MENTERI
PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI
REPUBLIK INDONESIA

SALINAN

PERATURAN MENTERI PENDAYAGUNAAN APARATUR NEGARA DAN REFORMASI BIROKRASI REPUBLIK INDONESIA
NOMOR 6 TAHUN 2020
TENTANG
JABATAN FUNGSIONAL MANGGALA INFORMATIKA

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PENDAYAGUNAAN APARATUR NEGARA DAN REFORMASI BIROKRASI REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk melaksanakan pengembangan karier dan peningkatan profesionalisme pegawai negeri sipil dalam melaksanakan tugas di bidang Sistem Manajemen Keamanan Informasi, perlu menetapkan Jabatan Fungsional Manggala Informatika pada instansi pemerintah;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi tentang Jabatan Fungsional Manggala Informatika;

Mengingat : 1. Pasal 17 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916);

3. Undang-Undang Nomor 5 Tahun 2014 tentang Aparatur Sipil Negara (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 6, Tambahan Lembaran Negara Republik Indonesia Nomor 5494);
4. Peraturan Pemerintah Nomor 11 Tahun 2017 tentang Manajemen Pegawai Negeri Sipil (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 63, Tambahan Lembaran Negara Republik Indonesia Nomor 6037) sebagaimana telah diubah dengan Peraturan Pemerintah Nomor 17 Tahun 2020 tentang Perubahan Atas Peraturan Pemerintah Nomor 11 Tahun 2017 Tentang Manajemen Pegawai Negeri Sipil;
5. Peraturan Presiden Nomor 47 Tahun 2015 tentang Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 89);
6. Keputusan Presiden Nomor 87 Tahun 1999 tentang Rumpun Jabatan Fungsional Pegawai Negeri Sipil, sebagaimana telah diubah dengan Peraturan Presiden Nomor 97 Tahun 2012 tentang Perubahan atas Keputusan Presiden Nomor 87 Tahun 1999 tentang Rumpun Jabatan Fungsional Pegawai Negeri Sipil (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 235);
7. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 13 Tahun 2019 tentang Pengusulan, Penetapan, dan Pembinaan Jabatan Fungsional Pegawai Negeri Sipil (Berita Negara Republik Indonesia Tahun 2019 Nomor 834);

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI PENDAYAGUNAAN APARATUR NEGARA DAN REFORMASI BIROKRASI TENTANG JABATAN FUNGSIONAL MANGGALA INFORMATIKA

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

1. Pegawai Negeri Sipil yang selanjutnya disingkat PNS adalah warga negara Indonesia yang memenuhi syarat tertentu, diangkat sebagai Pegawai aparatur sipil negara secara tetap oleh pejabat pembina kepegawaian untuk menduduki jabatan pemerintahan.
2. Jabatan Fungsional adalah sekelompok jabatan yang berisi fungsi dan tugas berkaitan dengan pelayanan fungsional yang berdasarkan pada keahlian dan keterampilan tertentu.
3. Pejabat yang Berwenang yang selanjutnya disingkat PyB adalah pejabat yang mempunyai kewenangan melaksanakan proses pengangkatan, pemindahan, dan pemberhentian PNS sesuai dengan ketentuan peraturan perundang-undangan.
4. Pejabat Pembina Kepegawaian yang selanjutnya disingkat PPK adalah pejabat yang mempunyai kewenangan menetapkan pengangkatan, pemindahan dan pemberhentian PNS, dan pembinaan manajemen PNS di instansi pemerintah sesuai dengan ketentuan peraturan perundang-undangan.
5. Instansi Pemerintah adalah instansi pusat dan instansi daerah.
6. Instansi Pusat adalah kementerian, lembaga pemerintah nonkementerian, kesekretariatan lembaga negara, dan kesekretariatan lembaga nonstruktural.
7. Instansi Daerah adalah perangkat daerah provinsi dan perangkat daerah kabupaten/kota yang meliputi sekretariat daerah, sekretariat dewan perwakilan rakyat daerah, dinas daerah, dan lembaga teknis daerah.
8. Jabatan Fungsional Manggala Informatika adalah jabatan yang mempunyai ruang lingkup tugas, tanggung

jawab, dan wewenang untuk melaksanakan Sistem Manajemen Keamanan Informasi.

9. Pejabat Fungsional Manggala Informatika yang selanjutnya disebut Manggala Informatika adalah Pegawai PNS yang diberikan tugas, tanggungjawab, wewenang dan hak secara penuh oleh PyB untuk melakukan kegiatan Sistem Manajemen Keamanan Informasi di Instansi Pemerintah sesuai dengan ketentuan peraturan perundang-undangan.
10. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah bagian dari keseluruhan sistem manajemen organisasi untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara dan meningkatkan sistem keamanan informasi.
11. Sasaran Kinerja Pegawai yang selanjutnya disingkat SKP adalah rencana kinerja dan target yang akan dicapai oleh seorang PNS yang harus dicapai setiap tahun.
12. Angka Kredit adalah satuan nilai dari tiap butir kegiatan dan/atau akumulasi nilai butir-butir kegiatan yang harus dicapai oleh Manggala Informatika dalam rangka pembinaan karier yang bersangkutan.
13. Angka Kredit Kumulatif adalah akumulasi nilai angka kredit minimal yang harus dicapai oleh Manggala Informatika sebagai salah satu syarat kenaikan pangkat dan jabatan.
14. Tim Penilai Angka Kredit Jabatan Fungsional yang selanjutnya disebut Tim Penilai adalah tim yang dibentuk dan ditetapkan oleh PyB dan bertugas mengevaluasi keselarasan hasil kerja dengan tugas yang disusun dalam SKP serta menilai capaian kinerja pejabat fungsional dalam bentuk Angka Kredit Pejabat Fungsional.
15. Standar Kompetensi adalah standar kemampuan yang disyaratkan untuk dapat melakukan pekerjaan tertentu dalam bidang Sistem Manajemen Keamanan Informasi

yang menyangkut aspek pengetahuan, keterampilan dan/atau keahlian, serta sikap kerja tertentu yang relevan dengan tugas dan syarat jabatan.

16. Karya Tulis/Karya Ilmiah adalah tulisan hasil pokok pikiran, pengembangan, dan hasil kajian/penelitian yang disusun oleh Manggala Informatika baik perorangan atau kelompok di bidang Sistem Manajemen Keamanan Informasi.
17. Instansi Pembina Jabatan Fungsional Manggala Informatika yang selanjutnya disebut Instansi Pembina adalah Badan yang menyelenggarakan tugas di bidang siber dan sandi negara.
18. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan dibidang pendayagunaan aparatur negara.

BAB II
KEDUDUKAN, TANGGUNG JAWAB, DAN KLASIFIKASI/RUMPUN JABATAN

Bagian Kesatu
Kedudukan dan Tanggung Jawab

Pasal 2

(1) Manggala Informatika berkedudukan sebagai pelaksana teknis fungsional dibidang Sistem Manajemen Keamanan Informasi pada Instansi Pemerintah.
(2) Manggala Informatika sebagaimana dimaksud pada ayat (1) berkedudukan di bawah dan bertanggung jawab secara langsung kepada Pejabat Pimpinan Tinggi Madya, Pejabat Pimpinan Tinggi Pratama, Pejabat Administrator, atau Pejabat Pengawas yang memiliki keterkaitan dengan pelaksanaan tugas Jabatan Fungsional Manggala Informatika, ditetapkan dalam peta jabatan sesuai dengan ketentuan peraturan perundang-undangan.
(3) Kedudukan Manggala Informatika sebagaimana

dimaksud pada ayat (2) ditetapkan dalam peta jabatan berdasarkan analisis tugas dan fungsi unit kerja, analisis jabatan, dan analisis beban kerja dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan

Pasal 3

Jabatan Fungsional Manggala Informatika merupakan jabatan karier PNS.

Bagian Kedua

Klasifikasi/Rumpun Jabatan

Pasal 4

Jabatan Fungsional Manggala Informatika termasuk dalam klasifikasi/rumpun kekomputeran.

BAB III

KATEGORI DAN JENJANG JABATAN FUNGSIONAL

Pasal 5

(1) Jabatan Fungsional Manggala Informatika merupakan Jabatan Fungsional kategori keahlian.
(2) Jenjang Jabatan Fungsional Manggala Informatika sebagaimana dimaksud pada ayat (1), dari jenjang terendah sampai jenjang tertinggi, terdiri atas:
    a. Manggala Informatika Ahli Pertama;
    b. Manggala Informatika Ahli Muda;
    c. Manggala Informatika Ahli Madya; dan
    d. Manggala Informatika Ahli Utama.
(3) Jenjang pangkat Jabatan Fungsional Manggala Informatika sebagaimana dimaksud pada ayat (2), ditetapkan sesuai dengan ketentuan peraturan perundang-undangan tercantum dalam Lampiran III sampai dengan Lampiran V yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

BAB IV

TUGAS JABATAN, UNSUR DAN SUB-UNSUR KEGIATAN, URAIAN KEGIATAN TUGAS JABATAN, DAN HASIL KERJA

Bagian Kesatu

Tugas Jabatan

Pasal 6

Tugas Jabatan Fungsional Manggala Informatika yaitu melaksanakan kegiatan penerapan Sistem Manajemen Keamanan Informasi.

Bagian Kedua

Unsur dan Sub-Unsur Kegiatan

Pasal 7

Unsur utama kegiatan Jabatan Fungsional Manggala Informatika yang dapat dinilai Angka Kreditnya yaitu penerapan Sistem Manajemen Keamanan Informasi yang terdiri atas sub-unsur:

a. tata kelola keamanan informasi;
b. manajemen risiko keamanan informasi;
c. operasional keamanan informasi;
d. arsitektur keamanan informasi;
e. pengembangan sistem keamanan informasi;
f. tanggap darurat keamanan informasi;
g. bina kepatuhan dan pemantauan kinerja; dan
h. manajemen pengamanan keberlangsungan layanan teknologi informasi.

Bagian Ketiga

Uraian Kegiatan Sesuai Dengan Jenjang Jabatan

Pasal 8

(1) Uraian kegiatan Jabatan Fungsional Manggala Informatika sesuai dengan jenjang jabatannya, sebagai

berikut:

a. Manggala Informatika Ahli Pertama, meliputi:
    1. menerapkan prosedur akses data;
    2. menyusun prosedur *acceptable use* dalam mendukung kebijakan keamanan data;
    3. mengumpulkan data terkait prosedur pengelolaan data strategis;
    4. mengumpulkan data program peningkatan kesadaran dan kompetensi di bidang Sistem Manajemen Keamanan Informasi;
    5. menyiapkan forum diskusi dalam rangka program peningkatan kesadaran dan kompetensi di bidang Sistem Manajemen Keamanan Informasi;
    6. menyiapkan dokumen program peningkatan kesadaran dan kompetensi di bidang Sistem Manajemen Keamanan Informasi;
    7. mengumpulkan data atau bukti tentang kompetensi sumber daya manusia di bidang Sistem Manajemen Keamanan Informasi;
    8. menyiapkan bahan rancangan struktur organisasi penerapan Sistem Manajemen Keamanan Informasi berikut tugas pokok dan fungsinya;
    9. melakukan forum diskusi tentang struktur organisasi penerapan Sistem Manajemen Keamanan Informasi berikut tugas pokok dan fungsinya;
    10. menyiapkan koordinasi dalam rangka penerapan Sistem Manajemen Keamanan Informasi dengan satuan kerja lain;
    11. mengumpulkan data terkait standar (*template*) dokumen perjanjian kerahasiaan;
    12. membuat dokumen standar perjanjian kerahasiaan;
    13. mengumpulkan data terkait pemenuhan

persyaratan Sistem Manajemen Keamanan Informasi bagi pihak eksternal;

