



**WALI KOTA YOGYAKARTA
DAERAH ISTIMEWA YOGYAKARTA**

KEPUTUSAN WALI KOTA YOGYAKARTA

NOMOR 143 TAHUN 2024

TENTANG

**PEMBENTUKAN JOGJAKARTA *COMPUTER SECURITY INCIDENT
RESPONSE TEAM***

WALI KOTA YOGYAKARTA,

- Menimbang : a. bahwa pemanfaatan teknologi informasi dan komunikasi (TIK) maupun teknologi terkait dapat menyebabkan kerawanan dan ancaman siber yang meliputi aspek kerahasiaan, keutuhan, ketersediaan, nir-sangkal, otentisitas, akuntabilitas dan keandalan layanan, sehingga dibutuhkan penyediaan pelayanan publik yang cepat, andal, dan aman;
- b. bahwa penyelenggara sistem elektronik wajib menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan, penanggulangan dan pemulihan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian;
- c. bahwa untuk menjamin sistem elektronik dapat beroperasi secara terus menerus, maka diperlukan mekanisme penanggulangan insiden dan/atau pemulihan insiden yang dilakukan oleh tim penanggulangan dan pemulihan insiden siber;
- d. bahwa untuk melaksanakan kegiatan sebagaimana dimaksud dalam huruf c, diperlukan *Jogjakota Computer Security Incident Response Team* (*Jogjakota CSIRT*);
- e. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c dan huruf d, perlu menetapkan Keputusan Wali Kota tentang Pembentukan *Jogjakota Computer Security Incident Response Team* (*Jogjakota CSIRT*);
- Mengingat : 1. Undang-Undang Nomor 16 Tahun 1950 tentang Pembentukan Daerah-daerah Kota Besar dalam Lingkungan Propinsi Djawa Timur, Djawa Tengah, Djawa Barat dan Dalam Daerah Istimewa Jogjakarta;
2. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah beberapa kali diubah, terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang;

3. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber;
4. Peraturan Wali Kota Yogyakarta Nomor 113 Tahun 2019 tentang Sistem Manajemen Keamanan Informasi;

MEMUTUSKAN:

- Menetapkan** : **KEPUTUSAN WALI KOTA TENTANG PEMBENTUKAN JOGJAKARTA *COMPUTER SECURITY INCIDENT RESPONSE TEAM* (JOGJAKARTA CSIRT).**
- KESATU** : Membentuk *Jogjakota Computer Security Incident Response Team* (Jogjakota CSIRT) dengan susunan personalia sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan Wali Kota ini.
- KEDUA** : *Jogjakota Computer Security Incident Response Team* (Jogjakota CSIRT) sebagaimana dimaksud dalam Diktum KESATU mempunyai layanan, berupa:
- a. Layanan Utama terdiri atas:
 1. pemberian peringatan terkait keamanan siber; dan
 2. pengelolaan insiden siber.
 - b. Layanan Tambahan terdiri atas:
 1. penanganan kerentanan sistem elektronik;
 2. penanganan artefak digital;
 3. pemberitahuan hasil pengamatan potensi ancaman;
 4. pendeteksian serangan;
 5. analisis risiko keamanan siber;
 6. konsultasi terkait kesiapan penanganan insiden siber; dan
 7. pembangunan kesadaran dan kepedulian terhadap keamanan siber.
- KETIGA** : *Jogjakota Computer Security Incident Response Team* (Jogjakota CSIRT) sebagaimana dimaksud dalam Diktum KESATU memiliki konstituen yaitu Perangkat Daerah Penyelenggara Teknologi Informasi di lingkungan Pemerintah Kota Yogyakarta.
- KEEMPAT** : *Jogjakota Computer Security Incident Response Team* (Jogjakota CSIRT) sebagaimana dimaksud dalam Diktum KESATU mempunyai tugas dan tanggung jawab:
- a. Pengarah
 1. Ketua:
 - a) menjamin terselenggaranya pengelolaan penanggulangan dan pemulihan insiden siber di Kota Yogyakarta yang meliputi organisasi, sumber daya manusia, dan anggaran yang memadai; dan

- b) memberikan pembinaan, kebijakan, sasaran, dan petunjuk teknis dalam penyelenggaraan pengelolaan pengaduan pelayanan insiden siber di Kota Yogyakarta.

