drs. Afrizal Zein M.Kom Lahir di Jakarta 13 Juli 1965 merupakan dosen tetap di Universitas Pamulang. Telah menamatkan S1 di Universitas Padjadjaran dan Lulus S2 di STMIK ERESHA pada tahun 2014 dengan predikat Cumlaude. Berpengalaman sebagai programmer diberbagai project dan membangun Aplikasi Komputer selama 25 tahun bekerja di Konsultan Komputer. Memiliki sertifikasi dalam bidang Pemograman dan Sistem Analis.


eureka media aksara
Anggota IKAPI
No. 225/JTE/2021

0858 5343 1992
eurekamediaaksara@gmail.com
Jl. Banjaran RT.20 RW.10
Bojongsari - Purbalingga 53362

DIREKTORAT JENDERAL KEKAYAAN INTELEKTUAL
KEMENTERIAN HUKUM & HAK ASASI MANUSIA R.I.
EC00202438317

ISBN 978-623-120-659-6

# REKAYASA PERTAHANAN CIBER

**Drs. Afrizal Zein M.Kom**

**PENERBIT CV. EUREKA MEDIA AKSARA**

**REKAYASA PERTAHANAN CIBER**

**Penulis** : Drs. Afrizal Zein M.Kom

**Desain Sampul** : Ardyan Arya Hayuwaskita

**Tata Letak** : Nur Aisah

**ISBN** : 978-623-120-659-6

**No. HKI** : EC00202438317

Diterbitkan oleh : **EUREKA MEDIA AKSARA, MEI 2024**
**ANGGOTA IKAPI JAWA TENGAH**
**NO. 225/JTE/2021**

**Redaksi:**
Jalan Banjaran, Desa Banjaran RT 20 RW 10 Kecamatan Bojongsari Kabupaten Purbalingga Telp. 0858-5343-1992

Surel : eurekamediaaksara@gmail.com

Cetakan Pertama : 2024

## KATA PENGANTAR

Puji Syukur penulis panjatkan kehadirat Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya sehingga penulisan buku "Rekayasa Pertahanan Ciber" dapat diselesaikan dengan baik dan tepat waktu.

Dengan penuh kebanggaan, kami dengan rendah hati mempersembahkan buku ini kepada para pembaca yang terhormat. Buku ini mengupas secara komprehensif mengenai upaya pertahanan siber yang berguna bagi para pembaca.

Adapun buku ini terdiri dari sebelas bab, yaitu bab 1 tentang rekayasa pertahanan ciber, bab 2 tentang analisis keamanan sistem informasi, bab 3 tentang vulmerabilitas jaringan, bab 4 tentang manajemen bencana, bab 5 tentang virus dan malware, bab 6 tentang sistem pencegahan intruisi, bab 7 tentang keamanan IoT dan komputasi awan, bab 8 tentang tata kelola keamanan sistem informasi, bab 9 tentang ancaman ciber dan resiko sistem informasi, bab 10 tentang model keamanan cloud computing, dan bab 11 tentang model keamanan mobile.

Penulis mengucapkan banyak terima kasih pada semua pihak yang telah membantu penyusunan buku ini. Sehingga buku ini bisa hadir di hadapan pembaca.

Penulis mengharapkan kritik dan saran pembaca demi kesempurnaan buku ini kedepannya. Akhir kata penulis mengucapkan terima kasih, mudah-mudahan buku ini bermanfaat bagi para pembaca.

Semoga buku ini mampu menjadi tonggak baru dalam memperkaya pengetahuan dan pemahaman para pembaca mengenai pertahanan siber di era yang serba digital ini.

Salam,

[Penulis]

## DAFTAR ISI

REKAYASA PERTAHANAN CIBER

Drs. Afrizal Zein M.Kom

# BAB 1 REKAYASA PERTAHANAN CIBER

## A. Pendahuluan

Dalam era digital yang semakin maju, rekayasa pertahanan ciber menjadi salah satu aspek yang sangat penting dalam memastikan keamanan dan kestabilan sistem informasi dan komunikasi. Perkembangan teknologi informasi dan komunikasi (TIK) telah membawa kemudahan dalam berbagai aspek kehidupan manusia, mulai dari komunikasi, bisnis, hingga pemerintahan. Namun, bersamaan dengan kemajuan tersebut, muncul pula ancaman-ancaman baru yang berkaitan dengan keamanan data dan informasi. Ancaman tersebut dapat datang dalam berbagai bentuk, seperti serangan malware, phishing, hacking, dan berbagai tindakan kriminal digital lainnya.