14. menginventarisasi aset;
15. mengidentifikasi penanggung jawab aset;
16. melakukan revisi dokumen penanggung jawab aset;
17. mengklasifikasi informasi;
18. melakukan penanganan informasi berdasarkan klasifikasi;
19. menyiapkan bahan tentang kebijakan dan prosedur pengendalian akses;
20. melakukan kegiatan pengendalian akses pengguna;
21. melakukan kegiatan pengendalian akses sistem informasi dan aplikasi;
22. mengidentifikasi pemberian dan penarikan hak akses aset informasi;
23. melakukan pemantauan pemberian dan penarikan hak akses aset informasi;
24. menyusun rencana evaluasi tingkat kepatuhan personil pihak ketiga terhadap kebijakan dan prosedur Sistem Manajemen Keamanan Informasi;
25. melakukan evaluasi tingkat kepatuhan personil pihak ketiga terhadap kebijakan dan prosedur Sistem Manajemen Keamanan Informasi;
26. menyiapkan bahan terkait prosedur pengamanan;
27. mengamankan akses fisik ke lokasi kerja;
28. mengumpulkan bahan terkait tata tertib Sistem Manajemen Keamanan Informasi di lokasi kerja dan ruangan peralatan komputer;
29. membuat dokumen tata tertib Sistem Manajemen Keamanan Informasi di lokasi kerja dan ruangan peralatan komputer;
30. menyiapkan bahan panduan pengamanan fisik

aset di lokasi kerja;

31. membuat panduan pengamanan fisik aset di lokasi kerja;
32. melakukan pengamanan fisik aset di lokasi kerja;
33. menerapkan kontrol keamanan untuk memenuhi rencana dan persyaratan keamanan fisik dan lingkungan;
34. mengumpulkan bahan panduan instalasi dan pemeliharaan infrastruktur, sistem dan peralatan pendukung;
35. membuat panduan instalasi dan pemeliharaan infrastruktur, sistem dan peralatan pendukung;
36. mengamankan instalasi dan pemeliharaan infrastruktur, sistem dan peralatan pendukung;
37. menyiapkan bahan prosedur pengelolaan aset;
38. membuat prosedur pengelolaan aset;
39. melakukan pengelolaan media;
40. menyiapkan bahan prosedur audit atau kaji-ulang tingkat efektifitas mitigasi risiko yang telah berjalan;
41. mengidentifikasi risiko dari aset;
42. membuat prosedur pengelolaan media;
43. membuat mekanisme enkripsi data;
44. mengelola penerapan mekanisme enkripsi data;
45. menyiapkan bahan prosedur keamanan jaringan;
46. melakukan penerapan standar konfigurasi keamanan pada sistem elektronik dan peralatan komunikasi;
47. membuat daftar induk Standar Operasional Prosedur (SOP) Sistem Manajemen Keamanan Informasi;
48. menyusun laporan kesiapan pengamanan terkait serah terima sistem elektronik ke dalam lingkup operasional;

49. menyusun pedoman pengendalian terhadap kode berbahaya;
50. menyusun Standar Operasional Prosedur (SOP) *back up* data dan sistem;
51. melakukan *back up* data dan sistem;
52. melakukan pengamanan atas layanan jaringan;
53. menyusun pedoman perlindungan informasi elektronik;
54. menyusun Standar Operasional Prosedur (SOP) pemantauan penggunaan sistem elektronik;
55. melakukan sinkronisasi waktu (NTP);
56. melakukan pengamanan peralatan;
57. menyediakan fasilitas pendukung untuk pengamanan informasi;
58. melakukan pengamanan sistem pengkabelan;
59. melakukan pemeliharaan peralatan;
60. melakukan prosedur pemindahan aset;
61. melakukan pengamanan peralatan yang berada di luar area kerja;
62. melakukan prosedur pemusnahan peralatan;
63. menyusun Standar Operasional Prosedur (SOP) *clear desk* dan *clean screen*;
64. melaksanakan prosedur *mobile computing*;
65. melakukan identifikasi protokol pertukaran informasi;
66. menyiapkan dokumen standar protokol pertukaran informasi;
67. menyusun dokumen kontrak dengan pihak ketiga yang memuat persyaratan Sistem Manajemen Keamanan Informasi;
68. menyusun dokumen kontrak yang memenuhi persyaratan Sistem Manajemen Keamanan Informasi pada penggunaan teknologi informasi dalam pengelolaan rantai pasokan (*supply chain*);
69. menerapkan kebijakan dan pedoman

penggunaan kriptografi;

70. menerapkan pedoman dan Standar Operasional Prosedur (SOP) penerapan manajemen kunci kriptografi;
71. melakukan pengelolaan terhadap gangguan, kegagalan dan kerugian atas penyelenggaraan sistem elektronik untuk pelayanan publik;
72. mengidentifikasi peraturan hukum yang berlaku terkait Sistem Manajemen Keamanan Informasi;
73. menerapkan pedoman penerapan hak kekayaan intelektual (HAKI);
74. menyusun Standar Operasional Prosedur (SOP) pengendalian rekaman (*evidence*) terhadap penyelenggaraan sistem elektronik;
75. menerapkan Standar Operasional Prosedur (SOP) pengendalian rekaman (*evidence*) terhadap penyelenggaraan sistem elektronik;
76. menyusun Standar Operasional Prosedur (SOP) perlindungan data pribadi;
77. menerapkan Standar Operasional Prosedur (SOP) perlindungan data pribadi;
78. menerapkan aturan tentang kontrol kriptografi;
79. melaksanakan kebijakan dan standar sistem manajemen pengamanan informasi;
80. membuat prosedur penanganan gangguan, kegagalan dan kerugian atas penyelenggaraan sistem elektronik untuk pelayanan publik;
81. membuat dan melaksanakan prosedur untuk menyediakan layanan sistem elektronik dalam kondisi darurat;
82. membuat prosedur untuk pemulihan layanan sistem elektronik;
83. mengidentifikasi peraturan perundang-undangan di bidang Sistem Manajemen Keamanan Informasi;

84. menyusun kompilasi peraturan perundang-undangan di bidang Sistem Manajemen Keamanan Informasi;
85. mengidentifikasi isu-isu aktual di bidang Sistem Manajemen Keamanan Informasi;
86. mengumpulkan data isu kebijakan di bidang Sistem Manajemen Keamanan Informasi;
87. membuat naskah akademis atas isu-isu kebijakan di bidang Sistem Manajemen Keamanan Informasi;
88. mengumpulkan data dan identifikasi isu-isu terkait penerapan kebijakan di bidang Sistem Manajemen Keamanan Informasi;
89. membuat *regulatory impact analysis* atas isu-isu kebijakan di bidang Sistem Manajemen Keamanan Informasi;
90. menyiapkan bahan *masterplan* atau *blueprint* di bidang Sistem Manajemen Keamanan Informasi;
91. menganalisis *masterplan* di bidang Sistem Manajemen Keamanan Informasi;
92. mengumpulkan bahan pemetaan keamanan informasi nasional;
93. mengumpulkan data terkait Norma, Standar, Prosedur dan Kriteria (NSPK) tata kelola keamanan informasi;
94. melaksanakan forum diskusi terkait dengan Norma, Standar, Prosedur dan Kriteria (NSPK) tata kelola keamanan informasi;
95. mengumpulkan data terkait Norma, Standar, Prosedur dan Kriteria (NSPK) pengamanan perangkat lunak;
96. mengumpulkan data terkait Norma, Standar, Prosedur dan Kriteria (NSPK) pengamanan perangkat keras;
97. mengumpulkan data terkait Norma, Standar,

Prosedur dan Kriteria (NSPK) tenaga ahli di bidang Sistem Manajemen Keamanan Informasi;

98. mengumpulkan data terkait Norma, Standar, Prosedur dan Kriteria (NSPK) sistem pengamanan;
99. menyiapkan bahan kegiatan bimbingan teknis;
100. membuat laporan pelaksanaan bimbingan teknis;
101. menyiapkan bahan kegiatan sosialisasi di bidang Sistem Manajemen Keamanan Informasi;
102. membuat laporan pelaksanaan sosialisasi di bidang Sistem Manajemen Keamanan Informasi;
103. memproses pendaftaran di bidang Sistem Manajemen Keamanan Informasi;
104. menyiapkan bahan kegiatan forum keamanan informasi nasional;
105. membuat laporan pelaksanaan forum keamanan informasi nasional;
106. menyiapkan bahan kegiatan diskusi publik atas regulasi di bidang Sistem Manajemen Keamanan Informasi;
107. mengadakan diskusi publik atas regulasi di bidang Sistem Manajemen Keamanan Informasi; dan
108. menyiapkan bahan *monitoring* dan evaluasi di bidang Sistem Manajemen Keamanan Informasi;

b. Manggala Informatika Ahli Muda, meliputi:
   1. mengidentifikasi persyaratan atau standar eksternal terkait penerapan Sistem Manajemen Keamanan Informasi;
   2. menganalisis aspek teknis dan fisik yang terkait dengan sumber daya manusia dan kontrol

keamanan informasi;

3. menyusun kebijakan dan standar operasional prosedur Sistem Manajemen Keamanan Informasi terhadap penyelenggaraan sistem elektronik untuk pelayanan publik sesuai dengan praktik terbaik (*best practices)*;
4. melaksanakan kebijakan dan SOP Sistem Manajemen Keamanan Informasi terhadap penyelenggaraan sistem elektronik untuk pelayanan publik sesuai dengan praktik terbaik (*best practices*);
5. melakukan analisis kinerja penerapan Sistem Manajemen Keamanan Informasi sesuai dengan parameter yang telah ditentukan;
6. menganalisis kesenjangan kondisi saat ini terhadap standar dan prosedur Sistem Manajemen Keamanan Informasi;
7. melaksanakan tindakan perbaikan sesuai dengan rekomendasi;
8. menyiapkan bahan kaji ulang kerangka kerja dalam rangka penyelenggaraan sistem elektronik untuk pelayanan publik;
9. mengidentifikasi kebijakan keamanan data terkait penerapan Sistem Manajemen Keamanan Informasi sesuai dengan tingkat risiko sistem elektronik;
10. menyusun kebijakan keamanan data terkait penerapan Sistem Manajemen Keamanan Informasi sesuai dengan tingkat risiko sistem elektronik;
11. menyusun prosedur otentikasi dan otorisasi akses data bagi pengguna;
12. melakukan evaluasi penerapan prosedur akses data;
13. melakukan evaluasi penerapan prosedur *acceptable use*;

14. menganalisis prosedur pengelolaan data strategis;
15. melaksanakan forum diskusi terkait prosedur pengelolaan data strategis;
16. membuat prosedur pengelolaan data strategis;
17. menganalisis kebutuhan program peningkatan kesadaran dan kompetensi di bidang Sistem Manajemen Keamanan Informasi;
18. melaksanakan kegiatan diseminasi informasi peningkatan kesadaran dan kompetensi bidang Sistem Manajemen Keamanan Informasi;
19. melakukan evaluasi efektivitas program kegiatan diseminasi informasi peningkatan kesadaran dan kompetensi bidang Sistem Manajemen Keamanan Informasi;
20. mengkaji materi peningkatan kesadaran dan kompetensi bidang Sistem Manajemen Keamanan Informasi;
21. menganalisis peningkatan kompetensi sumber daya manusia di bidang Sistem Manajemen Keamanan Informasi;
22. melakukan audit internal di bidang Sistem Manajemen Keamanan Informasi secara berkala;
23. mengidentifikasi persyaratan hukum dan peraturan di bidang Sistem Manajemen Keamanan Informasi;
24. menganalisis struktur organisasi penerapan Sistem Manajemen Keamanan Informasi berikut tugas pokok dan fungsinya;
25. menganalisis pemenuhan persyaratan Sistem Manajemen Keamanan Informasi bagi pihak eksternal;
26. menyusun dokumen Standar Operasional Prosedur (SOP) klasifikasi dan penanganan informasi;

