

# PANDUAN KEAMANAN SIBER

## MANAJEMEN RESIKO KEAMANAN DI TENGAH PANDEMI COVID-19



Panduan ini berisi mengenai hal-hal yang perlu diperhatikan oleh para pengambil kebijakan, pekerja berkaitan dengan isu keamanan informasi yang timbul sebagai akibat dari pandemi COVID-19 (*Corona Virus Disease 2019*) yang ditetapkan oleh WHO. Berdasarkan data bahwa kasus pasien COVID-19 di Indonesia meningkat cukup signifikan sejak diumumkan oleh Presiden Joko Widodo pada tanggal 2 Maret 2020. Sehingga untuk mencegah penyebaran infeksi COVID-19 telah dikeluarkan sejumlah strategi dan kebijakan baik oleh Pemerintah maupun sejumlah perusahaan di Indonesia mulai dari pembatasan interaksi hingga mewajibkan pekerja bekerja dari rumah (*Work From Home*).

### POTENSI RESIKO COVID-19 TERHADAP KEBERLANGSUNGAN BISNIS

Guna mencegah penyebaran dan penularan COVID-19 secara luas di wilayah Indonesia, setiap organisasi baik pemerintah maupun swasta harus menyusun rencana mengenai potensi dampak dari COVID-19 terhadap proses operasional layanan bisnisnya. Sehingga perlu diambil langkah untuk melakukan operasional bisnis/layanan melalui bekerja dari rumah (*Working From Home*).

### APA YANG DIMUAT DALAM PANDUAN INI?

Berkaitan dengan hal tersebut BSSN menilai ada beberapa aspek yang perlu menjadi perhatian serius bagi seluruh pemangku kepentingan untuk tetap menjalankan operasional layanan/bisnisnya dalam kondisi dan situasi darurat seperti saat ini.

Panduan berikut berisi mengenai rekomendasi

- **Identifikasi dan Persiapan**
- **Keamanan Rantai Pemasok**
- **Penerapan Keamanan Siber bagi Organisasi**
- **Keamanan Siber bagi Pekerja dan Pengguna**

Rekomendasi ini diharapkan dapat dijadikan sebagai acuan oleh seluruh pemangku kepentingan untuk menjamin keamanan dalam penyelenggaraan layanan/operasional bisnis melalui kebijakan *working from home*.

IDENTIFIKASI DAN  
PERSIAPAN

KEAMANAN RANTAI  
PEMASOK

PENERAPAN  
KEAMANAN SIBER  
BAGI ORGANISASI

KEAMANAN SIBER  
BAGI PEKERJA DAN  
PENGGUNA

# #1 IDENTIFIKASI DAN PERSIAPAN

Tahapan yang paling penting dan menentukan dalam upaya mereduksi dampak COVID-19 pada proses keberlangsungan bisnis/layanan adalah tahapan persiapan dan perencanaan. BSSN merekomendasikan langkah-langkah berikut dalam upaya perlindungan keamanan terhadap infrastruktur teknologi informasi yang menunjang layanan/bisnis.

**Identifikasi proses bisnis/sistem yang kritis** bagi organisasi yang tetap akan dijalankan dengan skema operasional melalui *working from home*.

**Identifikasi proses bisnis yang sulit / dikecualikan** untuk dilakukan secara teleworking. Umumnya hal ini yang membutuhkan akses fisik secara langsung ke dalam sistem.

**Tetapkan penanggung jawab** dari setiap proses bisnis atau sistem yang kritis tersebut, kemudian tetapkan tim beserta tugas dan tanggung jawabnya. Termasuk penanggung jawab keamanan informasi dari layanan tersebut.

**Buat aturan formal** mengenai mekanisme operasional dari layanan tersebut, jam kerja, pendefinisian *role akses*, dan kebijakan keamanan informasi.

**Latih pekerja** untuk menjalankan aturan formal yang ditetapkan

**Identifikasi fungsi esensial** maupun pemasok yang menunjang proses bisnis/layanan tersebut. Lakukan monitoring keamanan terhadap fungsi esensial serta pastikan rantai pasok terhadap fungsi esensial tersebut dapat berjalan.

**Lakukan penilaian secara kontinyu** mengenai kesiapan layanan dalam menghadapi perubahan proses bisnis dan dampak dari perubahan lingkungan.

**Rancang skenario** kerja bagi pekerja secara *remote*. Pembuatan skenario perlu dilakukan guna memilah dan mengantisipasi kondisi terburuk terjadinya *lockdown*.

**Selalu monitor mengenai kebijakan** pemerintah pusat maupun daerah terhadap upaya penanganan COVID-19 sehingga adaptasi proses bisnis dapat dilakukan secara cepat.