Dalam konteks ini, rekayasa pertahanan ciber menjadi sebuah disiplin yang penting untuk mengatasi ancaman-ancaman tersebut. Rekayasa pertahanan ciber melibatkan pengembangan strategi, kebijakan, dan teknologi untuk melindungi sistem informasi dan komunikasi dari serangan digital. Tujuan utamanya adalah untuk mencegah, mendeteksi, dan merespons ancaman-ancaman keamanan yang mungkin terjadi dalam lingkungan digital. jadi mari kita teruskan dengan memfokuskan pada pemahaman yang lebih dalam tentang apa itu rekayasa pertahanan ciber, mengapa hal itu penting, dan bagaimana hal itu berkembang dalam beberapa tahun terakhir.

# BAB 2 ANALISIS KEAMANAN SISTEM INFORMASI

## A. Pendahuluan

Keamanan sistem informasi merupakan salah satu aspek yang krusial dalam era digital saat ini. Dengan perkembangan teknologi informasi yang pesat, data dan informasi menjadi aset berharga yang harus dilindungi dengan baik. Ancaman terhadap keamanan sistem informasi dapat berasal dari berbagai sumber, mulai dari serangan siber yang kompleks hingga kesalahan manusia yang tidak disengaja. Oleh karena itu, analisis keamanan sistem informasi menjadi sangat penting dalam upaya untuk mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan yang mungkin timbul. Dalam pendahuluan ini, kita akan membahas tentang pentingnya analisis keamanan sistem informasi, konsep dasar yang terlibat dalam analisis keamanan, serta perkembangan terkini dalam domain ini.

### 1. Pentingnya Analisis Keamanan Sistem Informasi

Keamanan sistem informasi memiliki peran yang sangat penting dalam mengamankan data dan informasi dalam suatu organisasi. Beberapa alasan mengapa analisis keamanan sistem informasi sangat penting adalah sebagai berikut:

a. Perlindungan Data Sensitif: Data dan informasi yang disimpan dalam sistem informasi seringkali termasuk informasi sensitif, seperti informasi keuangan, data pelanggan, atau rahasia perusahaan. Analisis keamanan sistem informasi membantu dalam mengidentifikasi dan

# BAB 3 VURMERABILITAS JARINGAN

## A. Memahami Vulnerabilitas Jaringan dalam Keamanan Cyber

Dalam ekosistem digital yang terus berkembang, ancaman siber semakin kompleks dan sering kali berdampak besar pada organisasi dan individu. Salah satu faktor yang memperbesar risiko keamanan adalah vulnerabilitas jaringan, yang merupakan celah atau kelemahan dalam infrastruktur IT yang dapat dieksploitasi oleh penyerang untuk mendapatkan akses yang tidak sah atau merusak sistem. Dalam pendahuluan ini, kita akan menjelajahi konsep dasar vulnerabilitas jaringan, peran pentingnya dalam keamanan cyber, serta strategi untuk mengidentifikasi dan mengatasi vulnerabilitas tersebut.

### Konsep Dasar Vulnerabilitas Jaringan

Vulnerabilitas jaringan merujuk pada celah atau kelemahan dalam infrastruktur IT suatu organisasi yang dapat dieksploitasi oleh penyerang untuk melakukan serangan yang merugikan. Celah ini dapat muncul dalam berbagai bentuk, termasuk kelemahan perangkat lunak, konfigurasi yang tidak aman, atau kesalahan manusia. Penyerang dapat menggunakan vulnerabilitas ini untuk melakukan berbagai jenis serangan, mulai dari pencurian data hingga merusak sistem.