2. Wakil Ketua:

- a) memberikan masukan kepada Ketua untuk menjamin terselenggaranya pengelolaan insiden siber di Kota Yogyakarta meliputi organisasi, sumber daya manusia, dan anggaran yang memadai;
- b) membantu memberikan pembinaan, kebijakan, dan petunjuk teknis dalam pengelolaan penanggulangan, dan pemulihan insiden siber di Kota Yogyakarta; dan
- c) membantu Ketua dalam melaksanakan tugas dan tanggung jawabnya.

3. Anggota:

- a) memberikan masukan terhadap tujuan, sasaran, dan kegiatan pengelolaan penanggulangan dan pemulihan insiden siber;
- b) memberikan masukan terhadap pelaksanaan teknis pengelolaan penanggulangan dan pemulihan insiden siber;
- c) menyiapkan dukungan teknis operasional yang diperlukan oleh tim pelaksana; dan
- d) melaksanakan tugas terkait pengelolaan penanggulangan dan pemulihan insiden siber yang diberikan oleh Ketua Pengarah.

b. Pelaksana

1. Ketua:

- a. memimpin pelaksanaan tugas dan bertanggung jawab atas semua kegiatan *Jogjakota Computer Security Incident Response Team* Kota Yogyakarta (Jogjakota CSIRT);
- b. bertanggung jawab dalam pengelolaan sumber daya yang dibutuhkan untuk mengatasi permasalahan dan isu penting terkait keamanan siber dalam penyelenggaraan pemerintahan daerah di Kota Yogyakarta;
- c. mengoordinasikan *Jogjakota Computer Security Incident Response Team* Kota Yogyakarta (Jogjakota CSIRT) dengan instansi dan pihak-pihak yang berkepentingan lainnya terkait pelaksanaan tugas, fungsi dan perannya;
- d. memantau kinerja dan efektivitas *Jogjakota Computer Security Incident Response Team* Kota Yogyakarta (Jogjakota CSIRT);

- e. memberikan edukasi untuk meningkatkan kesadaran, kewaspadaan, dan peringatan mengenai keamanan siber di Kota Yogyakarta;
- f. membuat perencanaan strategis dan operasional mengenai Jogjakota CSIRT;
- g. melakukan koordinasi pencegahan dan penanggulangan insiden siber yang terjadi kepada Badan Siber dan Sandi Negara; dan
- h. menyusun dan menyampaikan laporan kepada tim pengarah.

2. Sekretaris:

- a. melaksanakan koordinasi, ketatausahaan, pembinaan dan pengendalian program, kegiatan, administrasi, sumber daya dan dokumentasi Jogjakota *Computer Security Incident Response Team* (Jogjakota CSIRT);
- b. menyediakan *Point of Contact* (POC) untuk operasional Jogjakota *Computer Security Incident Response Team* (Jogjakota CSIRT);
- c. mengoordinasikan tugas unsur anggota dalam pelaksanaan Jogjakota *Computer Security Incident Response Team* (Jogjakota CSIRT);
- d. mengelola fasilitas dan sumber daya yang dibutuhkan untuk operasional Jogjakota *Computer Security Incident Response Team* (Jogjakota CSIRT);
- e. mengoordinasikan kegiatan peningkatan kompetensi sumber daya manusia pengguna teknologi informasi di Kota Yogyakarta melalui pendidikan dan pelatihan terkait penanggulangan insiden siber;
- f. mengoordinasikan pelaksanaan sosialisasi dan informasi mengenai keamanan siber di lingkungan Jogjakota *Computer Security Incident Response Team* (Jogjakota CSIRT);
- g. melaksanakan evaluasi rutin terhadap pelaksanaan program dan kegiatan Jogjakota *Computer Security Incident Response Team* (Jogjakota CSIRT);
- h. mengoordinasikan pelaporan insiden siber kepada Badan Siber dan Sandi Negara (BSSN) dan pemberitahuan/notifikasi kepada pengguna layanan TIK atau komunitas *Computer Security Incident Response Team* (CSIRT) lainnya apabila diperlukan untuk membantu melindungi dari serangan siber; dan
- i. melaporkan hasil pelaksanaan tugas kepada ketua pelaksana.