27. melakukan evaluasi Standar Operasional Prosedur (SOP) klasifikasi dan penanganan informasi;
28. merumuskan peran dan tanggung jawab pegawai dan pihak ketiga;
29. melakukan sosialisasi peran dan tanggung jawab pegawai dan pihak ketiga;
30. membuat prosedur pengendalian akses;
31. mendiseminasikan prosedur pengendalian akses;
32. melakukan perubahan dokumen prosedur pengendalian akses;
33. menerapkan persyaratan bisnis untuk pengendalian akses;
34. memberikan rekomendasi persyaratan pada seleksi pegawai dan pihak ketiga dalam penerapan Sistem Manajemen Keamanan Informasi;
35. mengidentifikasi pelanggaran terhadap prosedur Sistem Manajemen Keamanan Informasi oleh pegawai atau personil pihak ketiga;
36. melakukan proses tindak lanjut terhadap pelanggaran prosedur Sistem Manajemen Keamanan Informasi oleh pegawai atau personil pihak ketiga;
37. menganalisis perimeter keamanan fisik;
38. membuat prosedur keamanan fisik;
39. menganalisis tata tertib Sistem Manajemen Keamanan Informasi di lokasi kerja dan ruangan peralatan komputer;
40. menganalisis panduan pengamanan fisik aset;
41. meninjau dan melakukan perubahan panduan pengamanan fisik aset;
42. mengidentifikasi persyaratan dan spesifikasi keamanan fisik;

43. membuat persyaratan dan spesifikasi keamanan fisik;
44. menganalisis risiko pada fasilitas fisik dan lingkungan;
45. menganalisis panduan instalasi dan pemeliharaan infrastruktur, sistem, dan peralatan pendukung;
46. menganalisis prosedur pengelolaan aset;
47. mengidentifikasi risiko terkait aspek teknis, fisik, sumber daya manusia dan prosedural terkait hubungan kerja dengan pihak ketiga;
48. membuat *risk register* terkait hubungan kerja dengan pihak ketiga;
49. menganalisis perubahan kerangka kerja dan strategi manajemen risiko;
50. mengkaji ulang tingkat efektifitas mitigasi risiko keamanan informasi;
51. menyusun tindakan perbaikan mitigasi risiko yang belum efektif;
52. menerapkan tindakan perbaikan mitigasi risiko yang belum efektif;
53. menyusun penilaian risiko keamanan informasi;
54. menyusun kajian risiko (*risk register*);
55. mengidentifikasi rencana mitigasi risiko;
56. menerapkan langkah mitigasi bersama pemilik risiko;
57. memvalidasi *risk register* termasuk langkah mitigasinya;
58. memverifikasi *risk register* termasuk langkah mitigasinya;
59. merencanakan proses analisa kerentanan dan pengujian penetrasi keamanan sistem informasi;
60. mengkoordinasikan proses analisa kerentanan dan pengujian penetrasi keamanan sistem

informasi;

61. menganalisis kerentanan penetrasi keamanan sistem elektronik;
62. melakukan penetrasi keamanan sistem elektronik;
63. membuat rekomendasi dan tindak lanjut terhadap hasil pengujian penetrasi keamanan sistem elektronik;
64. mengkaji keamanan informasi terhadap proses manajemen perubahan untuk memastikan perbaikan kerentanan;
65. melakukan diseminasi informasi terkait kerentanan, perbaikan atau mitigasi risiko yang telah diterapkan;
66. menerapkan pengendalian akses terhadap sistem operasi, aplikasi, dan jaringan;
67. memelihara pengendalian akses terhadap sistem operasi, aplikasi, dan jaringan;
68. menganalisis perimeter jaringan;
69. mendeteksi, menilai dan memonitor kerentanan dan ancaman keamanan jaringan;
70. memperbaiki kerentanan keamanan jaringan;
71. melaksanakan audit keamanan jaringan;
72. menganalisis prosedur keamanan jaringan dan sistem;
73. melaksanakan prosedur keamanan jaringan;
74. menganalisis laporan terkait adanya masalah keamanan (*anomali*);
75. menyusun uraian pemisahan tugas operasional;
76. menerapkan pemisahan fasilitas pengembangan, pengujian dan operasional;
77. mengidentifikasi keamanan layanan sistem elektronik;
78. memantau kinerja Sistem Manajemen Keamanan Informasi dalam pelaksanaan layanan pihak ketiga;

79. menyusun panduan pengelolaan perubahan terhadap layanan pihak ketiga;
80. menyusun panduan pengelolaan kapasitas sumber daya;
81. menyusun dokumentasi sistem infrastruktur dan aplikasi;
82. menyusun Standar Operasional Prosedur (SOP) pertukaran informasi;
83. menyusun Standar Operasional Prosedur (SOP) keamanan sistem elektronik untuk pelayanan publik;
84. membuat rekomendasi kebijakan keamanan informasi yang tersedia untuk umum atau publik;
85. menyusun panduan audit *log* sistem;
86. menyusun standar rekaman data *log* sistem;
87. menyusun kebijakan sinkronisasi waktu sistem elektronik;
88. menyusun prosedur perlindungan keamanan informasi terhadap perangkat yang ditinggal oleh penggunanya (*unattended user equipment*);
89. menyusun kebijakan *mobile computing*;
90. menyusun prosedur *teleworking*;
91. mengidentifikasi arsitektur keamanan informasi sesuai dengan standar internasional;
92. menyusun arsitektur keamanan informasi;
93. mengembangkan mekanisme dan standar keamanan informasi untuk mengamankan proses bisnis atau *platform* teknologi;
94. mengkaji kesesuaian penerapan protokol pertukaran informasi;
95. mengidentifikasi kebijakan keamanan informasi terkait hubungan dengan pihak ketiga;
96. melakukan pemantauan dan *review* layanan pihak ketiga;
97. mengelola perubahan terhadap layanan pihak

ketiga;

98. menganalisis persyaratan keamanan informasi dalam siklus hidup pengembangan sistem elektronik;
99. melakukan penerapan persyaratan Sistem Manajemen Keamanan Informasi terhadap layanan aplikasi pada jaringan publik;
100. melakukan penerapan persyaratan Sistem Manajemen Keamanan Informasi terhadap layanan transaksi pada aplikasi;
101. menyusun standar keamanan informasi terhadap pengembangan sistem elektronik;
102. menyusun prosedur kontrol perubahan sistem elektronik;
103. mengendalikan perubahan atas *software packages*;
104. menyusun *secure system engineering principle*;
105. mengkaji keamanan lingkungan pengembangan sistem elektronik;
106. menerapkan persyaratan Sistem Manajemen Keamanan Informasi dalam pengembangan aplikasi oleh pihak ketiga;
107. menguji fungsionalitas keamanan sistem elektronik;
108. menguji tingkat penerimaan sistem dan kriteria yang berhubungan dengan Sistem Manajemen Keamanan Informasi serta menyusun tindakan korektif yang diperlukan;
109. menyusun Standar Operasional Prosedur (SOP) perlindungan data uji sistem;
110. menyusun kebijakan dan pedoman penggunaan kriptografi;
111. menyusun panduan dan Standar Operasional Prosedur (SOP) penerapan manajemen kunci kriptografi;
112. membentuk pusat pengendalian terhadap

gangguan, kegagalan dan kerugian atas penyelenggaraan sistem elektronik untuk pelayanan publik;

113. mengelola pusat pengendalian terhadap gangguan, kegagalan dan kerugian atas penyelenggaraan sistem elektronik untuk pelayanan publik;
114. melakukan pengendalian terhadap gangguan, kegagalan dan kerugian atas penyelenggaraan sistem elektronik untuk pelayanan publik;
115. melakukan evaluasi upaya pengendalian terhadap gangguan, kegagalan dan kerugian atas penyelenggaraan sistem elektronik untuk pelayanan publik;
116. menyusun panduan penerapan Hak Kekayaan Intelektual (HAKI);
117. menyusun aturan tentang kontrol kriptografi;
118. analisis tingkat kepatuhan terhadap ketentuan internal dan eksternal;
119. menyusun kerangka kerja dan manajemen Keberlangsungan layanan sistem elektronik sesuai dengan persyaratan Sistem Manajemen Keamanan Informasi yang berlaku;
120. merancang, mengembangkan, dan menerapkan strategi keberlangsungan layanan dan rencana penanggulangan krisis atau bencana;
121. melakukan sosialisasi rencana keberlangsungan layanan sistem elektronik dan penanggulangan krisis atau bencana;
122. menerapkan proses yang menjamin kesiapan kemampuan sumber daya manusia dalam menjaga keberlangsungan layanan;
123. menyusun kebijakan terkait koordinasi untuk menjaga keberlangsungan dan pemulihan layanan dengan *stakeholder* terkait;
124. menyusun prosedur terkait koordinasi kegiatan

menjaga keberlangsungan dan pemulihan layanan dengan *stakeholder* terkait;

125. menganalisis peraturan perundang-undangan di bidang Sistem Manajemen Keamanan Informasi;
126. mengklasifikasikan peraturan perundang-undangan di bidang Sistem Manajemen Keamanan Informasi;
127. menganalisis isu aktual di bidang Sistem Manajemen Keamanan Informasi;
128. menyiapkan naskah rekomendasi kebijakan di bidang Sistem Manajemen Keamanan Informasi;
129. melaksanakan forum diskusi terkait dengan isu kebijakan di bidang Sistem Manajemen Keamanan Informasi;
130. menyusun naskah akademik di bidang Sistem Manajemen Keamanan Informasi;
131. melaksanakan forum diskusi terkait penyusunan naskah akademik di bidang Sistem Manajemen Keamanan Informasi;
132. menyusun naskah *Regulatory Impact Analysis* (RIA) di bidang Sistem Manajemen Keamanan Informasi;
133. melaksanakan forum diskusi terkait *masterplan* di bidang Sistem Manajemen Keamanan Informasi;
134. membuat dokumen *masterplan* keamanan informasi nasional;
135. menganalisis peta keamanan informasi nasional;
136. melaksanakan forum diskusi terkait dengan peta keamanan informasi nasional;
137. membuat peta keamanan informasi nasional;
138. menganalisis norma, standar, prosedur dan kriteria (NSPK) tata kelola keamanan informasi;

139. membuat norma, standar, prosedur dan kriteria (NSPK) tata kelola keamanan informasi;
140. menganalisis norma, standar, prosedur dan kriteria (NSPK) pengamanan perangkat lunak;
141. melaksanakan forum diskusi terkait dengan norma, standar, prosedur dan kriteria (NSPK) pengamanan perangkat lunak;
142. membuat norma, standar, prosedur dan kriteria (NSPK) pengamanan perangkat lunak;
143. menganalisis norma, standar, prosedur dan kriteria (NSPK) pengamanan perangkat keras;
144. melaksanakan forum diskusi terkait dengan norma, standar, prosedur dan kriteria (NSPK) pengamanan perangkat keras;
145. membuat norma, standar, prosedur dan kriteria (NSPK) pengamanan perangkat keras;
146. menganalisis norma, standar, prosedur dan kriteria (NSPK) tenaga ahli di bidang Sistem Manajemen Keamanan Informasi;
147. melaksanakan forum diskusi terkait dengan norma, standar, prosedur dan kriteria (NSPK) tenaga ahli di bidang Sistem Manajemen Keamanan Informasi;
148. membuat norma, standar, prosedur dan kriteria (NSPK) tenaga ahli di bidang Sistem Manajemen Keamanan Informasi;
149. menganalisis norma, standar, prosedur dan kriteria (NSPK) Sistem Manajemen Keamanan Informasi;
150. melaksanakan forum diskusi terkait dengan norma, standar, prosedur dan kriteria (NSPK) Sistem Manajemen Keamanan Informasi;
151. menyiapkan norma, standar, prosedur dan kriteria (NSPK) Sistem Manajemen Keamanan Informasi;
152. memberikan bimbingan teknis di bidang Sistem

