WALI KOTA DEPOK
PROVINSI JAWA BARAT

KEPUTUSAN WALI KOTA DEPOK
NOMOR : 821.27/Kpts/Diskominfo/Huk/2024

TENTANG
PEMBENTUKAN *COMPUTER SECURITY INCIDENT RESPONSE TEAM*

WALI KOTA DEPOK,

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 berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Keputusan Wali Kota Depok tentang Pembentukan *Computer Security Incident Response Team*;

Mengingat :

1. Undang-Undang Nomor 15 Tahun 1999 tentang Pembentukan Kotamadya Daerah Tingkat II Depok dan Kotamadya Daerah Tingkat II Cilegon (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 49, Tambahan Lembaran Negara Republik Indonesia Nomor 3828);
2. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) 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 (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6736);

3. Undang-Undang...

3. 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 4834) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842);
4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
5. Peraturan Badan Siber Dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi Di Pemerintah Daerah;
6. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber;
7. Peraturan Daerah Kota Depok Nomor 10 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Depok (Lembaran Daerah Kota Depok Tahun 2016 Nomor 10) sebagaimana telah diubah dengan Peraturan Daerah Kota Depok Nomor 10 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Depok (Lembaran Daerah Kota Depok Tahun 2021 Nomor 4);

MEMUTUSKAN:

Menetapkan :

KESATU : Pembentukan *Computer Security Incident Response Team* yang selanjutnya disebut DEPOK-CSIRT, dengan susunan dan struktur sebagaimana tercantum dalam Lampiran I Keputusan Wali Kota ini.

KEDUA : Tugas dan tanggung jawab DEPOK-CSIRT sebagaimana dimaksud dalam Diktum KESATU, tercantum dalam Lampiran II Keputusan Wali Kota ini.

KETIGA : DEPOK-CSIRT sebagaimana dimaksud dalam Diktum KESATU mempunyai layanan berupa:

a. layanan reaktif, yaitu:
   1. pemberian peringatan siber (*alerts and warning*);
   2. penanggulangan dan pemulihan insiden siber (*incident handling*);
   3. penanganan kerawanan (*vulnerability handling*); dan
   4. penanganan artifak (*artifact handling*).
b. layanan proaktif yaitu audit atau penilaian keamanan (*security audit or assessment*);
c. layanan manajemen kualitas keamanan, yaitu:
   1. analisis risiko (*risk analysis*); dan
   2. edukasi dan pelatihan (*education/training*).

KETIGA : Dalam melaksanakan tugasnya DEPOK-CSIRT sebagaimana dimaksud dalam Diktum KESATU bertangggung jawab kepada Wali Kota Depok.

KEEMPAT : Segala biaya yang timbul sebagai akibat ditetapkannya Keputusan ini dibebankan pada Anggaran Pendapatan dan Belanja Daerah Kota Depok.

KELIMA…

KELIMA : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Depok
pada tanggal 5 Juli 2024

WALI KOTA DEPOK,

MOHAMMAD IDRIS

LAMPIRAN I KEPUTUSAN WALI KOTA DEPOK
NOMOR : 821.27/Kpts/Diskominfo/Huk/2024
TANGGAL : 5 Juli 2024

SUSUNAN *COMPUTER SECURITY INCIDENT RESPONSE TEAM*

I. Pengarah : Sekretaris Daerah Kota Depok.
II. Penanggung Jawab : Asisten Administrasi Umum Sekretariat Daerah Kota Depok.
III. Ketua : Kepala Dinas Komunikasi dan Informatika Kota Depok.
IV. Sekretaris : Sekretaris Dinas Komunikasi dan Informatika Kota Depok.
V. Tim Penanggulangan dan Pemulihan Insiden
Koordinator : Kepala Bidang Statistik dan Persandian pada Dinas Komunikasi Dan Informatika Kota Depok.

