Tentang MSIG Indonesia

PT Asuransi MSIG Indonesia (MSIG Indonesia) merupakan salah satu perusahaan asuransi umum terkemuka di Indonesia yang berkomitmen menyediakan solusi asuransi yang komprehensif dan inovatif bagi individu maupun korporasi. Sejak berdiri pada tahun 1975, MSIG Indonesia telah membangun reputasi sebagai perusahaan dengan ketangguhan finansial, keandalan, serta layanan yang berorientasi pada nasabah.

Perusahaan menawarkan portofolio produk asuransi yang luas, didukung oleh keahlian manajemen risiko dan kapabilitas digital untuk memberikan ketenangan bagi nasabah. MSIG Indonesia merupakan bagian dari MS&AD Insurance Group Holdings Inc., salah satu grup asuransi umum terbesar di dunia dengan peringkat kredit yang kuat, serta didukung oleh Mitsui Sumitomo Insurance Company Limited.

PT Asuransi MSIG Indonesia
Gedung Summitmas 2, Lantai 15
Jl. Jenderal Sudirman Kav. 61 - 62
Jakarta 12190, Indonesia

Telepon : (021) 252 3110 (*Hunting*)
Fax : (021) 252 6761 (*General*)
Pusat Layanan : 1500 674 (MSI)
WhatsApp : +62 811 1974 5674
Email : msig@id.msig-asia.com
URL : www.msig.co.id

Scan QR code untuk informasi lengkap mengenai produk

msigid
msig_id
msig_id
MSIG Indonesia

PT Asuransi MSIG Indonesia Berizin dan Diawasi oleh Otoritas Jasa Keuangan.

KONTAK LAYANAN PENGADUAN

Telepon : (021) 2523110 (*Hunting*)
Email : customer@id.msig-asia.com

KANTOR CABANG DAN PERWAKILAN

Bandung	Telp. (022) 3000 0851 | 3000 0852 | idn_bandung@id.msig-asia.com
Batam	Telp. (0778) 550 8203 | 550 9225 | idn_batam@id.msig-asia.com
Denpasar	Telp. (0361) 471 7227 | 471 7228 | idn_denpasar@id.msig-asia.com
Medan	Telp. (061) 452 8783 | 452 8795 | idn_medan@id.msig-asia.com
Palembang	Telp. (0711) 563 0711 | 563 0712 | idn_palembang@id.msig-asia.com
Semarang	Telp. (024) 841 7010 | 841 7013 | idn_semarang@id.msig-asia.com
Surabaya	Telp. (031) 531 8876 | 531 8496 | idn_surabaya@id.msig-asia.com

Brosur ini hanya memuat informasi umum mengenai Asuransi *Cyber* MSIG dan bukan merupakan kontrak/perjanjian asuransi. Rincian mengenai kondisi pertanggungan dan pengecualiannya dituangkan di dalam Polis. Tertanggung wajib membaca dan memahami Polis.

IPB-V55-E5-2026-06

ASURANSI *CYBER* MSIG

Perlindungan Daring untuk Kenyamanan Bisnis Anda



MSIG

PROTECTING GOALS POWERING FUTURES

A Member of MS&AD INSURANCE GROUP

PAHAMI & MILIKI ASURANSI

Asuransi *Cyber* MSIG

Perlindungan Daring untuk Kenyamanan Bisnis Anda

Memberikan ganti rugi kepada Anda atau membayar atas nama Anda di atas risiko sendiri yang berlaku atas:

1. Biaya investigasi
2. Biaya respons
3. Biaya pemulihan
4. Gangguan usaha
5. Tanggung gugat
6. Kerugian akibat pemerasan
7. Regulasi

yang timbul karena pelanggaran kerahasiaan, pelanggaran privasi atau pelanggaran keamanan

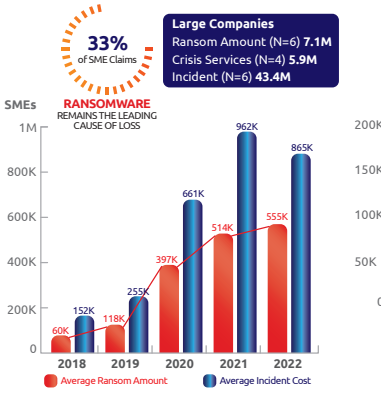
Kami akan menyediakan jaminan sesuai yang tertera di dalam Polis selama periode Polis sesuai ketentuan dan kondisi yang berlaku.