Manajemen Keamanan Informasi;

153. melakukan uji kompetensi personil di bidang Sistem Manajemen Keamanan Informasi;
154. menyelenggarakan forum keamanan informasi nasional; dan
155. melakukan *monitoring* dan evaluasi di bidang Sistem Manajemen Keamanan Informasi;

c. Manggala Informatika Ahli Madya, meliputi:
   1. mengidentifikasi dan menganalisis risiko keamanan informasi terkait dengan penyelenggaraan sistem elektronik untuk pelayanan publik di sektor terkait;
   2. mengumpulkan dan mengkaji data referensi dan hasil pengelolaan keamanan informasi pada instansi;
   3. menyusun rencana kerja induk jangka menengah atau panjang terkait pengelolaan keamanan informasi nasional;
   4. menyusun sasaran dan target kinerja utama Sistem Manajemen Keamanan Informasi di sektor terkait;
   5. merencanakan pemantauan pelaksanaan keamanan informasi di instansi;
   6. melakukan evaluasi pelaksanaan Sistem Manajemen Keamanan Informasi di semua area terkait;
   7. merencanakan pengukuran efektifitas dan efisiensi keamanan informasi di instansi;
   8. mengukur efektifitas dan efisiensi keamanan informasi di setiap area;
   9. membuat rencana analisis tingkat kematangan penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;
   10. mengukur tingkat kematangan keamanan informasi di setiap area;
   11. mengidentifikasi dan menganalisis risiko

sistem elektronik untuk pelayanan publik di sektor terkait;

12. mengidentifikasi permasalahan dan kebutuhan keamanan informasi penerapan Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;
13. mengkaji kebutuhan keamanan informasi dan standar teknis perlindungan informasi infrastruktur yang kritikal (*critical information infrastructure*) di sektor strategis terkait;
14. mengumpulkan dan mengkaji rencana kerja induk jangka menengah dan panjang terkait Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;
15. merencanakan konsultasi kepada jabatan fungsional manggala informatika satu tingkat dibawahnya;
16. melakukan konsultasi kepada jabatan fungsional manggala informatika satu tingkat dibawahnya;
17. merencanakan evaluasi kompetensi dan kinerja jabatan fungsional manggala informatika satu tingkat dibawahnya;
18. melakukan evaluasi kompetensi dan kinerja jabatan fungsional manggala informatika satu tingkat dibawahnya;
19. membuat rencana kegiatan diseminasi regulasi di bidang Sistem Manajemen Keamanan Informasi;
20. mengkaji materi diseminasi regulasi di bidang Sistem Manajemen Keamanan Informasi;
21. melakukan evaluasi kegiatan diseminasi regulasi di bidang Sistem Manajemen Keamanan Informasi;

22. mengidentifikasi program peningkatan kinerja Sistem Manajemen Keamanan Informasi terhadap penyelenggaraan sistem elektronik untuk pelayanan publik;
23. menganalisis dan menyusun program peningkatan kinerja Sistem Manajemen Keamanan Informasi terhadap penyelenggaraan sistem elektronik untuk pelayanan publik;
24. melakukan evaluasi program peningkatan kinerja Sistem Manajemen Keamanan Informasi terhadap penyelenggaraan sistem elektronik untuk pelayanan publik;
25. menyusun kerangka kerja di bidang Sistem Manajemen Keamanan Informasi;
26. mengidentifikasi sasaran kinerja Sistem Manajemen Keamanan Informasi dalam rangka penyelenggaraan sistem elektronik untuk pelayanan publik;
27. mengidentifikasi mekanisme pengukuran sasaran kinerja Sistem Manajemen Keamanan Informasi dalam rangka penyelenggaraan sistem elektronik untuk pelayanan publik;
28. mengkaji ulang kerangka kerja Sistem Manajemen Keamanan Informasi dalam rangka penyelenggaraan sistem elektronik untuk pelayanan publik;
29. mengkaji kepatuhan kebijakan di bidang Sistem Manajemen Keamanan Informasidi instansi terhadap hukum dan peraturan terkait lainnya;
30. melakukan evaluasi kepatuhan kebijakan Sistem Manajemen Keamanan Informasi di instansi terhadap hukum dan peraturan terkait lainnya;
31. melakukan evaluasi kebijakan Sistem

Manajemen Keamanan Informasi untuk mematuhi semua undang-undang dan peraturan perlindungan data pribadi;

32. merancang struktur organisasi penerapan Sistem Manajemen Keamanan Informasi berikut tugas pokok dan fungsinya;
33. menyusun dokumen pemenuhan persyaratan Sistem Manajemen Keamanan Informasi pihak eksternal;
34. meninjau proyek konstruksi fisik agar sesuai dengan kontrol keamanan fisik dan lingkungan;
35. melakukan evaluasi efektifitas kebijakan dan prosedur keamanan fisik dan lingkungan serta membuat rekomendasi untuk perbaikan yang diperlukan;
36. melakukan evaluasi proses pengadaan yang memiliki implikasi terhadap keamanan fisik;
37. menilai akurasi dan efektivitas pengukuran kinerja sistem keamanan fisik, dan membuat rekomendasi untuk perbaikannya;
38. meninjau dokumen panduan instalasi dan pemeliharaan infrastruktur, sistem, dan peralatan pendukung;
39. meninjau dokumen kebijakan dan prosedur pengelolaan aset;
40. melakukan evaluasi terhadap pihak ketiga terkait tingkat kepatuhan Sistem Manajemen Keamanan Informasi sesuai dengan kesepakatan;
41. menyusun strategi manajemen risiko keamanan informasi;
42. menerapkan strategi manajemen risiko keamanan informasi;
43. menyesuaikan strategi manajemen risiko keamanan informasi untuk menindaklanjuti

perubahan pada kondisi dan lingkungan instansi;

44. mengkaji ulang tingkat efektifitas mitigasi risiko keamanan informasi yang telah berjalan;
45. memantau proses penerapan mitigasi risiko keamanan informasi dan proses perbaikan yang diperlukan;
46. memeriksa adanya kerentanan baru terkait aspek teknis, keamanan fisik, sumber daya manusia dan prosedur operasional;
47. merespon terhadap adanya kerentanan baru terkait aspek teknis, keamanan fisik, sumber daya manusia dan prosedur operasional;
48. melakukan pemantauan tingkat kepatuhan secara kontinu terhadap prosedur pengelolaan media;
49. menguji efektifitas teknologi keamanan jaringan;
50. melakukan keamanan jaringan komunikasi elektronik yang bersifat rahasia dari gangguan dan penyadapan;
51. membuat laporan kinerja keamanan jaringan;
52. meninjau atau menyesuaikan kebijakan dan prosedur keamanan jaringan;
53. melakukan evaluasi proses operasional untuk mengidentifikasi pelanggaran kebijakan Sistem Manajemen Keamanan Informasi;
54. mengintegrasikan solusi arsitektur keamanan dengan arsitektur teknologi informasi;
55. mengkaji kesesuaian penerapan arsitektur keamanan informasi;
56. mengusulkan perbaikan ataupun perubahan terhadap arsitektur keamanan informasi;
57. merancang mekanisme, komponen dan teknologi keamanan informasi;
58. mengembangkan metodologi untuk evaluasi

kelaikan langkah-langkah mitigasi risiko yang diterapkan dalam sistem elektronik;

59. menilai tingkat efektifitas dan kehandalan keamanan sistem, mekanisme, dan produk;
60. menyusun dan menerapkan proses dan fungsi manajemen keberlangsungan layanan sistem elektronik;
61. menguji dan mengevaluasi rencana keberlangsungan layanan sistem elektronik;
62. menganalisis dampak terjadinya kondisi darurat dan menyusun *recovery time objective* (RTO) dan *recovery point objective* (RPO) yang sesuai dengan kebutuhan instansi;
63. menganalisis asas-manfaat untuk penerapan kontrol keamanan informasi baru;
64. mengevaluasi hasil uji-coba rencana keberlangsungan layanan sistem elektronik;
65. melakukan pengukuran efektifitas rencana keberlangsungan layanan sistem elektronik, dan menyusun langkah perbaikan;
66. memastikan seluruh komponen infrastruktur dan fasilitas pemulihan layanan sistem elektronik dapat berfungsi dengan baik; dan
67. melakukan pembinaan sumber daya manusia di bidang Sistem Manajemen Keamanan Informasi; dan

d. Manggala Informatika Ahli Utama, meliputi:
    1. mengembangkan kebijakan manajemen risiko keamanan informasi terkait dengan penyelenggaraan sistem elektronik untuk pelayanan publik di sektor terkait;
    2. merumuskan dan mengevaluasi kebijakan mitigasi risiko keamanan informasi terkait dengan penyelenggaraan sistem elektronik untuk pelayanan publik di sektor terkait;
    3. membuat rekomendasi hasil kajian risiko

keamanan informasi keamanan informasi terkait dengan penyelenggaraan sistem elektronik untuk pelayanan publik di sektor terkait;

4. membuat desain strategi dan kebijakan Sistem Manajemen Keamanan Informasidi sektor terkait;
5. membuat rekomendasi strategi dan kebijakan Sistem Manajemen Keamanan Informasi di sektor terkait;
6. melakukan koordinasi penyusunan rencana kerja induk Sistem Manajemen Keamanan Informasi di sektor terkait;
7. melakukan analisis sasaran dan target kinerja utama Sistem Manajemen Keamanan Informasi di sektor terkait;
8. melakukan evaluasi penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;
9. melakukan evaluasi tingkat efektifitas dan efisiensi penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;
10. menganalisis tingkat kematangan penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;
11. menyusun kerangka kerja manajemen risiko keamanan informasi terhadap penyelenggaraan sistem elektronik untuk pelayanan publik di sektor terkait;
12. mengevaluasidan menyusun mitigasi risiko keamanan informasi terhadap penyelenggaraan sistem elektronik untuk pelayanan publik di sektor terkait;
13. merumuskan hasil kajian risiko keamanan informasi terhadap penyelenggaraan sistem elektronik untuk pelayanan publik di sektor

terkait;

14. mengidentifikasi dan menganalisis sistem elektronik strategis untuk pelayanan publik di sektor terkait;
15. menyusun kerangka kerja penerapan Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;
16. menyusun strategi penerapan Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;
17. melakukan koordinasi penerapan Sistem Manajemen Keamanan Informasi dengan organisasi lainnya baik dalam maupun luar negeri;
18. mengevaluasi dan membuat rekomendasi hasil koordinasi terkait penerapan Sistem Manajemen Keamanan Informasi dengan organisasi lainnya baik dalam maupun luar negeri;
19. menyusun persyaratan teknis kelaikan sistem elektronik strategis untuk pelayanan publik di sektor terkait;
20. melakukan penyusunan konsep rencana kerja induk jangka menengah dan panjang terkait Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;
21. menyusun rencana kerja induk jangka menengah dan panjang terkait Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;
22. menyusun rencana evaluasi penerapan Sistem Manajemen Keamanan Informasi pada sistem

elektronik strategis untuk pelayanan publik di sektor terkait;

23. melakukan evaluasi penerapan Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;
24. merencanakan penilaian tingkat kematangan penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;
25. melakukan analisis tingkat kematangan penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;
26. melakukan validasi hasil analisis tingkat kematangan tingkat kematangan penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;
27. melakukan koordinasi mekanisme pelaporan terjadinya gangguan, kegagalan dan kerugian penyelenggaraan sistem elektronik untuk pelayanan publik dalam sektor terkait;
28. merencanakan kegiatan peningkatan kepedulian pengamanan penyelenggaraan sistem elektronik di sektor terkait;
29. melaksanakan kegiatan peningkatan kepedulian pengamanan penyelenggaraan sistem elektronik di sektor terkait;
30. mengidentifikasi permasalahan dan menganalisis terkait pengamanan penyelenggaraan sistem elektronik yang bersifat strategis;
31. menyusun rencana konsultasi terkait pengamanan penyelenggaraan sistem elektronik yang bersifat strategis;
32. melakukan konsultasi terkait pengamanan penyelenggaraan sistem elektronik yang bersifat strategis;

33. mengevaluasi hasil konsultasi terkait pengamanan penyelenggaraan sistem elektronik yang bersifat strategis;
34. merencanakan penelitian dan pengembangan model atau kerangka kerja baru terkait Sistem Manajemen Keamanan Informasi;
35. melakukan koordinasi dengan *stakeholder* terkait dalam rangka penelitian dan pengembangan model atau kerangka kerja baru tentang Sistem Manajemen Keamanan Informasi; dan
36. membuat model atau kerangka kerja baru terkait Sistem Manajemen Keamanan Informasi.