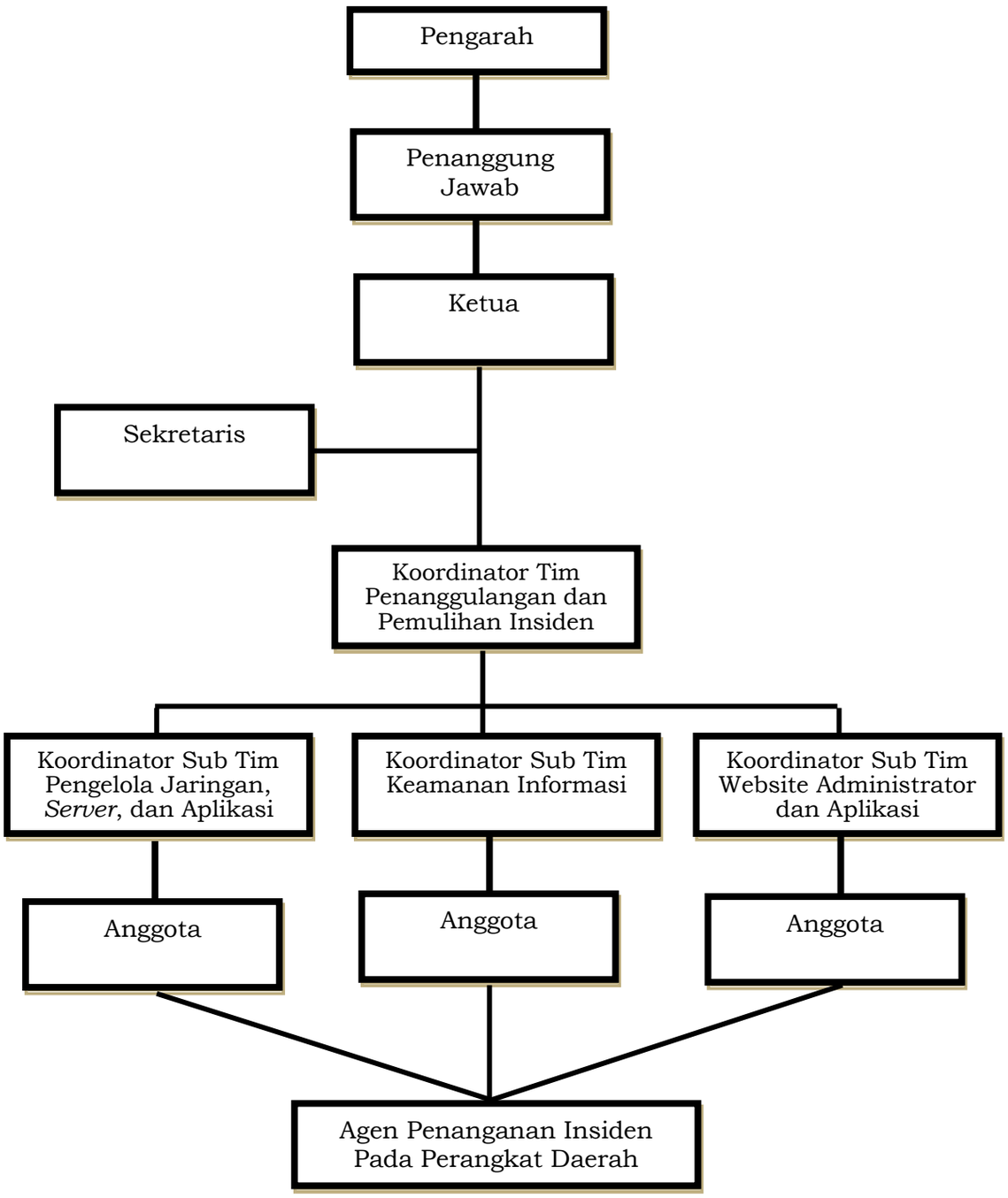
A. Sub Tim Pengelola Jaringan, *Server,* dan Aplikasi
1. Koordinator : Pranata Komputer Ahli Muda Bidang Aplikasi dan Informatika pada Dinas Komunikasi Dan Informatika Kota Depok.
2. Anggota : Pranata Komputer Bidang Aplikasi dan Informatika pada Dinas Komunikasi Dan Informatika Kota Depok.

B. Sub Tim Keamanan Informasi
1. Koordinator : Kepala Seksi Persandian
2. Anggota :
a. Pranata Komputer Bidang Statistik dan Persandian pada Dinas Komunikasi Dan Informatika Kota Depok; dan
b. Sandiman Bidang Statistik dan Persandian pada Dinas Komunikasi Dan Informatika Kota Depok.

C. Sub Tim Website Administrator dan Aplikasi
1. Koordinator : Kepala Bidang Aplikasi dan Infromatika pada Dinas Komunikasi Dan Informatika Kota Depok.
2. Anggota : Pranata Komputer Bidang Aplikasi dan Informatika pada Dinas Komunikasi Dan Informatika Kota Depok.

VI. Agen Penanganan Insiden Pada Perangkat Daerah:
Agen Transformasi Digital dari Setiap Perangkat Daerah.

STRUKTUR *COMPUTER SECURITY INCIDENT RESPONSE TEAM*



WALI KOTA DEPOK,

MOHAMMAD IDRIS

LAMPIRAN II KEPUTUSAN WALI KOTA DEPOK
NOMOR : 821.27/Kpts/Diskominfo/Huk/2024
TANGGAL : 5 Juli 2024