Mengapa kita membutuhkan Asuransi Siber?

Tren keamanan siber di Indonesia telah berkembang pesat seiring dengan pertumbuhan lanskap digital negara ini.

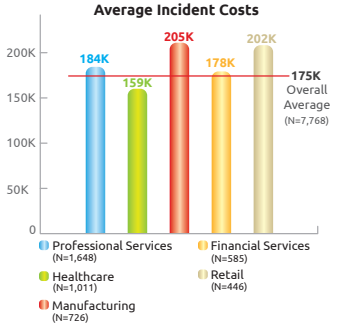
- **Peningkatan Serangan Siber:** Indonesia telah mengalami peningkatan serangan siber, termasuk *ransomware, phishing,* dan pelanggaran data. Seiring dengan semakin banyaknya bisnis dan individu yang menggunakan internet, peluang bagi kejahatan siber pun semakin besar.
- **Ancaman *Ransomware:*** Serangan *ransomware* semakin sering terjadi dan semakin canggih. Serangan ini sering kali menargetkan infrastruktur penting dan organisasi besar, yang menuntut tebusan besar untuk pemulihan data.
- ***Phishing* dan Rekayasa Sosial:** Serangan *phishing,* termasuk *spear-phishing,* telah menjadi tren. Penjahat dunia maya menggunakan taktik ini untuk mengelabui individu dan organisasi agar mengungkapkan informasi sensitif.
- **Masalah Privasi Data:** Dengan adanya peraturan baru seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) yang disahkan pada tahun 2022, perlindungan data menjadi semakin penting. Namun, masih ada tantangan dalam menerapkan dan menegakkan peraturan ini secara efektif.
- **Kesadaran dan Pelatihan Publik:** Ada peningkatan fokus pada peningkatan kesadaran dan pelatihan keamanan siber di kalangan individu dan organisasi untuk pertahanan yang lebih baik terhadap ancaman siber.
- **Ancaman yang Muncul:** Meningkatnya penggunaan perangkat *Internet of Things (IoT)* dan *cloud computing* menimbulkan kerentanan baru. Penjahat dunia maya semakin gencar menargetkan area ini untuk mengeksploitasi langkah-langkah keamanan yang lemah.
- **Biaya Keseluruhan Insiden Siber:** Jika hal itu terjadi pada Anda, pelanggaran atau insiden siber dapat mengakibatkan kerugian hingga ratusan ribu dolar.

Average Costs from Ransomware



Business Sector
Top 5 by Number of Claims - SMEs

Average Incident Costs



Sumber: Net Diligence

Berikut ini beberapa kasus aktual insiden siber di Indonesia:

1. Pada tahun 2023, salah satu bank Islam terbesar di negara ini mengalami serangan siber yang parah. Serangan ini melibatkan *ransomware* yang menargetkan infrastruktur digital bank, mengenkripsi data penting, dan mengganggu layanannya. Serangan *ransomware* tersebut menyebabkan gangguan operasional yang signifikan, memengaruhi layanan perbankan dan akses nasabah ke rekening mereka. Serangan ini juga menimbulkan kekhawatiran tentang keamanan lembaga keuangan di Indonesia. Serangan tersebut menyebabkan penghentian sementara beberapa layanan dan mendorong bank untuk bekerja sama dengan para ahli keamanan siber guna menyelesaikan masalah dan memperkuat struktur keamanannya. Insiden tersebut menyoroti perlunya peningkatan praktik keamanan siber di dalam lembaga keuangan.