(2) Manggala Informatika yang melaksanakan kegiatan sebagaimana dimaksud pada ayat (1) diberikan nilai Angka Kredit tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

(3) Rincian kegiatan masing-masing jenjang jabatan sebagaimana dimaksud pada ayat (1) diatur oleh Instansi Pembina.

Bagian Keempat

Hasil Kerja

Pasal 9

Hasil kerja tugas jabatan bagi Jabatan Fungsional Manggala Informatika sesuai dengan jenjang jabatannya adalah sebagai berikut:

a. Manggala Informatika Ahli Pertama, meliputi:
    1. laporan penerapan prosedur akses data;
    2. dokumen prosedur *acceptable use*;
    3. data dan informasi terkait prosedur pengelolaan data strategis;
    4. data dan informasi program peningkatan kesadaran

dan kompetensi di bidang Sistem Manajemen Keamanan Informasi;

5. laporan forum diskusi peningkatan kesadaran dan kompetensi di bidang Sistem Manajemen Keamanan Informasi;
6. dokumen program peningkatan kesadaran dan kompetensi di bidang Sistem Manajemen Keamanan Informasi;
7. data atau bukti kompetensi di bidang Sistem Manajemen Keamanan Informasi;
8. rancangan struktur organisasi penerapan Sistem Manajemen Keamanan Informasi berikut tugas pokok dan fungsinya;
9. laporan pelaksanaan forum diskusi tentang struktur organisasi penerapan Sistem Manajemen Keamanan Informasi berikut tugas pokok dan fungsinya;
10. laporan koordinasi untuk penerapan Sistem Manajemen Keamanan Informasi dengan satuan kerja lain;
11. data dan informasi terkait standar perjanjian kerahasiaan;
12. dokumen standar perjanjian kerahasiaan;
13. data terkait pemenuhan persyaratan Sistem Manajemen Keamanan Informasi bagi pihak eksternal;
14. daftar inventaris aset (informasi, perangkat keras, perangkat lunak, personil dan sebagainya);
15. data dan informasi terkait penanggung jawab aset;
16. dokumen perubahan penanggung jawab aset;
17. dokumen klasifikasi informasi;
18. laporan kegiatan penanganan informasi;
19. bahan kebijakan dan prosedur pengendalian akses;
20. laporan pengendalian akses pengguna;
21. laporan pengendalian akses sistem dan aplikasi;
22. dokumen identifikasi pemberian dan penarikan hak akses aset informasi;

23. laporan pemantauan pemberian dan penarikan hak akses aset informasi;
24. rencana evaluasi tingkat kepatuhan personil pihak ketiga terhadap kebijakan dan prosedur Sistem Manajemen Keamanan Informasi;
25. laporan evaluasi tingkat kepatuhan personil pihak ketiga terhadap kebijakan dan prosedur Sistem Manajemen Keamanan Informasi;
26. bahan terkait prosedur pengamanan;
27. laporan keamanan akses fisik;
28. bahan tentang tata tertib Sistem Manajemen Keamanan Informasi di lokasi kerja dan ruangan peralatan komputer;
29. dokumen tata tertib Sistem Manajemen Keamanan Informasi di lokasi kerja dan ruangan peralatan komputer;
30. bahan panduan pengamanan fisik aset di lokasi kerja;
31. panduan pengamanan fisik aset di lokasi kerja;
32. laporan pelaksanaan pengamanan fisik aset di lokasi kerja;
33. laporan penerapan kontrol keamanan fisik dan lingkungan;
34. bahan panduan instalasi dan pemeliharaan infrastruktur, sistem dan peralatan pendukung;
35. panduan instalasi dan pemeliharaan infrastruktur, sistem dan peralatan pendukung;
36. laporan pengamanan instalasi dan pemeliharaan infrastruktur, sistem dan peralatan pendukung;
37. bahan prosedur pengelolaan aset;
38. dokumen prosedur pengelolaan aset;
39. laporan pengelolaan media (*media handling*);
40. bahan prosedur audit atau kaji-ulang tingkat efektifitas mitigasi risiko yang telah berjalan;
41. daftar risiko dari aset;
42. dokumen prosedur pengelolaan media (*universal*

serial bus, removeable storage dan lain-lain);

43. dokumen standar dan prosedur mekanisme enkripsi data;
44. laporan penerapan mekanisme enkripsi data;
45. bahan prosedur keamanan jaringan;
46. laporan penerapan standar konfigurasi keamanan pada sistem elektronik dan peralatan komunikasi;
47. daftar induk Standar Operasional Prosedur (SOP) Sistem Manajemen Keamanan Informasi;
48. laporan kesiapan pengamanan terkait serah terima sistem elektronik ke dalam lingkup operasional;
49. pedoman pengendalian terhadap kode berbahaya;
50. dokumen Standar Operasional Prosedur (SOP) *back up* data dan sistem;
51. laporan *back up* data dan sistem;
52. laporan pengamanan atas layanan jaringan;
53. pedoman perlindungan informasi elektronik;
54. Standar Operasional Prosedur (SOP) pemantauan penggunaan sistem elektronik;
55. laporan pelaksanaan sinkronisasi waktu sistem elektronik;
56. laporan pengamanan peralatan;
57. laporan ketersediaan fasilitas pendukung untuk pengamanan informasi;
58. laporan pengamanan sistem pengkabelan;
59. laporan pemeliharaan peralatan;
60. laporan penerapan prosedur pemindahan aset;
61. laporan pengamanan peralatan yang berada di luar area kerja;
62. laporan prosedur pemusnahan peralatan;
63. Standar Operasional Prosedur (SOP) *clear desk* dan *clean screen*;
64. laporan pelaksanaan prosedur *mobile computing*;
65. dokumen bahan standar protokol pertukaran informasi;
66. dokumen standar protokol pertukaran informasi;

67. dokumen kontrak pihak ketiga yang memuat persyaratan Sistem Manajemen Keamanan Informasi;
68. dokumen kontrak yang memenuhi persyaratan keamanan informasi pada penggunaan teknologi informasi dalam pengelolaan rantai pasokan (*supply chain*);
69. laporan penerapan kebijakan dan pedoman penggunaan kriptografi;
70. laporan penerapan manajemen kunci kriptografi;
71. laporan pengelolaan terhadap gangguan, kegagalan dan kerugian atas penyelenggaraan sistem elektronik untuk pelayanan publik;
72. laporan identifikasi peraturan hukum yang berlaku;
73. laporan penerapan hak kekayaan intelektual (HAKI);
74. dokumen Standar Operasional Prosedur (SOP) pengendalian rekaman (*evidence*) terhadap penyelenggaraan sistem elektronik;
75. laporan penerapan Standar Operasional Prosedur (SOP) pengendalian rekaman (*evidence*) terhadap penyelenggaraan sistem elektronik;
76. standar operasional prosedur (SOP) perlindungan data pribadi;
77. laporan penerapan perlindungan data pribadi;
78. laporan penerapan aturan tentang kontrol kriptografi;
79. laporan pelaksanaan kebijakan dan standar Sistem Manajemen Keamanan Informasi;
80. dokumen prosedur penanganan gangguan, kegagalan dan kerugian atas penyelenggaraan sistem elektronik untuk pelayanan publik;
81. dokumen prosedur untuk menyediakan layanan sistem elektronik dalam kondisi darurat;
82. dokumen prosedur untuk pemulihan layanan sistem elektronik;
83. daftar peraturan perundang-undangan di bidang Sistem Manajemen Keamanan Informasi;
84. kompilasi peraturan perundang-undangan di bidang

Sistem Manajemen Keamanan Informasi;

85. laporan identifikasi isu aktual di bidang Sistem Manajemen Keamanan Informasi;
86. data dan informasi mengenai isu kebijakan di bidang Sistem Manajemen Keamanan Informasi;
87. laporan *desk study* isu-isu kebijakan di bidang Sistem Manajemen Keamanan Informasi;
88. data dan informasi mengenai isu terkait penerapan kebijakan di bidang Sistem Manajemen Keamanan Informasi;
89. laporan *desk study*;
90. data dan informasi mengenai *masterplan*/*blueprint* di bidang Sistem Manajemen Keamanan Informasi;
91. hasil analisis *masterplan* di bidang Sistem Manajemen Keamanan Informasi;
92. data dan informasi mengenai peta keamanan informasi nasional;
93. data dan informasi mengenai NSPK tata kelola;
94. pendapat ahli terkait dengan NSPK tata kelola;
95. data dan informasi mengenai NSPK Perangkat Lunak;
96. data dan informasi mengenai NSPK Perangkat Keras;
97. data dan informasi mengenai NSPK Tenaga Ahli di bidang Sistem Manajemen Keamanan Informasi;
98. data dan informasi mengenai NSPK Sistem Pengamanan;
99. bahan kegiatan bimbingan teknis di bidang Sistem Manajemen Keamanan Informasi;
100. laporan kegiatan bimbingan teknis di bidang Sistem Manajemen Keamanan Informasi;
101. bahan kegiatan seminar di bidang Sistem Manajemen Keamanan Informasi;
102. laporan kegiatan seminar di bidang Sistem Manajemen Keamanan Informasi;
103. daftar peserta tenaga ahli dan auditor yang lulus sertifikasi (*white list*);
104. bahan kegiatan Forum Keamanan Informasi

Nasional;

105. laporan pelaksanaan Forum Keamanan Informasi Nasional;
106. bahan kegiatan diskusi publik atas regulasi di bidang Sistem Manajemen Keamanan Informasi;
107. laporan diskusi publik atas regulasi di bidang Sistem Manajemen Keamanan Informasi; dan
108. bahan kegiatan *monitoring* dan evaluasi di bidang Sistem Manajemen Keamanan Informasi;

b. Manggala Informatika Ahli Muda, meliputi:
   1. dokumen persyaratan atau standar eksternal;
   2. dokumen analisis aspek teknis dan fisik yang terkait dengan sumber daya manusia dan kontrol keamanan informasi;
   3. dokumen kebijakan dan standar operasional prosedur Sistem Manajemen Keamanan Informasi;
   4. laporan pelaksanaan kebijakan dan standar operasional prosedur Sistem Manajemen Keamanan Informasi;
   5. laporan analisis kinerja penerapan Sistem Manajemen Keamanan Informasi sesuai dengan parameter yang telah ditentukan;
   6. laporan hasil analisis kesenjangan kondisi saat ini terhadap standar dan prosedur Sistem Manajemen Keamanan Informasi;
   7. laporan pelaksanaan tindakan perbaikan sesuai dengan rekomendasi;
   8. bahan kaji ulang kerangka kerja keamanan informasi;
   9. laporan identifikasi kebijakan keamanan data terkait penerapan Sistem Manajemen Keamanan Informasi sesuai dengan tingkat risiko sistem elektronik;
   10. kebijakan keamanan data terkait penerapan Sistem Manajemen Keamanan Informasi sesuai dengan tingkat risiko sistem elektronik;
   11. dokumen prosedur otentikasi dan otorisasi akses bagi pengguna;

