MENGUATKAN KOMITMEN DAN MEMBANGUN KETANGGUHAN TIM PUNGGAWA SIBER KOTA MAGELANG

Oleh:
H. Damar Prasetyono
Wali Kota Magelang



Pemerintahan Digital Membutuhkan Keamanan yang Kuat



Pemanfatan teknologi digital semakin luas



Layanan pemerintahan makin bergaitung pada sistem elektronik



Keamanan digital menjaga kelancaran pemerintahan



Data dan Informasi Adalah Amanah yang Harus Dijaga



- Untuk administrasi
- Untuk perencanaan
- Untuk pengambilan keputusan
- Untuk pelayanan masyarakat

Ancaman Siber Dapat Terjadi Dalam Aktivitas Sehari-hari

- Pencurian akun
- Berita hoaks
- Link palsu
- Virus berbahaya
- Kebocoran data
- Gangguan sistem



Kesiapsiagaan Siber Membutuhkan Keterlibatan Seluruh Unsur Pemerintahan



Dampaknya dapat melalui berbagai unit kerja

Perlu informasi yang cepat dan koordinasi tepat

Dibutuhkan personel yang memahami keamanan informasi

Kota Magelang Telah Membangun Fondasi Keamanan Siber



15 Desember 2023

Pembentukan Tim Tanggap Insiden Siber Kota Magelang melalui SK Wali Kota Nomor 046/293/112 Tahun 2023.



18 Januari 2024

Registrasi MAGELANGKOTA-CSIRT oleh BSSN melalui STR Nomor 301/CSIRT.01.02.01/BSSN/01/2024.



21 Agustus 2026

Penetapan Tim Punggawa Siber melalui SK Wali Kota Nomor 500.12/063/112 Tahun 2026.



Menunjukkan Komitmen yang Terus Diperkuat

Punggawa Siber Adalah Penguatan Kesiapan dan Koordinasi



- Memperkuat kesiapan menghadapi ancaman
- Mendorong keterlibatan perangkat daerah
- Menghubungkan unsur pembina dan teknis
- Meningkatkan kapasitas SDM
- Memperkuat koordinasi penanganan insiden

Keamanan Siber Adalah Tanggung Jawab Bersama





Kepala Daerah

Memberikan arah, dukungan, dan mendorong pelaksanaan kebijakan.



Perangkat Daerah dan Kelurahan

Memastikan penerapan keamanan informasi dan penugasan personel.



Personel Punggawa Siber

Menjalankan tugas pembinaan, pemantauan, penanganan, dan pemulihan sesuai peran masing-masing.

Kenali, Laporkan, dan Tangani Ancaman Siber



Kenali dan Identifikasi Ancaman



Terima dan Verifikasi Laporan



Lakukan Penanganan Terkoordinasi



Pulihkan dan Evaluasi

Kenali dan Identifikasi Ancaman Siber

Amati aktivitas digital dan waspadai tanda-tanda yang tidak biasa.





Akses atau aktivitas akun tidak dikenal

Misalnya ada percobaan masuk (login) atau penggunaan akun dari perangkat, lokasi, atau waktu yang tidak biasa.



Pesan atau tautan mencurigakan

Misalnya pesan yang tidak biasa, tidak relevan, atau berisi tautan/alamat website yang ragu keamanannya.



Perubahan atau gangguan sistem yang tidak wajar

Misalnya layanan menjadi lambat, tidak dapat diakses, atau muncul tampilan/pesan kesalahan yang tidak biasa.



Jika menemukan indikasi tersebut, jangan abaikan. Catat hal yang terlihat dan lanjutkan melalui mekanisme pelaporan yang berlaku.

Terima dan Verifikasi Laporan

Kelola setiap laporan dugaan insiden dengan melakukan verifikasi awal untuk memastikan jenis dan dampaknya.



Proses yang Dilakukan



1. Terima Laporan

Terima laporan indikasi insiden dari personel melalui kanal pelaporan yang ditetapkan.



2. Verifikasi Awal

Periksa dan pastikan informasi laporan, seperti waktu kejadian, layanan/sistem yang terdampak, serta gejalanya.



3. Identifikasi Jenis dan Dampak

Tentukan apakah laporan termasuk insiden siber, serta nilai tingkat dampaknya (mis. rendah, sedang, tinggi).



4. Catat dan Tindak Lanjuti

Dokumentasikan hasil verifikasi dan teruskan ke proses penanganan sesuai prosedur yang berlaku.



Tujuan: **Memastikan setiap laporan ditangani dengan tepat, cepat, dan sesuai prioritas.**

Lakukan Penanganan Terkoordinasi

Tangani insiden secara terkoordinasi sesuai tugas, fungsi, dan kewenangan masing-masing, dengan dukungan Diskominsta Kota Magelang.



Langkah Penanganan

1. Terima Laporan

Terima laporan indikasi insiden dari personel melalui kanal pelaporan yang ditetapkan.

2. Verifikasi Awal

Periksa dan pastikan informasi laporan, seperti waktu kejadian, layanan/sistem yang terdampak, serta gejalanya.

3. Identifikasi Jenis dan Dampak

Tentukan apakah laporan termasuk insiden siber, serta nilai tingkat dampaknya (mis. rendah, sedang, tinggi).

4. Pemulihan Layanan

Lakukan perbaikan dan pemulihan layanan agar sistem dapat kembali berjalan dengan aman dan normal.

Tujuan: **Memastikan setiap laporan ditangani dengan tepat, cepat, dan sesuai prioritas.**

Pulihkan dan Evaluasi Layanan

Kembalikan layanan agar berfungsi normal, serta lakukan evaluasi untuk memperkuat keamanan ke depan.



Langkah yang Dilakukan



1 Pemulihan Sistem dan Layanan

Lakukan perbaikan teknis dan pastikan layanan kembali berjalan dengan aman dan normal.



2 Evaluasi Penyebab dan Dampak

Tinjau kembali akar penyebab, dampak, serta efektivitas penanganan yang telah dilakukan.



3 Perbaikan dan Penguatan

Tindak lanjuti hasil evaluasi, misalnya perbaikan sistem, peningkatan pengamanan, atau pembaruan prosedur.



4 Dokumentasi dan Pelaporan

Simpan catatan penanganan secara lengkap dan laporkan hasilnya sesuai ketentuan yang berlaku.



Tujuan: Layanan kembali pulih, risiko serupa dapat dicegah, dan keamanan sistem makin kuat.

Dukungan Kepala Perangkat Daerah Menjadi Kunci Keberhasilan



- Berikan perhatian terhadap pelaksanaan tugas Punggawa Siber.
- Pastikan personel memahami tanggung jawabnya.
- Dukung peningkatan kapasitas SDM.
- Dorong penerapan keamanan informasi di setiap unit kerja.


Bersama Menjaga
Pemerintahan Digital
yang Aman dan Terpercaya
Perkuat koordinasi
Jaga keamanan data dan informasi
Tingkatkan kesiapsiagaan
Bangun budaya informasi yang bertanggung jawab
Jaga kelancaran pelayanan