# #2 KEAMANAN RANTAI PEMASOK

Tahapan berikutnya adalah memastikan tersedianya dukungan keberlangsungan proses bisnis/layanan berkaitan dengan ketersediaan dukungan dari pemasok. Langkah-langkah yang direkomendasikan pada tahapan ini antara lain:

**Lakukan penilaian mengenai rantai pasok yang berkaitan dengan proses bisnis/layanan organisasi** berkaitan dengan kemungkinan dampak gangguan akibat keterlambatan pengiriman pasokan/logistik maupun keterlambatan proses manufaktur akibat pandemi global COVID-19.

**Komunikasi dengan penyedia/rantai pemasok yang digunakan oleh organisasi anda** mengenai tantangan yang mungkin dihadapi dalam kondisi terburuk akibat pandemi COVID-19.

**Identifikasi** potensi penyedia/pemasok lain yang dapat mendukung proses operasional bisnis/layanan ketika terjadi gangguan

**Komunikasikan hal ini kepada pengguna/konsumen** mengenai keterbatasan yang dihadapi serta langkah mitigasi yang dilakukan oleh organisasi.

# #3 PENERAPAN KEAMANAN SIBER BAGI ORGANISASI

Mengingat hampir sebagian besar organisasi menerapkan kebijakan bekerja dari rumah saat pandemi COVID-19, BSSN merekomendasikan langkah-langkah berikut untuk tetap menjamin keamanan serta keberlangsungan layanan :

**Memastikan keamanan dari sistem yang dapat diakses secara remote**

- Pastikan jaringan privat virtual dan sistem lainnya yang diakses secara *remote* telah dilakukan *patch* keamanannya

- Lakukan monitoring keamanan terhadap seluruh sistem dan aktifitas pengguna yang mengakses sistem tersebut
- Terapkan kebijakan Otentikasi *Multi Factor*, seperti dengan menggunakan OTP atau Token
- Pastikan setiap pengguna telah dibatasi hak akses sesuai dengan rolenya dalam organisasi/layanan
- Pastikan seluruh mesin telah dilindungi dengan perimeter keamanan (*firewall*, IDS, IPS), anti-virus dan anti-malware.

Lakukan uji kapasitas dan koneksi koneksi *remote* yang diberikan untuk menjamin keberlangsungan layanan

Pastikan rencana keberlanjutan bisnis dimutakhirkan.

**Berikan edukasi mengenai keamanan informasi** pada setiap pekerja yang melakukan pekerjaan secara *remote*.

**Mutakhirkan rencana tanggap insiden keamanan** untuk menyesuaikan dengan kondisi perubahan lingkungan kerja yang tersebar dari berbagai lokasi.

## #4 KEAMANAN SIBER BAGI PEKERJA DAN PENGGUNA

Kondisi pandemi COVID-19 telah banyak dimanfaatkan oleh pelaku kejahatan siber untuk menuai keuntungan, karena informasi terkait dengan penyebaran COVID-19 atau perkembangannya sangat dicari oleh pengguna/konsumen. Metode phishing melalui e-mail atau tautan halaman situs berbahaya kerap kali menjadi metode yang efektif untuk dijalankan oleh pelaku kejahatan. Oleh karena itu kita sebagai pengguna/konsumen harus senantiasa waspada terhadap hal ini. BSSN merekomendasikan pengguna/konsumen harus tetap waspada terhadap berbagai bentuk kejahatan siber dengan melakukan langkah-langkah berikut :

**Hindari untuk mengklik tautan di dalam email yang berisi ajakan/promosi/informasi** dan selalu waspada terhadap setiap file elektronik yang dilampirkan, karena bisa saja mengandung konten yang berbahaya.

**Jangan mengungkapkan informasi pribadi/informasi finansial** kepada siapapun

**Selalu kunjungi situs resmi pemerintah** untuk mendapatkan update mengenai kondisi COVID-19 untuk menghindari anda dari infeksi malware karena mengklik tautan yang tidak dikenal

**Selalu lengkapi perangkat mobile/komputer anda dengan** antivirus yang diupdate definisinya secara berkala

**Pastikan anda tidak membagikan informasi mengenai kredensial (*username/password*)** anda kepada orang lain

**Pastikan bahwa keluarga dan atau anak tidak menggunakan perangkat yang digunakan untuk melakukan akses kerja dari rumah**, guna meminimalisir kondisi yang secara sengaja atau tidak menghapus atau memodifikasi informasi pada perangkat elektronik atau bahkan lebih buruk yang mungkin dapat mengakibatkan perangkat terinfeksi.

### HIMBAUAN KEPADA MASYARAKAT

- Memilih informasi tentang Virus COVID-19 dari sumber yang jelas dan dapat dipertanggungjawabkan
- Memverifikasi kebenaran setiap informasi tentang Virus COVID-19 yang diterima dari media sosial
- Berperan aktif dalam memberikan klarifikasi yang benar, apabila menemukan informasi hoaks tentang Virus COVID-19
- Saling mengingatkan akan dampak negatif dari penyebaran informasi hoaks tentang Virus COVID-19