12. laporan evaluasi penerapan prosedur akses data;
13. laporan evaluasi penerapan prosedur *acceptable use*;
14. laporan analisis prosedur pengelolaan data strategis;
15. laporan forum diskusi terkait prosedur pengelolaan data strategis;
16. dokumen prosedur pengelolaan data strategis;
17. laporan analisis kebutuhan program peningkatan kesadaran dan kompetensi di bidang Sistem Manajemen Keamanan Informasi;
18. laporan pelaksanaan diseminasi informasi peningkatan kesadaran dan kompetensi bidang Sistem Manajemen Keamanan Informasi;
19. laporan evaluasi efektivitas diseminasi informasi peningkatan kesadaran dan kompetensi bidang Sistem Manajemen Keamanan Informasi;
20. materi peningkatan kesadaran dan kompetensi bidang Sistem Manajemen Keamanan Informasi;
21. laporan analisis peningkatan kompetensi sumber daya manusia di bidang Sistem Manajemen Keamanan Informasi;
22. laporan audit internal di bidang Sistem Manajemen Keamanan Informasi;
23. dokumen persyaratan hukum dan peraturan di bidang Sistem Manajemen Keamanan Informasi;
24. laporan hasil analisis struktur organisasi penerapan Sistem Manajemen Keamanan Informasi berikut tugas pokok dan fungsinya;
25. dokumen hasil analisis pemenuhan persyaratan Sistem Manajemen Keamanan Informasibagi pihak eksternal;
26. dokumen Standar Operasional Prosedur (SOP) klasifikasi dan penanganan informasi;
27. laporan evaluasi Standar Operasional Prosedur (SOP) klasifikasi dan penanganan informasi;
28. dokumen peran dan tanggung jawab pegawai dan pihak ketiga;

29. laporan sosialisasi dokumen peran dan tanggung jawab pegawai dan pihak ketiga;
30. dokumen prosedur pengendalian akses;
31. laporan diseminasi prosedur pengendalian akses;
32. dokumen perubahan prosedur pengendalian akses;
33. laporan penerapan persyaratan bisnis untuk pengendalian akses;
34. rekomendasi persyaratan pada seleksi pegawai dan pihak ketiga dalam penerapan Sistem Manajemen Keamanan Informasi;
35. laporan identifikasi pelanggaran terhadap prosedur Sistem Manajemen Keamanan Informasi oleh pegawai atau personil pihak ketiga;
36. laporan tindak lanjut terhadap pelanggaran terhadap prosedur Sistem Manajemen Keamanan Informasi oleh pegawai atau personil pihak ketiga;
37. laporan analisis perimeter keamanan fisik;
38. dokumen prosedur keamanan fisik;
39. dokumen hasil analisis tata tertib Sistem Manajemen Keamanan Informasi di lokasi kerja dan ruangan peralatan komputer;
40. laporan hasil analisis tentang panduan pengamanan fisik aset di lokasi kerja;
41. dokumen perubahan pedoman pengamanan fisik aset;
42. laporan identifikasi persyaratan dan spesifikasi keamanan fisik;
43. dokumen persyaratan dan spesifikasi keamanan fisik;
44. laporan penilaian ancaman dan kerentanan;
45. laporan hasil analisis panduan instalasi dan pemeliharaan infrastruktur, sistem, dan peralatan pendukung;
46. laporan hasil analisis tentang prosedur pengelolaan aset;
47. laporan identifikasi risiko terkait hubungan kerja dengan pihak ketiga;
48. *risk register* terkait hubungan kerja dengan pihak

ketiga;

49. dokumen hasil analisis perubahan kerangka kerja dan strategi manajemen risiko keamanan informasi;
50. dokumen hasil kaji-ulang tingkat efektifitas mitigasi risiko keamanan informasi;
51. dokumen langkah perbaikan mitigasi risiko yang belum efektif;
52. laporan penerapan tindakan perbaikan mitigasi risiko yang belum efektif;
53. laporan penilaian risiko;
54. laporan kajian risiko (*risk register*);
55. dokumen identifikasi rencana mitigasi risiko;
56. laporan penerapan mitigasi risiko;
57. laporan validasi kajian risiko (*risk register*);
58. laporan verifikasi kajian risiko (*risk register*);
59. dokumen rencana analisa kerentanan dan pengujian penetrasi keamanan sistem informasi;
60. laporan koordinasi proses analisa kerentanan dan pengujian penetrasi keamanan sistem informasi;
61. laporan analisis kerentanan penetrasi keamanan sistem elektronik;
62. laporan hasil uji penetrasi keamanan sistem elektronik;
63. rekomendasi dan tindak lanjut terhadap hasil pengujian penetrasi keamanan sistem elektronik;
64. laporan kajian keamanan informasi terhadap proses manajemen perubahan;
65. laporan diseminasi informasi terkait kerentanan, perbaikan atau mitigasi risiko yang telah diterapkan;
66. laporan penerapan pengendalian akses terhadap sistem operasi, aplikasi, dan jaringan;
67. laporan pemeliharaan pengendalian akses terhadap sistem operasi, aplikasi, dan jaringan;
68. laporan data jaringan;
69. laporan deteksi, penilaian, dan monitor kerentanan dan ancaman keamanan jaringan;

70. laporan perbaikan kerentanan dan ancaman keamanan jaringan;
71. laporan audit keamanan jaringan;
72. laporan hasil analisis prosedur keamanan jaringan;
73. laporan pelaksanaan prosedur keamanan jaringan;
74. laporan terkait indikasi adanya *anomali*;
75. dokumen uraian pemisahan tugas operasional;
76. laporan pemisahan fasilitas pengembangan, pengujian dan operasional;
77. laporan hasil identifikasi keamanan layanan sistem elektronik;
78. laporan pemantauan kinerja Sistem Manajemen Keamanan Informasi dalam pelaksanaan layanan pihak ketiga;
79. panduan pengelolaan perubahan terhadap layanan pihak ketiga;
80. panduan pengelolaan kapasitas sumber daya;
81. dokumentasi sistem infrastruktur dan aplikasi;
82. dokumen Standar Operasional Prosedur (SOP) pertukaran informasi;
83. dokumen Standar Operasional Prosedur (SOP) keamanan sistem elektronik untuk pelayanan publik;
84. dokumen rekomendasi kebijakan keamanan informasi yang tersedia untuk umum atau publik;
85. dokumen panduan audit *log* sistem;
86. dokumen standar rekaman data *log* sistem;
87. dokumen kebijakan sinkronisasi waktu sistem elektronik;
88. dokumen prosedur perlindungan terhadap barang yang ditinggal oleh penggunanya (*unattended user equipment*);
89. dokumen kebijakan *mobile computing*;
90. dokumen prosedur *teleworking*;
91. dokumen hasil identifikasi arsitektur keamanan informasi;
92. dokumen arsitektur keamanan informasi;

93. draft pengembangan mekanisme dan standar keamanan informasi untuk mengamankan proses bisnis atau *platform* teknologi;
94. laporan kajian penerapan protokol pertukaran informasi;
95. dokumen kebijakan keamanan informasi terkait hubungan dengan pihak ketiga;
96. dokumen hasil pemantauan dan *review* layanan pihak ketiga;
97. dokumen perubahan terhadap layanan pihak ketiga;
98. dokumen hasil analisis persyaratan keamanan informasi dalam siklus hidup pengembangan sistem elektronik;
99. laporan penerapan persyaratan Sistem Manajemen Keamanan Informasi terhadap layanan aplikasi pada jaringan publik;
100. laporan penerapan persyaratan Sistem Manajemen Keamanan Informasi terhadap layanan transaksi pada aplikasi;
101. dokumen standar keamanan informasi terhadap pengembangan sistem elektronik;
102. dokumen prosedur kontrol perubahan sistem elektronik;
103. laporan pengendalian perubahan atas *software packages*;
104. dokumen *secure system engineering principle*;
105. dokumen kajian keamanan lingkungan pengembangan sistem elektronik;
106. laporan penerapan persyaratan keamanan informasi dalam pengembangan aplikasi oleh pihak ketiga;
107. laporan pengujian keamanan sistem elektronik;
108. laporan pengujian tingkat penerimaan sistem elektronik;
109. dokumen standar operasional prosedur (SOP) perlindungan data uji sistem;
110. dokumen kebijakan dan pedoman penggunaan

kriptografi;

111. dokumen panduan dan Standar Operasional Prosedur (SOP) penerapan manajemen kunci kriptografi;
112. pusat pengendalian terhadap gangguan, kegagalan dan kerugian atas penyelenggaraan sistem elektronik untuk pelayanan publik;
113. laporan kegiatan pusat pengendalian terhadap gangguan, kegagalan dan kerugian atas penyelenggaraan sistem elektronik untuk pelayanan publik;
114. laporan pengendalian terhadap gangguan, kegagalan dan kerugian atas penyelenggaraan sistem elektronik untuk pelayanan publik;
115. laporan evaluasi upaya pengendalian terhadap gangguan, kegagalan dan kerugian atas penyelenggaraan sistem elektronik untuk pelayanan publik;
116. dokumen panduan penerapan Hak Kekayaan Intelektual (HAKI);
117. dokumen aturan tentang kontrol kriptografi;
118. laporan analisis tingkat kepatuhan terhadap ketentuan internal dan eksternal;
119. dokumen kerangka kerja dan kebijakan manajemen Keberlangsungan layanan sistem elektronik sesuai dengan persyaratan Sistem Manajemen Keamanan Informasi yang berlaku;
120. dokumen perencanaan, pengembangan, dan penerapan strategi keberlangsungan layanan dan rencana penanggulangan krisis atau bencana;
121. laporan sosialisasi rencana keberlangsungan layanan sistem elektronik dan penanggulangan krisis atau bencana;
122. laporan pelaksanaan proses yang menjamin kesiapan kemampuan sumber daya manusia dalam menjaga keberlangsungan layanan;

123. dokumen kebijakan terkait koordinasi untuk menjaga kelangsungan dan pemulihan layanan dengan *stakeholder* terkait;
124. dokumen prosedur terkait koordinasi kegiatan menjaga kelangsungan dan pemulihan layanan dengan *stakeholder* terkait;
125. laporan hasil analisis peraturan perundang-undangan di bidang Sistem Manajemen Keamanan Informasi;
126. daftar klasifikasi peraturan perundang-undangan di bidang Sistem Manajemen Keamanan Informasi;
127. laporan hasil analisis isu aktual di bidang Sistem Manajemen Keamanan Informasi;
128. naskah rekomendasi kebijakan di bidang Sistem Manajemen Keamanan Informasi;
129. laporan forum diskusi terkait dengan isu-isu kebijakan di bidang Sistem Manajemen Keamanan Informasi;
130. naskah akademik di bidang Sistem Manajemen Keamanan Informasi;
131. laporan forum diskusi terkait dengan penyusunan naskah akademik di bidang Sistem Manajemen Keamanan Informasi;
132. dokumen *Regulatory Impact Analysis* (RIA) di bidang Sistem Manajemen Keamanan Informasi;
133. laporan forum diskusi terkait dengan *masterplan* di bidang Sistem Manajemen Keamanan Informasi;
134. dokumen *masterplan* keamanan informasi nasional;
135. dokumen analisis peta keamanan informasi nasional;
136. laporan forum diskusi terkait dengan peta keamanan informasi nasional;
137. dokumen peta keamanan informasi nasional;
138. laporan hasil analisis norma, standar, prosedur dan kriteria (NSPK) tata kelola keamanan informasi;
139. dokumen norma, standar, prosedur dan kriteria (NSPK) tata kelola keamanan informasi;