### Peran Penting Vulnerabilitas Jaringan dalam Keamanan Cyber

Vulnerabilitas jaringan memainkan peran penting dalam keamanan cyber dengan beberapa cara:

1. Menyediakan Pintu Masuk bagi Penyerang: Vulnerabilitas jaringan memberikan pintu masuk bagi penyerang untuk

# BAB 4 MANAJEMEN BENCANA

## A. Mengelola Bencana

Bencana alam dan insiden darurat dapat terjadi tanpa pemberitahuan dan menyebabkan dampak yang merusak bagi masyarakat, lingkungan, dan ekonomi. Untuk mengurangi kerugian yang ditimbulkan oleh bencana dan meningkatkan kemampuan dalam menghadapinya, konsep pengelolaan bencana menjadi semakin penting. Dalam pendahuluan ini, kita akan mengeksplorasi makna dan urgensi pengelolaan bencana, serta peran pentingnya dalam membangun kesiapsiagaan, mengurangi risiko, dan memperkuat ketahanan komunitas.

### 1. Makna Pengelolaan Bencana

Pengelolaan bencana merujuk pada rangkaian kegiatan yang direncanakan dan terkoordinasi untuk mengurangi risiko, mengelola dampak, dan memulihkan keadaan pasca-bencana. Ini melibatkan berbagai tahapan, mulai dari pencegahan dan mitigasi hingga tanggap darurat dan pemulihan. Tujuannya adalah untuk melindungi nyawa, harta benda, dan sumber daya manusia, serta meminimalkan kerugian yang disebabkan oleh bencana.

### 2. Urgensi Pengelolaan Bencana

Pentingnya pengelolaan bencana semakin dipahami dengan meningkatnya frekuensi dan intensitas bencana di seluruh dunia. Perubahan iklim, urbanisasi yang cepat, dan ketidakstabilan politik merupakan beberapa faktor yang menyebabkan meningkatnya risiko bencana. Dengan pengelolaan bencana yang efektif, kita dapat mengurangi

# BAB 5 VIRUSES AND MALWARE

## A. Pendahuluan

Dalam era digital yang semakin maju, ancaman siber seperti virus dan malware telah menjadi salah satu masalah terbesar dalam keamanan cyber. Virus dan malware merupakan perangkat lunak berbahaya yang dirancang untuk merusak, mencuri data, atau mengganggu fungsi normal sistem komputer. Dalam makalah ini, kita akan mengeksplorasi konsep dasar virus dan malware, jenis-jenis yang ada, dampaknya terhadap keamanan cyber, serta strategi untuk melindungi diri dari ancaman ini.

### 1. Konsep Dasar Virus dan Malware

a. Virus: Virus adalah program komputer berbahaya yang dapat menyebar dan menempel pada file atau program lainnya. Virus biasanya merusak sistem atau menyebabkan gangguan, dan dapat menyebar melalui jaringan, email, atau perangkat penyimpanan yang terinfeksi.

b. Malware: Malware adalah istilah umum yang digunakan untuk merujuk kepada berbagai jenis perangkat lunak berbahaya, termasuk virus, worm, trojan, ransomware, dan spyware. Malware dapat melakukan berbagai macam tindakan berbahaya, mulai dari mencuri informasi hingga merusak sistem.

# BAB 6 SISTEM PENCEGAHAN INTRUSI

## A. Apa Itu Sistem Pencegahan Intrusi

Dalam era digital yang semakin maju, keamanan sistem dan jaringan menjadi semakin penting bagi organisasi dan individu. Ancaman intrusi sistem, baik dari luar maupun dari dalam, dapat menyebabkan kerugian yang signifikan, termasuk kehilangan data, pencurian informasi sensitif, dan gangguan operasional. Dalam makalah ini, kita akan membahas strategi pencegahan intrusi sistem, termasuk definisi, jenis-jenis, pentingnya, serta langkah-langkah yang dapat diambil untuk melindungi sistem dari ancaman intrusi.

### 1. Definisi dan Jenis Intrusi Sistem

- Definisi Intrusi Sistem: Intrusi sistem merujuk kepada upaya tidak sah untuk memasuki, merusak, atau mengganggu sistem komputer atau jaringan. Ini dapat dilakukan oleh penyerang dari luar (serangan eksternal) atau oleh anggota internal organisasi yang tidak sah (serangan internal).
- Jenis Intrusi Sistem: Intrusi sistem dapat dibagi menjadi beberapa jenis, termasuk:
- Serangan Malware: Serangan malware seperti virus, worm, trojan, dan ransomware dapat digunakan untuk mencuri data, merusak sistem, atau memberikan akses ke sistem kepada penyerang.
- Serangan Denial of Service (DoS): Serangan DoS bertujuan untuk mengganggu layanan atau sumber daya sistem dengan mengirimkan volume lalu lintas yang sangat