TUGAS DAN TANGGUNG JAWAB
COMPUTER SECURITY INCIDENT RESPONSE TEAM

I. Pengarah:
Memberikan pembinaan dan arahan kebijakan Penyelenggaraan DEPOK-CSIRT

II. Penanggungjawab:
Memberikan pertimbangan dalam penyusunan rencana Penyelenggaraan DEPOK-CSIRT

III. Ketua:
a. memimpin pelaksanaan tugas dan bertanggung jawab atas kegiatan Depok-CSIRT;
b. menyediakan *Point Of Contact* (POC) untuk Depok-CSIRT, berupa alamat email, nomor telepon, dan komunikasi lainnya;
c. bertanggung jawab dalam pengalokasian sumber daya yang dibutuhkan untuk mengoperasionalkan layanan Depok-CSIRT;
d. mengoordinasikan Depok-CSIRT dengan instansi dan pihak-pihak terkait lainnya dalam rangka pelaksanaan tugas dan fungsi Depok-CSIRT, serta menjalin kerja sama antar CSIRT;
e. memantau operasional dan kinerja Depok-CSIRT;
f. membuat perencanaan operasional dan strategis mengenai Depok-CSIRT;
g. mengoordinasikan edukasi dan pelatihan mengenai keamanan siber di lingkungan Depok-CSIRT; dan
h. menyusun dan menyampaikan laporan kepada Wali Kota Depok.

IV. Sekretaris:
a. melaksanakan fungsi kesekretariatan/ketatausahaan meliputi administrasi dan dokumentasi pada operasional layanan Depok -CSIRT;
b. membantu Ketua Depok-CSIRT dalam menjalankan tugas dan tanggung jawabnya; dan
c. menyelenggarakan rapat-rapat koordinasi.

V. Koordinator Tim Penanggulangan dan Pemulihan Insiden:
a. menjadi narahubung untuk Depok-CSIRT dan melakukan tugas koordinasi apabila terjadi insiden siber;
b. menerima peringatan siber yang ditujukan untuk Depok -CSIRT dan memberikan peringatan siber ke CSIRT 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 artifak yang ditemukan;
f. melakukan analisis risiko;
g. melakukan audit atau penilaian keamanan; dan
h. menjadi tim teknis yang memberikan edukasi dan pelatihan.

A. Sub Tim Pengelola Jaringan, *Server,* dan Aplikasi:
   1. membuat dokumentasi jaringan yang beroperasi, berupa dokumentasi konfigurasi, dokumentasi lalu lintas normal (*baseline*) jaringan, dan dokumentasi performa jaringan;
   2. menyiapkan perangkat jaringan yang diperlukan untuk melakukan deteksi intrusi di jaringan dan analisa log di *server*;
   3. melakukan analisa log dan rekam digital lainnya pada jaringan dan *server*;
   4. menerapkan konsep keamanan pada konfigurasi jaringan dan meminimalisir celah keamanan di jaringan;
   5. melakukan pemantauan lalu lintas jaringan dan memeriksa apabila terdapat anomali di jaringan;
   6. melakukan tindakan korektif pada jaringan dan *server* sebagai solusi atas insiden siber maupun temuan celah keamanan;
   7. berkoordinasi dengan *Internet Service Provider* (ISP), jika diperlukan; dan
   8. menjadi tim teknis yang memberikan edukasi dan pelatihan.

B. Sub Tim Keamanan Informasi:
   1. melakukan deteksi dan identifikasi serangan siber;
   2. melakukan triase insiden meliputi penilaian dampak dan prioritas insiden;
   3. melakukan analisis dan menemukan celah keamanan yang menjadi penyebab insiden siber;
   4. melakukan tindakan korektif untuk menanggulangi insiden siber;
   5. melakukan tindakan korektif berupa perbaikan celah keamanan (*hardening*) untuk mencegah insiden terulang kembali;
   6. melakukan pemeriksaan dan analisis terhadap artifak yang ditemukan;
   7. melakukan audit atau penilaian keamanan;
   8. melakukan analisis risiko; dan
   9. menjadi tim teknis yang memberikan edukasi dan pelatihan.

C. Sub Tim *Website Administrator* dan Aplikasi:
   1. melakukan pengelolaan terhadap *content* website atau sistem informasi dan komunikasi lainnya;
   2. melakukan *backup* data secara berkala dan menyiapkan *website* cadangan sebagai solusi sementara apabila terjadi insiden siber;
   3. berkoordinasi dengan pengguna sistem informasi ketika insiden;
   4. melakukan tindakan korektif pada aplikasi sebagai solusi atas insiden siber maupun temuan celah keamanan.

VI. Agen Penanganan Insiden Pada Perangkat Daerah:
Melakukan monitoring Keamanan Informasi yang terjadi pada masing-masing Perangkat Daerah di Pemerintah Kota Depok dan melaporkan kejadian Insiden Siber yang terjadi kepada Tim Penanggulangan dan Pemulihan Insiden DEPOK-CSIRT.

WALI KOTA DEPOK,

MOHAMMAD IDRIS