140. laporan hasil analisis norma, standar, prosedur dan kriteria (NSPK) pengamanan perangkat lunak;
141. laporan forum diskusi terkait dengan norma, standar, prosedur dan kriteria (NSPK) pengamanan perangkat lunak;
142. dokumen norma, standar, prosedur dan kriteria (NSPK) pengamanan perangkat lunak;
143. dokumen hasil analisis norma, standar, prosedur dan kriteria (NSPK) pengamanan perangkat keras;
144. laporan forum diskusi terkait norma, standar, prosedur dan kriteria (NSPK) pengamanan perangkat keras;
145. dokumen norma, standar, prosedur dan kriteria (NSPK) pengamanan perangkat keras;
146. hasil analisis norma, standar, prosedur dan kriteria (NSPK) tenaga ahli di bidang Sistem Manajemen Keamanan Informasi;
147. laporan forum diskusi terkait dengan norma, standar, prosedur dan kriteria (NSPK) tenaga ahli di bidang Sistem Manajemen Keamanan Informasi;
148. dokumen norma, standar, prosedur dan kriteria (NSPK) tenaga ahli di bidang Sistem Manajemen Keamanan Informasi;
149. hasil analisis norma, standar, prosedur dan kriteria (NSPK) Sistem Manajemen Keamanan Informasi;
150. laporan forum diskusi terkait dengan norma, standar, prosedur dan kriteria (NSPK) Sistem Manajemen Keamanan Informasi;
151. dokumen norma, standar, prosedur dan kriteria (NSPK) Sistem Manajemen Keamanan Informasi;
152. notulensi bimbingan teknis di bidang Sistem Manajemen Keamanan Informasi;
153. materi uji kompetensi;
154. laporan kegiatan forum keamanan informasi nasional; dan
155. hasil *monitoring* dan evaluasi di bidang Sistem

Manajemen Keamanan Informasi;

c. Manggala Informatika Ahli Madya, meliputi:
   1. laporan identifikasi dan analisis risiko;
   2. laporan kajian kondisi berjalan dan kebutuhan pengamanan informasi;
   3. dokumen rencana kerja induk jangka menengah/panjang;
   4. dokumen sasaran dan target kinerja utama terkait pengelolaan keamanan informasi nasional;
   5. dokumen rencana pemantauan pelaksanaan keamanan informasi;
   6. laporan evaluasi pelaksanaan Sistem Manajemen Keamanan Informasi di semua area terkait;
   7. dokumen rencana pengukuran efektifitas dan efisiensi keamanan informasi di instansi;
   8. laporan pengukuran efektifitas dan efisiensi keamanan informasi di setiap area;
   9. dokumen perencanaan tingkat kematangan keamanan informasi di instansi;
   10. laporan pengukuran tingkat kematangan keamanan informasi di setiap area;
   11. laporan identifikasi dan analisis risiko sistem elektronik untuk pelayanan publik di sektor terkait;
   12. dokumen hasil identifikasi permasalahan dan kebutuhan keamanan informasi penerapan Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;
   13. laporan kajian kebutuhan keamanan dan standar teknis perlindungan informasi infrastruktur yang kritikal (*critical information infrastructure*) di sektor terkait;
   14. materi rencana kerja induk jangka menengah dan panjang terkait Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;

15. dokumen rencana konsultasi kepada Jabatan Fungsional Manggala Informatika satu tingkat dibawahnya;
16. laporan pelaksanaan konsultasi kepada Jabatan Fungsional Manggala Informatika satu tingkat dibawahnya;
17. dokumen rencana evaluasi kompetensi dan kinerja Jabatan Fungsional Manggala Informatika satu tingkat dibawahnya;
18. laporan evaluasi kompetensi dan kinerja Jabatan Fungsional Manggala Informatika satu tingkat dibawahnya;
19. dokumen perencanaan kegiatan diseminasi regulasi di bidang Sistem Manajemen Keamanan Informasi;
20. materi diseminasi regulasi di bidang Sistem Manajemen Keamanan Informasi;
21. laporan pelaksanaan kegiatan diseminasi regulasi di bidang Sistem Manajemen Keamanan Informasi;
22. draft program peningkatan kinerja Sistem Manajemen Keamanan Informasi;
23. laporan hasil analisis dan dokumen program peningkatan kinerja Sistem Manajemen Keamanan Informasi;
24. laporan evaluasi program peningkatan kinerja Sistem Manajemen Keamanan Informasi;
25. rancangan kerangka kerja di bidang Sistem Manajemen Keamanan Informasi;
26. laporan identifikasi sasaran kinerja Sistem Manajemen Keamanan Informasi;
27. laporan identifikasi mekanisme pengukuran sasaran kinerja Sistem Manajemen Keamanan Informasi;
28. dokumen hasil kaji ulang kerangka kerja keamanan informasi;
29. dokumen analisis kajian kepatuhan kebijakan di bidang Sistem Manajemen Keamanan Informasi di instansi terhadap hukum dan peraturan terkait

lainnya;

30. laporan evaluasi kepatuhan kebijakan sistem manajemen keamanan di instansi terhadap hukum dan peraturan terkait lainnya;
31. laporan evaluasi kebijakan Sistem Manajemen Keamanan Informasi mematuhi semua undang-undang dan peraturan perlindungan data pribadi;
32. rancangan struktur organisasi penerapan Sistem Manajemen Keamanan Informasi berikut tugas pokok dan fungsinya;
33. dokumen pemenuhan persyaratan Sistem Manajemen Keamanan Informasi bagi pihak eksternal;
34. laporan peninjauan kontruksi fisik sesuai dengan kontrol keamanan informasi;
35. laporan evaluasi efektifitas kebijakan dan prosedur keamanan fisik dan lingkungan serta dokumen rekomendasi untuk perbaikan yang diperlukan;
36. laporan evaluasi proses pengadaan memiliki implikasi terhadap keamanan fisik;
37. laporan penilaian akurasi dan efektivitas pengukuran kinerja sistem keamanan fisik beserta dokumen rekomendasi;
38. dokumen perubahan panduan instalasi dan pemeliharaan infrastruktur, sistem, dan peralatan pendukung;
39. dokumen perubahan kebijakan dan prosedur pengelolaan aset;
40. laporan evaluasi terhadap pihak ketiga terkait tingkat kepatuhan Sistem Manajemen Keamanan Informasi sesuai dengan kesepakatan;
41. dokumen strategi manajemen risiko keamanan informasi;
42. laporan pelaksanaan strategi manajemen risiko keamanan informasi;
43. dokumen perubahan strategi manajemen risiko keamanan informasi;

44. laporan kaji-ulang tingkat efektifitas mitigasi risiko keamanan informasi yang sudah berjalan;
45. laporan pemantauan proses penerapan mitigasi risiko keamanan informasi dan proses perbaikan yang diperlukan;
46. laporan pemeriksaan adanya kerentanan baru;
47. laporan penerapan langkah mitigasi yang diperlukan terhadap kerentanan baru;
48. laporan pemantauan tingkat kepatuhan secara kontinu terhadap prosedur pengelolaan media;
49. laporan pengujian efektifitas teknologi keamanan jaringan;
50. laporan pelaksanaan keamanan jaringan komunikasi elektronik yang bersifat rahasia dari gangguan dan penyadapan;
51. laporan kinerja keamanan jaringan;
52. dokumen perubahan kebijakan dan prosedur keamanan jaringan;
53. laporan evaluasi proses operasional untuk mengidentifikasi pelanggaran kebijakan Sistem Manajemen Keamanan Informasi;
54. laporan hasil integrasi solusi arsitektur keamanan informasi;
55. laporan kajian kesesuaian penerapan arsitektur keamanan informasi;
56. laporan usulan perubahan arsitektur keamanan informasi;
57. dokumen mekanisme dan standar keamanan informasi;
58. dokumen metodologi untuk evaluasi kelaikan langkah-langkah mitigasi risiko yang diterapkan dalam sistem elektronik;
59. laporan kajian efektifitas dan kehandalan keamanan sistem, mekanisme, dan produk;
60. laporan manajemen keberlangsungan layanan sistem elektronik;

61. dokumen hasil uji dan evaluasi rencana keberlangsungan layanan sistem elektronik;
62. dokumen analisis dampak terjadinya kondisi darurat dan menyusun *recovery time objective* (RTO) & *recovery point objective* (RPO) yang sesuai dengan kebutuhan instansi;
63. dokumen analisis azas-manfaat untuk penerapan kontrol keamanan informasi baru;
64. laporan evaluasi uji coba rencana kelangsungan layanan sistem elektronik;
65. laporan hasil pengukuran berkala rencana keberlangsungan layanan sistem elektronik dan rekomendasi langkah perbaikan;
66. laporan kesiapan infrastruktur dan fasilitas pemulihan layanan sistem elektronik; dan
67. laporan kegiatan pembinaan sumber daya manusia di bidang Sistem Manajemen Keamanan Informasi; dan

d. Manggala Informatika Ahli Utama, meliputi:
    1. kebijakan manajemen risiko keamanan informasi di sektor terkait;
    2. kebijakan mitigasi risiko keamanan informasi di sektor terkait;
    3. dokumen rekomendasi rekomendasi hasil kajian risiko keamanan informasi di sektor terkait;
    4. desain strategi dan kebijakan Sistem Manajemen Keamanan Informasi di sektor terkait;
    5. dokumen rekomendasi strategi dan kebijakan Sistem Manajemen Keamanan Informasi di sektor terkait;
    6. laporan koordinasi penyusunan rencana kerja induk Sistem Manajemen Keamanan Informasi di sektor terkait;
    7. dokumen hasil analisis sasaran dan target kinerja utama Sistem Manajemen Keamanan Informasi di sektor terkait;
    8. laporan evaluasi penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;

9. laporan evaluasi tingkat efektifitas dan efisiensi penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;
10. dokumen hasil analisis tingkat kematangan penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;
11. konsep kerangka kerja manajemen risiko keamanan informasi terhadap penyelenggaraan sistem elektronik untuk pelayanan publik di sektor terkait;
12. dokumen hasil evaluasi mitigasi risiko keamanan informasi terhadap penyelenggaraan sistem elektronik untuk pelayanan publik di sektor terkait;
13. dokumen hasil kajian risiko keamanan informasi terhadap penyelenggaraan sistem elektronik untuk pelayanan publik di sektor terkait;
14. dokumen hasil identifikasi dan analisis sistem elektronik strategis untuk pelayanan publik di sektor terkait;
15. konsep kerangka kerja penerapan Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;
16. konsep strategi penerapan Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;
17. laporan koordinasi penerapan Sistem Manajemen Keamanan Informasi dengan organisasi lainnya baik dalam maupun luar negeri;
18. dokumen hasil evaluasi dan rekomendasi hasil koordinasi terkait penerapan Sistem Manajemen Keamanan Informasi dengan organisasi lainnya baik dalam maupun luar negeri;
19. konsep persyaratan teknis kelaikan sistem elektronik strategis untuk pelayanan publik di sektor terkait;
20. konsep rencana kerja induk jangka menengah dan panjang terkait Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk

pelayanan publik di sektor terkait;

21. dokumen rencana kerja induk terkait keamanan informasi sistem elektronik untuk pelayanan publik dan sektor strategis terkait;
22. dokumen rencana evaluasi penerapan Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;
23. laporan evaluasi penerapan Sistem Manajemen Keamanan Informasi pada sistem elektronik strategis untuk pelayanan publik di sektor terkait;
24. dokumen rencana penilaian tingkat kematangan penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;
25. laporan analisis tingkat kematangan penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;
26. laporan validasi hasil analisis tingkat kematangan tingkat kematangan penerapan Sistem Manajemen Keamanan Informasi di sektor terkait;
27. laporan koordinasi mekanisme pelaporan terjadinya gangguan, kegagalan dan kerugian penyelenggaraan sistem elektronik untuk pelayanan publik dalam sektor terkait;
28. dokumen perencanaan kegiatan peningkatan kepedulian pengamanan penyelenggaraan sistem elektronik di sektor terkait;
29. laporan pelaksanaan kegiatan peningkatan kepedulian pengamanan penyelenggaraan sistem elektronik di sektor terkait;
30. laporan identifikasi permasalahan dan menganalisis terkait pengamanan penyelenggaraan sistem elektronik yang bersifat strategis;
31. dokumen rencana konsultasi terkait pengamanan penyelenggaraan sistem elektronik yang bersifat strategis;

32. laporan konsultasi terkait pengamanan penyelenggaraan sistem elektronik yang bersifat strategis;
33. laporan evaluasi hasil konsultasi terkait pengamanan penyelenggaraan sistem elektronik yang bersifat strategis;
34. dokumen perencanaan penelitian dan pengembangan model atau kerangka kerja baru terkait Sistem Manajemen Keamanan Informasi;
35. laporan koordinasi dengan *stakeholder* terkait dalam rangka penelitian dan pengembangan model atau kerangka kerja baru tentang Sistem Manajemen Keamanan Informasi; dan
36. dokumen model atau kerangka kerja baru terkait Sistem Manajemen Keamanan Informasi.