3. Tim Penanggulangan dan Pemulihan Insiden:
- a. menjadi narahubung untuk Jogjakota *Computer Security Incident Response Team* (Jogjakota CSIRT) dan melakukan tugas koordinasi apabila terjadi insiden siber;
 - b. menerima peringatan siber yang ditujukan untuk Jogjakota *Computer Security Incident Response Team* (Jogjakota CSIRT) dan memberikan peringatan siber ke *Computer Security Incident Response Team* lainnya;
 - c. melakukan penanggulangan dan pemulihan insiden secara cepat dan tepat;
 - d. melakukan tindakan korektif atas celah kerawanan (*vulnerability*) yang ditemukan;
 - e. melakukan pemeriksaan dan analisis terhadap artefak yang ditemukan;
 - f. memberitahukan hasil pengamatan potensi ancaman;
 - g. melakukan analisis risiko keamanan siber;
 - h. melakukan konsultasi terkait kesiapan penanganan Insiden Siber; dan/atau
 - i. melakukan pembangunan kesadaran dan kepedulian terhadap keamanan siber.

KELIMA : Tim sebagaimana dimaksud dalam Diktum KEEMPAT angka 3 dipimpin oleh seorang koordinator dan bertanggung jawab atas 3 (tiga) Sub Tim yang terdiri atas:

- a. Sub Tim Pengelola Jaringan dan *Server*;
- b. Sub Tim Keamanan Informasi; dan
- c. Sub Tim *Website* Administrator dan aplikasi.

KEENAM : Sub Tim Pengelola Jaringan dan *Server* sebagaimana dimaksud dalam Diktum KELIMA huruf a mempunyai tugas dan tanggung jawab:

- a. membuat dokumentasi jaringan yang beroperasi, berupa dokumentasi konfigurasi, dokumentasi lalu lintas normal (*baseline*) jaringan, dan dokumentasi performa jaringan;
- b. menyiapkan perangkat jaringan yang diperlukan untuk melakukan deteksi intrusi di jaringan dan analisa log di server;
- c. melakukan analisa log dan rekam digital lainnya pada jaringan dan server;
- d. menerapkan konsep keamanan pada konfigurasi jaringan dan meminimalisir celah keamanan di jaringan;
- e. melakukan pemantauan lalu lintas jaringan dan memeriksa apabila terdapat anomali di jaringan;

- f. melakukan tindakan korektif pada jaringan dan server sebagai solusi atas insiden siber maupun temuan celah keamanan;
- g. berkoordinasi dengan Internet Service Provider (ISP), jika diperlukan; dan
- h. menjadi tim teknis yang memberikan edukasi dan pelatihan.

KETUJUH : Sub Tim Keamanan Informasi sebagaimana dimaksud dalam Diktum KELIMA huruf b mempunyai tugas dan tanggung jawab:

- a. melakukan deteksi dan identifikasi serangan siber;
- b. melakukan triase insiden meliputi penilaian dampak dan prioritas insiden;
- c. melakukan analisis dan menemukan celah keamanan yang menjadi penyebab insiden siber;
- d. melakukan tindakan korektif untuk menanggulangi insiden siber;
- e. melakukan tindakan korektif berupa perbaikan celah keamanan (hardening) untuk mencegah insiden terulang kembali;
- f. melakukan pemeriksaan dan analisis terhadap artefak yang ditemukan;
- g. melakukan audit atau penilaian keamanan; dan
- h. menjadi tim teknis yang memberikan edukasi dan pelatihan.