# BAB 7 KEAMANAN IoT DAN KOMPUTASI AWAN

## A. Pendahuluan

Internet of Things (IoT) merujuk pada jaringan perangkat fisik yang terhubung ke internet, yang mampu saling berkomunikasi dan bertukar data tanpa interaksi manusia. IoT mencakup berbagai jenis perangkat, termasuk sensor, kamera, kendaraan, perangkat rumah tangga pintar, peralatan industri, dan banyak lagi. Konsep ini telah membawa revolusi dalam berbagai bidang, mulai dari rumah pintar hingga kota pintar, dan dari manufaktur hingga kesehatan.

**1. Fitur Utama IoT:**

- Konektivitas: Perangkat IoT terhubung ke internet melalui berbagai teknologi, termasuk Wi-Fi, Bluetooth, Zigbee, dan LTE, memungkinkannya untuk berkomunikasi dan bertukar data secara real-time.
- Sensors and Data Collection: Perangkat IoT dilengkapi dengan berbagai jenis sensor yang memungkinkannya untuk mendeteksi lingkungan sekitarnya, seperti suhu, kelembaban, cahaya, gerakan, dan banyak lagi. Data yang dikumpulkan oleh sensor ini digunakan untuk analisis dan pengambilan keputusan.
- Interkoneksi dan Interoperabilitas: IoT memungkinkan perangkat dari berbagai vendor dan platform untuk saling berinteraksi dan berintegrasi, menciptakan ekosistem yang terhubung dan terpusat.

# BAB 8 TATA KELOLA KEAMANAN SISTEM INFORMASI

## A. Pengertian TKSI

Tata Kelola Keamanan Sistem Informasi (TKSI) adalah pendekatan sistematis dalam mengelola dan melindungi keamanan informasi suatu organisasi. Konsep TKSI melibatkan perencanaan, pengimplementasian, pengawasan, dan penilaian berkelanjutan terhadap kebijakan, prosedur, dan kontrol keamanan untuk mengurangi risiko keamanan, melindungi data sensitif, dan memastikan kelangsungan bisnis. TKSI membantu organisasi untuk mengelola dan mengurangi risiko terhadap ancaman keamanan seperti serangan cyber, pencurian data, atau kehilangan informasi penting.

Secara lebih rinci, TKSI mencakup berbagai aspek, termasuk:

1. **Kebijakan Keamanan:** Pengembangan, penerapan, dan pemantauan kebijakan keamanan informasi yang mencakup pengaturan akses, penggunaan sandi yang aman, pengelolaan identitas, dan pengendalian keamanan lainnya.
2. **Manajemen Risiko:** Identifikasi, evaluasi, dan mitigasi risiko keamanan yang mungkin terjadi, termasuk analisis risiko, penentuan prioritas, dan implementasi kontrol keamanan yang sesuai.
3. **Kepatuhan dan Regulasi:** Memastikan bahwa organisasi mematuhi semua peraturan hukum dan regulasi terkait dengan keamanan informasi, seperti GDPR, HIPAA, PCI DSS, dan lainnya.

# BAB 9

# ANCAMAN CIBER DAN RESIKO SISTEM INFORMASI

## A. Ancaman Ciber

Di era digital yang terus berkembang, ancaman siber menjadi salah satu tantangan terbesar dalam menjaga keamanan informasi dan infrastruktur teknologi. Ancaman-ancaman ini tidak hanya mengancam individu dan perusahaan, tetapi juga lembaga pemerintah dan infrastruktur kritis. Dalam makalah ini, kita akan menjelajahi berbagai jenis ancaman siber, dampaknya, serta strategi untuk mengatasi dan mencegahnya.

**Jenis Ancaman Siber**

1. **Malware:** Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak atau mencuri data dari sistem komputer. Ini termasuk virus, worm, trojan, ransomware, dan spyware.
2. **Serangan Phishing:** Phishing adalah teknik manipulasi yang digunakan oleh penyerang untuk mendapatkan informasi sensitif dari korban dengan menyamar sebagai entitas tepercaya melalui email, pesan teks, atau media sosial.
3. **Serangan Denial-of-Service (DoS):** Serangan DoS bertujuan untuk membuat layanan atau sumber daya tidak tersedia bagi pengguna yang sah dengan membanjiri jaringan atau server dengan lalu lintas palsu.
4. **Serangan Man-in-the-Middle (MITM):** Dalam serangan MITM, penyerang mencuri atau memanipulasi komunikasi antara dua pihak yang sah tanpa diketahui oleh keduanya.