2. Pada tahun 2024, terjadi kebocoran data yang cukup besar yang melibatkan Badan Siber dan Sandi Negara (BSSN). Pembobolan ini membocorkan informasi sensitif terkait operasional keamanan siber dan komunikasi internal BSSN. Pembobolan ini menimbulkan kekhawatiran serius terhadap keamanan infrastruktur keamanan siber Indonesia dan lembaga yang bertanggung jawab atas pertahanan siber nasional. Pembobolan ini menyoroti potensi risiko ancaman internal dan perlunya praktik keamanan yang lebih ketat. BSSN, bekerja sama dengan lembaga pemerintah lain dan pakar keamanan siber, mengambil tindakan segera untuk mengatasi kebocoran tersebut, mengamankan sistem yang terdampak, dan meningkatkan langkah-langkah keamanan internal. Insiden ini juga mendorong peninjauan ulang strategi keamanan siber nasional.

Jaminan

1. **Biaya Penyelidikan IT Forensik**
   Menjamin biaya tenaga ahli keamanan IT eksternal. Termasuk biaya penasihat hukum untuk menunjuk, mengawasi, dan memandu ahli keamanan IT eksternal.
2. **Biaya Tanggapan Privasi**
   Menjamin biaya yang timbul sebagai akibat dari Pelanggaran Privasi.
3. **Biaya Pemulihan Data**
   Menjamin biaya atas nama Tertanggung jika data telah terkorupsi, terhapus, dienkripsi, rusak, atau hancur. Termasuk biaya untuk pemulihan, restorasi, masukan, konfigurasi, atau penggantian.
4. **Kerugian Akibat Gangguan Usaha**
   Menjamin biaya jika Tertanggung tidak dapat menggunakan aset data untuk aktivitas bisnis.
5. **Tanggung Gugat**
   Menjamin pembayaran yang diwajibkan secara hukum atas nama Tertanggung akibat dari kerusakan aset data pihak ketiga yang disebabkan oleh Pelanggaran Kerahasiaan, Pelanggaran Privasi, atau Pelanggaran Keamanan.
6. **Kerugian Akibat Pemerasan**
   Menjamin kerugian karena ancaman yang timbul akibat pengungkapan informasi rahasia, aset data yang rusak, dan terganggunya ketersediaan sistem komputer.
7. **Denda/Biaya Regulasi**
   Menjamin sanksi regulasi dan biaya regulasi terkait yang diakibatkan oleh Pelanggaran Privasi.

KISARAN PREMI UNTUK BISNIS UKM

Pendapatan Bruto Tahunan (dalam USD)	Batas Ganti Rugi (dalam USD)				
	250.000	500.000	1.000.000	1.500.000	2.000.000
500 ribu - 2 juta	1.300 - 1.600	1.650 - 1.900			
2 juta - 5 juta	1.600 - 1.900	1.900 - 2.300			
5 juta - 10 juta	1.900 - 2.500	2.300 - 3.100	3.100 - 3.900	4.700 - 4.900	5.900 - 6.200
10 juta - 15 juta	2.500 - 3.500	3.100 - 4.400	3.900 - 5.500	4.900 - 6.800	6.200 - 8.300
15 juta - 25 juta	3.500 - 5.700	4.400 - 7.000	5.500 - 8.700	6.800 - 11.200	8.300 - 13.600
25 juta - 35 juta	5.700 - 8.000	7.000 - 9.800	8.700 - 12.300	11.200 - 15.200	13.600 - 18.500
35 juta - 50 juta	8.000 - 10.900	9.800 - 13.150	12.300 - 16.400	15.200 - 21.000	18.500 - 25.700

Catatan:

1) Tabel di atas adalah kisaran premi berdasarkan pendapatan kotor tahunan dan batas ganti rugi hanya untuk pertanggungan standar.
2) Premi final akan bergantung pada jumlah pendapatan kotor tahunan aktual dari calon Tertanggung.
3) Premi final dapat berada di luar kisaran premi di atas, tergantung pada pertimbangan Underwriting setelah menganalisis informasi dalam SPPA.
4) Secara umum, kisaran premi di atas dapat diterapkan jika kriteria pada SPPA terpenuhi (jawab "Ya" untuk pertanyaan pada Pertanyaan Bagian 2A dan Pertanyaan Bagian 3 A-K).