KEDELAPAN : Sub Tim *Website Administrator* dan aplikasi sebagaimana dimaksud dalam Diktum KELIMA huruf c dipimpin oleh seorang koordinator dan mempunyai tugas dan tanggung jawab:

- a. melakukan pengelolaan terhadap konten website atau sistem informasi dan komunikasi lainnya;
- b. melakukan backup data secara berkala dan menyiapkan website cadangan sebagai solusi sementara apabila terjadi insiden siber;
- c. berkoordinasi dengan pengguna sistem informasi ketika insiden; dan
- d. melakukan tindakan korektif pada aplikasi sebagai solusi atas insiden siber maupun temuan celah keamanan.

KESEMBILAN : Dalam melaksanakan tugas, Ketua *Jogjakota Computer Security Incident Response Team* (Jogjakota CSIRT) bertanggung jawab kepada Wali Kota Yogyakarta.

KESEPULUH : Untuk kelancaran pelaksanaan tugas *Jogjakota Computer Security Incident Response Team* (Jogjakota CSIRT) dapat berkoordinasi dan bekerja sama dengan pihak lain sesuai dengan ketentuan peraturan perundang-undangan.

- KESEBELAS : Segala biaya yang timbul sebagai akibat ditetapkannya Keputusan Wali Kota ini dibebankan pada anggaran pendapatan dan belanja daerah Kota Yogyakarta.
- KEDUABELAS : Keputusan Wali Kota ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Yogyakarta
pada tanggal 27 Februari 2024

Pj. WALI KOTA YOGYAKARTA,



SINGGIH RAHARJO

Tembusan:

- Yth. 1. Inspektur inspektorat Kota Yogyakarta;
2. Kepala BPKAD Kota Yogyakarta; dan
3. Yang bersangkutan.
-

LAMPIRAN

KEPUTUSAN WALI KOTA YOGYAKARTA

NOMOR 143 TAHUN 2024

TENTANG

PEMBENTUKAN JOGJAKARTA
 COMPUTER SECURITY INCIDENT
 RESPONSE TEAM

SUSUNAN PERSONALIA

JOGJAKARTA COMPUTER SECURITY INCIDENT RESPONSE TEAM

NO.	JABATAN DALAM TIM	JABATAN DALAM INSTANSI
A.	Pengarah	
	I. Ketua	Wali Kota Yogyakarta
	II. Wakil Ketua	Sekretaris Daerah Kota Yogyakarta
	III. Anggota	Asisten Sekretaris Daerah Bidang Administrasi Umum
B.	Pelaksana	
	I. Ketua	Kepala Dinas Komunikasi Informatika dan Persandian Kota Yogyakarta
	II. Sekretaris	Sekretaris Dinas Komunikasi Informatika dan Persandian Kota Yogyakarta
	III. Koordinator Tim Penanggulangan dan Pemulihan Insiden	Kepala Bidang Persandian dan Telekomunikasi pada Dinas Komunikasi Informatika dan Persandian Kota Yogyakarta
	Sub Tim Pengelola Jaringan dan Server	
	a. Koordinator	Kepala Bidang Infrastruktur Telematika pada Dinas Komunikasi Informatika dan Persandian Kota Yogyakarta
	b. Anggota	Personil yang ditunjuk pada Bidang Infrastruktur Telematika Dinas Komunikasi Informatika dan Persandian Kota Yogyakarta
	Sub Tim Keamanan Informasi	
	a. Koordinator	Ketua Tim Kerja Pengamanan Informasi pada Dinas Komunikasi Informatika dan Persandian Kota Yogyakarta
	b. Anggota	Personil yang ditunjuk pada Tim Kerja Pengamanan Informasi Dinas Komunikasi Informatika dan Persandian Kota Yogyakarta

Sub Tim <i>Website Administrator</i> dan Aplikasi	
a. Koordinator	Kepala Bidang Sistem Informasi dan Statistik pada Dinas Komunikasi Informatika dan Persandian Kota Yogyakarta
b. Anggota	Personil yang ditunjuk pada Bidang Sistem Informasi dan Statistik Dinas Komunikasi Informatika dan Persandian Kota Yogyakarta

Pi. WALI KOTA YOGYAKARTA,



SINGGIH RAHARJO