# BAB 10 MODEL KEAMANAN CLOUD COMPUTING

## A. Pendahuluan

Komputasi awan (cloud computing) telah menjadi fondasi bagi banyak organisasi dalam menyimpan, mengelola, dan mengakses data mereka secara efisien dan efektif. Namun, dengan keuntungan yang ditawarkan oleh komputasi awan juga datang tantangan keamanan yang unik. Dalam makalah ini, kita akan menjelajahi model keamanan dalam komputasi awan, strategi untuk melindungi data, dan kerangka kerja untuk mengelola risiko keamanan dalam lingkungan yang terdistribusi.

**Pentingnya Keamanan dalam Komputasi Awan**

1. Perlindungan Data: Keamanan adalah prioritas utama dalam komputasi awan untuk melindungi data sensitif dari akses yang tidak sah, perubahan tidak sah, atau kebocoran.
2. Kepercayaan Pelanggan: Keamanan yang kuat dalam komputasi awan membantu membangun kepercayaan pelanggan dan memastikan bahwa data mereka aman dan terlindungi.
3. Kepatuhan Hukum: Mematuhi regulasi keamanan data, seperti GDPR atau HIPAA, menjadi lebih mudah dengan menerapkan model keamanan yang sesuai dalam komputasi awan.
4. Kontinuitas Bisnis: Mengelola risiko keamanan dalam komputasi awan membantu organisasi dalam merencanakan pemulihan bencana dan memastikan kelangsungan operasi bisnis dalam situasi darurat.

# BAB 11 MODEL KEAMANAN MOBILE

## A. Keamanan Mobile

Dalam era yang semakin terhubung dan mobile, perangkat seluler telah menjadi bagian penting dari kehidupan sehari-hari. Namun, dengan pertumbuhan penggunaan perangkat mobile juga datang tantangan keamanan yang signifikan. Dalam makalah ini, kita akan membahas model keamanan mobile, strategi untuk melindungi data dan privasi pengguna, serta pentingnya kesadaran keamanan dalam penggunaan perangkat mobile.

**Pentingnya Keamanan Mobile**

1. Data Sensitif: Pengguna perangkat mobile sering menyimpan data sensitif seperti informasi pribadi, kata sandi, dan data keuangan di perangkat mereka. Perlindungan data ini sangat penting untuk mencegah akses yang tidak sah.
2. Privasi Pengguna: Pengguna perangkat mobile memiliki hak atas privasi mereka. Melindungi privasi pengguna melibatkan pencegahan akses yang tidak sah terhadap data pribadi dan lokasi mereka.
3. Keamanan Transaksi: Perangkat mobile sering digunakan untuk transaksi keuangan, belanja online, dan aktivitas penting lainnya. Perlindungan terhadap transaksi ini penting untuk mencegah penipuan dan pencurian identitas.
4. Keamanan Perusahaan: Banyak organisasi mengizinkan akses perangkat mobile ke jaringan perusahaan dan data sensitif. Model keamanan mobile yang kuat diperlukan

## DAFTAR PUSTAKA


Infantono, J. Budiarto, A. Persada, F. Azzuhri, and Z.Abidin, "Content Filtering PornografiHalaman Web Berbasis Citra dan Teks pada Sistem Terintegrasi ServerInternet", AAU-JDST,vol. 5, no. 2, pp. 125-132, Jan.2021

Anne W. Brascomb (ed), Toward A Law of Global Communication Network, New York: Lognman,1986.

Ardiyanti, Handrini. 2014. "Cyber-Security dan Tantangan Pengembangannya di Indonesia". Jurnal Politica. Vol. 5. No. 1 . Juni.

Arianto, Adi Rio. 2017. "Cyber Security: Geometripolitika dan Dimensi Pembangunan KeamananDunia Era Horizontal Abad21". Jurnal Power In International Relations. Universitas PotensiUtama. Vol. 1. No.2. Februari.

