Kementerian Kesehatan
Sekretariat Jenderal
Jalan H.R. Rasuna Said Blok X-5 Kavling 4-9
Jakarta Selatan 12950
(021) 5201590 (hunting)
https://www.kemkes.go.id

Yth.

1. para pejabat pimpinan tinggi madya;
2. para pimpinan unit/satuan kerja;
3. pengampu sistem informasi di unit/satuan kerja; dan
4. tim tanggap insiden siber;

di lingkungan Kementerian Kesehatan

SURAT EDARAN
NOMOR HK.02.02/A/4071/2024
TENTANG
HIMBAUAN PENCEGAHAN DAN MITIGASI *RANSOMWARE* DI LINGKUNGAN KEMENTERIAN KESEHATAN

Himbauan mengenai pencegahan dan mitigasi *ransomware* pada layanan publik diatur dalam Surat Edaran Kepala Badan Siber dan Sandi Negara Nomor 42 Tahun 2024 tentang Himbauan Pencegahan dan Mitigasi *Ransomware* pada Layanan Publik. Dalam rangka memberikan penjelasan secara lengkap mengenai tata cara tindakan pencegahan dan penanganan terhadap ancaman *malware* khususnya *ransomware* di lingkungan Kementerian Kesehatan, maka diperlukan acuan sebagai upaya untuk mencegah serangan siber pada layanan kesehatan.

Maksud dan tujuan Surat Edaran ini dimaksudkan sebagai tindak lanjut dan acuan bagi pengelola sistem informasi kesehatan di lingkungan Kementerian Kesehatan dalam melakukan tindakan pencegahan dan penanganan terhadap ancaman *malware* khususnya *ransomware*.

Mengingat ketentuan:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);
2. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820);

3. Undang-Undang Nomor 17 Tahun 2023 tentang Kesehatan (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 105, Tambahan Lembaran Negara Republik Indonesia Nomor 6887);
4. Peraturan Pemerintah Nomor 46 Tahun 2014 tentang Sistem Informasi Kesehatan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 126, Tambahan Lembaran Negara Republik Indonesia Nomor 5542);
5. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
8. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
9. Peraturan Menteri Kesehatan Nomor 5 Tahun 2022 tentang Organisasi dan Tata Kerja Kementerian Kesehatan (Berita Negara Republik Indonesia Tahun 2022 Nomor 156);
10. Peraturan Badan Siber dan Sandi Negara Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital (Berita Negara Republik Indonesia Tahun 2023 Nomor 872);
11. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber (Berita Negara Republik Indonesia Tahun 2024 Nomor 43).

Sehubungan dengan hal tersebut, disampaikan kepada para pejabat pimpinan tinggi madya, para pimpinan unit/satuan kerja, pengampu sistem informasi di unit/satuan kerja, dan tim tanggap insiden siber di lingkungan Kementerian Kesehatan mengenai tindakan pencegahan dan penanganan terhadap ancaman *malware* khususnya *ransomware* di lingkungan Kementerian Kesehatan sebagai berikut:

1. Pengelola sistem informasi kesehatan di lingkungan Kementerian Kesehatan dalam melakukan tindakan pencegahan dan penanganan terhadap ancaman *malware* khususnya *ransomware* melaksanakan hal-hal sebagai berikut:
    a. meningkatkan *security awareness* dengan cara mempelajari panduan penanganan insiden siber yang telah diterbitkan oleh Badan Siber dan Sandi Negara;

b. berkoordinasi dengan Kementerian Kesehatan *Computer Security Incident Response Team* (Kemenkes CSIRT) melalui *helpdesk* di nomor telepon seluler 08119056765 dalam melaksanakan langkah-langkah pencegahan;

c. menerapkan langkah-langkah pencegahan sesuai ketentuan teknis sebagaimana dimaksud dalam Surat Edaran ini; dan

d. melaporkan hasil pelaksanaan kegiatan pencegahan dan penanganan secara berkala triwulan kepada Kemenkes CSIRT melalui *e-mail* csirt@kemkes.go.id.

2. Pengelola sistem informasi kesehatan di lingkungan Kementerian Kesehatan dalam melakukan tindakan pencegahan dan penanganan terhadap ancaman *malware* khususnya *ransomware* melaksanakan langkah-langkah sesuai ketentuan teknis sebagai berikut:

a. tindakan pencegahan meliputi:

1) mengimplementasikan mekanisme perubahan *password* secara berkala;

2) menerapkan prinsip least *privileges*/memberikan kewenangan sesuai kebutuhan pada jaringan ataupun sistem operasi;

3) melakukan *update* dan *patching* pada seluruh perangkat lunak terkait sistem informasi kesehatan;

4) memastikan kembali seluruh sistem operasi dan perangkat lunak sudah menggunakan *security patches* terkini melalui pengelola IT satuan kerja;

5) memastikan para pengembang sistem yang bekerja sama menerapkan standar manajemen keamanan informasi sistem pemerintahan berbasis elektronik serta standar teknis dan prosedur keamanan sistem pemerintahan berbasis elektronik sesuai dengan ketentuan peraturan perundang-undangan.

6) melaksanakan prosedur *backup* atau pemulihan data secara berkala yang dilakukan oleh pengelola pusat data sistem informasi kesehatan ditempatkan yang periode pelaksanaannya dapat disesuaikan dengan kebutuhan sistem; dan

7) menggunakan aplikasi *antivirus* atau *antimalware* dengan versi terbaru atau yang paling mutakhir dan memastikan dilakukannya pemindaian secara berkala minimal satu minggu sekali.

b. tindakan penanganan meliputi:

1) melaksanakan langkah-langkah panduan penanganan insiden siber yang terdapat pada tautan https://link.kemkes.go.id/panduaninsidensiber;

2) melaporkan insiden *ransomware* kepada Kemenkes CSIRT melalui *e-mail* csirt@kemkes.go.id; dan

3) berdasarkan laporan insiden sebagaimana dimaksud pada angka 1), Kemenkes CSIRT melakukan pengelolaan insiden dan pelaporan sesuai dengan ketentuan peraturan perundang-undangan.

3. Kepala Pusat Data dan Teknologi Informasi melakukan monitoring dan evaluasi, serta melaporkan pelaksanaan Surat Edaran ini secara berkala atau sewaktu-waktu sesuai dengan kebutuhan kepada Sekretaris Jenderal.

Demikian Surat Edaran ini untuk dapat dilaksanakan dengan penuh tanggung jawab sesuai dengan ketentuan peraturan perundang-undangan.

Ditetapkan di Jakarta
Pada tanggal 29 Juli 2024

SEKRETARIS JENDERAL
KEMENTERIAN KESEHATAN,

ttd.

KUNTA WIBAWA DASA NUGRAHA

Tembusan:
1. Menteri Kesehatan; dan
2. Wakil Menteri Kesehatan.

Salinan sesuai dengan aslinya
Kepala Biro Hukum
Sekretariat Jenderal Kementerian Kesehatan,

Indah Febrianti, S.H., M.H.
NIP 197802122003122003