Perluasan Jaminan (Opsional)

1. **Gangguan Usaha dan Biaya Pemulihan Akibat Kesalahan Operasional**
   Menjamin kerusakan aset data dan sistem komputer yang disebabkan oleh kesalahan yang tidak disengaja dari karyawan.
2. **Tanggung Gugat Media**
   Menjamin kerugian dan biaya klaim yang timbul dari klaim pelanggaran konten.
3. **Pelanggaran Informasi Pribadi**
   Menjamin ganti rugi dan biaya yang timbul akibat dari "pelanggaran informasi pribadi".
4. **Pembayaran Kartu Industri/*Payment Card Industry* (PCI)**
   Menjamin pembayaran sebagai akibat dari pelanggaran kartu pembayaran. (Bagian ini hanya relevan bagi Tertanggung yang memproses atau menyimpan informasi kartu pembayaran).
5. **Kerugian Gangguan Reputasi**
   Memberikan ganti rugi kepada Tertanggung atas kerugian gangguan bisnis yang secara langsung dan semata-mata disebabkan oleh penurunan merek/reputasi.
6. **Kejahatan Siber**
   Memberikan ganti rugi atas kerugian keuangan secara langsung sebagai akibat dari transfer dana yang Anda lakukan yang disebabkan oleh:
   - Ketergantungan pada instruksi yang tidak sah, tidak jujur, atau ilegal yang disisipkan ke dalam sistem komputer atau aset data Anda.
   - Akses ke sistem komputer atau aset data Anda yang diperoleh melalui pelanggaran keamanan.

Mohon diperhatikan bahwa premi tambahan akan berlaku untuk perjanjian asuransi tambahan di atas.

Keuntungan Produk

- Produk fleksibel yang dapat disesuaikan dengan kebutuhan cakupan dan anggaran
- Saluran bantuan penanganan insiden 24/7. Tenaga ahli dari vendor akan menyediakan layanan di setiap tahapan proses penanganan insiden; Investigasi Forensik TI/Hubungan Masyarakat/Pusat Panggilan/Perlindungan Identitas, dll.



Pengecualian

1. Cedera Tubuh
2. Tanggung Jawab Kontraktual
3. Tindakan Tidak Jujur
4. Program Ilegal
5. Infrastruktur
6. Kepailitan Tertanggung atau Pihak Ketiga
7. Peristiwa Fisik
8. Tindakan Sebelumnya
9. Kerusakan Properti

Lainnya sesuai dengan *Wording* Polis

PROSES PENANGANAN INSIDEN OLEH MSIG

Ahli bidang siber dan penasihat hukum MSIG akan bekerja atas nama Tertanggung sebagai bagian dari Layanan Bantuan 24/7 Asuransi Cyber MSIG

1. ***Pemegang Polis menghubungi nomor telepon Layanan Penanganan Insiden***
2. ***Pengelola Respons mencatat informasi penting***
3. ***Pengelola Respons menghubungi para ahli hukum yang berwenang***
4. ***Pemeriksaan terhadap laporan - eskalasi apabila timbul permasalahan terkait dengan laporan***
5. ***Menghubungi Pemegang Polis untuk melakukan pemeriksaan (dalam kurun waktu 2 jam)***
6. ***Pengelola Respons menghubungi/ mempertimbangkan penunjukkan vendor***
7. ***Pengelola Respons membuat laporan dalam waktu 24/48 jam***
8. ***Pengelola Insiden menyetujui lembar laporan/template laporan untuk diselesaikan***
9. ***Insiden diselesaikan***
10. ***Melakukan peninjauan ulang dengan Pemegang Polis - pelajaran yang didapat dari insiden***