B.L. Berg, H. Lune, Qualitative Research methods for The Social Sciences, ninth edition, (England,Essex: Pearson Education Limited, 2017).

Badri, Muhammad. 2011. Perang cyber dalam dinamika komunikasi internasional dalam buku Komunikasi militer, Aspikom.

Barrinha A, Renard T."Cyber-diplomacy: the making of an International society in the digitalage". Global Affairs, (2017)

Brascomb, Anne W. 1986. Toward A Law of Global Communication Network. USA: Longman.Buzan, Barry. 1998. Security: A Framework for Analysis. Boulder: Lynne Reinner Publishers.

Bilah and A. Infantono, "Pengembangan Aplikasi Mobile Kamus Istilah Aeronautika padaPlatform Android Sesuai StandarISO 25010", senastindo, vol. 1, pp. 195-202, Oct. 2021.

Chintia, E. dkk. 2019. Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia danPenanganannya. Journal of Information Engineering and Educational Technology.

Ghernaouti, Solange. 2013. Cyber Power: Crime, Conflict and Security in Cyberspace. Lausanne:EPFL Press.Igwe, K., & Ibegwam, A. 2014.

Imperative of Cyber Ethics Education to Cyber Crimes Preventionand Cyber Security in Nigeria. International Journal of ICT and Management II

## TENTANG PENULIS

**Drs. Afrizal Zein M.Kom** Lahir di Jakarta 13 Juli 1965 merupakan dosen tetap di Universitas Pamulang. Telah menamatkan S1 di Universitas Padjadjaran dan Lulus S2 di STMIK ERESHA pada tahun 2014 dengan predikat Cumlaude. Berpengalaman sebagai programmer diberbagai project dan membangun Aplikasi Komputer selama 25 tahun bekerja di Konsultan Komputer. Memiliki sertifikasi dalam bidang Pemograman dan Sistem Analis.

REPUBLIK INDONESIA
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA

# SURAT PENCATATAN CIPTAAN

Dalam rangka pelindungan ciptaan di bidang ilmu pengetahuan, seni dan sastra berdasarkan Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta, dengan ini menerangkan:

| | | |
|---|---|---|
| Nomor dan tanggal permohonan | : | EC00202438317, 15 Mei 2024 |
| **Pencipta** | | |
| Nama | : | **Drs. Afrizal Zein, M.Kom** |
| Alamat | : | Griya Bukit Jaya Blok F8 No. 79 RT 03/26 Gunung Putri Kabupaten Bogor, Gunung Putri, Bogor, Jawa Barat, - |
| Kewarganegaraan | : | Indonesia |
| **Pemegang Hak Cipta** | | |
| Nama | : | **Drs. Afrizal Zein, M.Kom** |
| Alamat | : | Griya Bukit Jaya Blok F8 No. 79 RT 03/26 Gunung Putri Kabupaten Bogor, Gunung Putri, Bogor, Jawa Barat - |
| Kewarganegaraan | : | Indonesia |
| Jenis Ciptaan | : | **Buku** |
| Judul Ciptaan | : | **Rekayasa Pertahanan Ciber** |
| Tanggal dan tempat diumumkan untuk pertama kali di wilayah Indonesia atau di luar wilayah Indonesia | : | 4 Mei 2024, di Purbalingga |
| Jangka waktu pelindungan | : | Berlaku selama hidup Pencipta dan terus berlangsung selama 70 (tujuh puluh) tahun setelah Pencipta meninggal dunia, terhitung mulai tanggal 1 Januari tahun berikutnya. |
| Nomor pencatatan | : | 000613673 |

adalah benar berdasarkan keterangan yang diberikan oleh Pemohon.
Surat Pencatatan Hak Cipta atau produk Hak terkait ini sesuai dengan Pasal 72 Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta.

a.n. MENTERI HUKUM DAN HAK ASASI MANUSIA
DIREKTUR JENDERAL KEKAYAAN INTELEKTUAL
u.b
Direktur Hak Cipta dan Desain Industri

IGNATIUS M.T. SILALAHI
NIP. 196812301996031001

Disclaimer:
Dalam hal pemohon memberikan keterangan tidak sesuai dengan surat pernyataan, Menteri berwenang untuk mencabut surat pencatatan permohonan.