Pasal 10

Dalam hal unit kerja tidak terdapat Manggala Informatika yang sesuai dengan jenjang jabatannya untuk melaksanakan kegiatan sebagaimana dimaksud dalam Pasal 8 ayat (1), Manggala Informatika yang berada satu tingkat di atas, atau satu tingkat di bawah jenjang jabatannya dapat melakukan kegiatan tersebut berdasarkan penugasan secara tertulis dari pimpinan unit kerja yang bersangkutan.

Pasal 11

(1) Penilaian Angka Kredit atas hasil penugasan sebagaimana dimaksud dalam Pasal 10 ditetapkan sebagai berikut:
    a. Manggala Informatika yang melaksanakan tugas Manggala Informatika yang berada satu tingkat di atas jenjang jabatannya, Angka Kredit yang diperoleh ditetapkan paling besar 80% (delapan puluh persen) dari Angka Kredit setiap butir kegiatan; dan
    b. Manggala Informatika yang melaksanakan tugas

Manggala Informatika yang berada satu tingkat di bawah jenjang jabatannya, Angka Kredit yang diperoleh ditetapkan paling besar 100% (seratus persen) dari Angka Kredit setiap butir kegiatan.

(2) Ketentuan sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

BAB V
PENGANGKATAN DALAM JABATAN

Bagian Kesatu
Umum

Pasal 12

PyB mengangkat dalam Jabatan Fungsional Manggala Informatika yaitu pejabat sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 13

Pengangkatan PNS ke dalam Jabatan Fungsional Manggala Informatika dilakukan melalui pengangkatan:

a. pertama;
b. perpindahan dari jabatan lain;
c. penyesuaian (*inpassing*); dan
d. promosi.

Bagian Kedua
Pengangkatan Pertama

Pasal 14

(1) Pengangkatan dalam Jabatan Fungsional Manggala Informatika melalui pengangkatan pertama sebagaimana dimaksud dalam Pasal 13 huruf a, harus memenuhi persyaratan sebagai berikut:
    a. berstatus PNS;

b. memiliki integritas dan moralitas yang baik;
c. sehat jasmani dan rohani;
d. berijazah paling rendah sarjana atau diploma empat bidang teknik elektro dan informatika;
e. nilai prestasi kerja paling rendah bernilai baik dalam 1 (satu) tahun terakhir.

(2) Pengangkatan pertama sebagaimana dimaksud pada ayat (1) merupakan pengangkatan untuk mengisi lowongan kebutuhan Jabatan Fungsional Manggala Informatika dari Calon PNS.

(3) Calon PNS sebagaimana dimaksud pada ayat (2) setelah diangkat sebagai PNS dan telah mengikuti dan lulus uji kompetensi, paling lama 1 (satu) tahun diangkat dalam Jabatan Fungsional Manggala Informatika.

(4) PNS sebagaimana dimaksud pada ayat (3), paling lama 3 (tiga) tahun setelah diangkat harus mengikuti dan lulus pendidikan dan pelatihan fungsional di bidang keamanan informasi.

(5) Manggala Informatika yang belum mengikuti dan/atau tidak lulus pendidikan dan pelatihan fungsional di bidang keamanan informasi sebagaimana dimaksud pada ayat (4) tidak diberikan kenaikan jenjang satu tingkat di atasnya.

(6) Angka Kredit untuk pengangkatan pertama dalam Jabatan Fungsional Manggala Informatika dinilai dan ditetapkan pada saat mulai melaksanakan tugas Jabatan Fungsional Manggala Informatika.

Bagian Ketiga

Perpindahan dari Jabatan Lain

Pasal 15

(1) Pengangkatan dalam Jabatan Fungsional Manggala Informatika melalui perpindahan dari jabatan lain sebagaimana dimaksud dalam Pasal 13 huruf b, dilakukan dengan ketentuan sebagai berikut:

a. berstatus PNS;
b. memiliki integritas dan moralitas yang baik;
c. sehat jasmani dan rohani;
d. berijazah paling rendah sarjana atau diploma empat bidang teknik elektro dan informatika;
e. mengikuti dan lulus uji Kompetensi Teknis, Kompetensi, Manajerial, dan Kompetensi Sosial Kultural;
f. memiliki pengalaman dibidang Keamanan Informasi paling sedikit 2 (dua) tahun; dan
g. nilai prestasi kerja paling sedikit bernilai baik dalam 2 (dua) tahun terakhir; dan
h. berusia paling tinggi:
    1) 53 (lima puluh tiga) tahun bagi yang akan menduduki Jabatan Fungsional Manggala Informatika Ahli Pertama dan Jabatan Fungsional Manggala Informatika Ahli Muda;
    2) 55 (lima puluh lima) tahun bagi yang akan menduduki Jabatan Fungsional Manggala Informatika Ahli Madya; dan
    3) 60 (enam puluh) tahun bagi yang akan menduduki Jabatan Fungsional Manggala Informatika Ahli Utama bagi PNS yang telah menduduki Jabatan Pimpinan Tinggi.

(2) Pengangkatan Jabatan Fungsional Manggala Informatika sebagaimana dimaksud pada ayat (1) harus mempertimbangkan ketersediaan lowongan kebutuhan untuk jenjang Jabatan Fungsional Manggala Informatika yang akan diduduki.

(3) Pangkat yang ditetapkan bagi PNS sebagaimana dimaksud pada ayat (1) yaitu sama dengan pangkat yang dimilikinya dan jenjang jabatan yang ditetapkan sesuai dengan jumlah Angka Kredit yang ditetapkan oleh pejabat yang berwenang menetapkan Angka Kredit.

(4) Angka Kredit untuk pengangkatan dalam Jabatan Fungsional Manggala Informatika melalui perpindahan

dinilai dan ditetapkan dari tugas jabatan dengan mempertimbangkan pengalaman dalam pelaksanaan tugas di bidang penerapan Sistem Manajemen Keamanan Informasi.

Bagian Keempat

Pengangkatan Melalui Penyesuaian (*Inpassing*)

Pasal 16

(1) Pengangkatan dalam Jabatan Fungsional Manggala Informatika melalui penyesuaian (*inpassing*) sebagaimana dimaksud dalam Pasal 13 angka c harus memenuhi persyaratan sebagai berikut:
   a. berstatus sebagai PNS;
   b. memiliki integritas dan moralitas yang baik;
   c. sehat jasmani dan rohani;
   d. berijazah paling rendah sarjana atau diploma empat;
   e. mengikuti dan lulus uji Kompetensi Teknis, Kompetensi, Manajerial, dan Kompetensi Sosial Kultural;
   f. memiliki pengalaman dalam pelaksanaan tugas di bidang keamanan informasi paling sedikit 2 (dua) tahun; dan
   g. nilai prestasi kinerja paling kurang bernilai baik dalam 2 (dua) tahun terakhir.

(2) Pengangkatan dalam Jabatan Fungsional Manggala Informatika sebagaimana dimaksud pada ayat (1) dapat dilakukan apabila PNS yang pada saat berlakunya Peraturan Menteri ini, memiliki pengalaman dan masih melaksanakan tugas di bidang penerapan sistem manajemen keamanan informasi berdasarkan keputusan Pejabat yang Berwenang.

(3) Pengangkatan dalam Jabatan Fungsional Manggala Informatika sebagaimana dimaksud pada ayat (1) dilakukan dengan mempertimbangkan kebutuhan pada jenjang jabatan yang akan diduduki.

(4) Angka Kredit Kumulatif untuk penyesuaian (*inpassing*) dalam Jabatan Fungsional Manggala Informatika, tercantum dalam Lampiran VI yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

(5) Angka Kredit Kumulatif untuk penyesuaian (*inpassing*) sebagaimana dimaksud pada ayat (4) hanya berlaku 1 (satu) kali selama masa penyesuaian (*inpassing*).

(6) Tata cara pengangkatan dalam Jabatan Fungsional Manggala Informatika melalui penyesuaian (*inpassing*) diatur oleh Instansi Pembina.

Bagian Kelima

Pengangkatan melalui Promosi

Pasal 17

(1) Pengangkatan dalam Jabatan Fungsional Manggala Informatika melalui promosi sebagaimana dimaksud dalam Pasal 13 huruf b, dilaksanakan dalam hal:
   a. pengangkatan dalam Jabatan Fungsional Manggala Informatika; atau
   b. kenaikan jenjang jabatan satu tingkat lebih tinggi.

(2) Pengangkatan dalam Jabatan Fungsional Manggala Informatika melalui promosi sebagaimana dimaksud pada ayat (1) huruf a berlaku bagi PNS yang belum menduduki Jabatan Fungsional Manggala Informatika.

(3) Pengangkatan dalam Jabatan Fungsional Manggala Informatika melalui promosi sebagaimana dimaksud pada ayat (1) huruf b berlaku bagi Pejabat Fungsional dalam satu kategori Jabatan Fungsional.

(4) Pengangkatan dalam Jabatan Fungsional Manggala Informatika melalui promosi sebagaimana dimaksud pada ayat (2) dan ayat (3), harus memenuhi persyaratan sebagai berikut:
   a. mengikuti dan lulus uji Kompetensi sesuai standar kompetensi yang telah disusun oleh instansi pembina;

b. nilai kinerja/prestasi kerja paling rendah bernilai baik dalam 2 (dua) tahun terakhir.
c. memiliki rekam jejak yang baik;
d. tidak pernah melakukan pelanggaran kode etik dan profesi PNS; dan
e. tidak pernah dikenakan hukuman disiplin PNS.

(5) Pengangkatan dalam Jabatan Fungsional Manggala Informatika melalui promosi sebagaimana dimaksud pada ayat (1) harus mempertimbangkan kebutuhan untuk jenjang jabatan fungsional yang akan diduduki.

(6) Angka Kredit untuk pengangkatan dalam Jabatan Fungsional Manggala Informatika melalui promosi dinilai dan ditetapkan dari tugas Jabatan Fungsional Manggala Informatika.

BAB VI
PELANTIKAN DAN PENGAMBILAN SUMPAH/JANJI

Pasal 18

(1) Setiap PNS yang diangkat menjadi Manggala Informatika wajib dilantik dan diambil sumpah/janji menurut agama atau kepercayaannya kepada Tuhan Yang Maha Esa.

(2) Sumpah/janji sebagaimana dimaksud pada ayat (1) berdasarkan ketentuan peraturan perundang-undangan.

BAB VII

PENILAIAN KINERJA

Bagian Kesatu

Umum

Pasal 19

(1) Penilaian kinerja Manggala Informatika bertujuan untuk menjamin objektivitas pembinaan yang didasarkan sistem prestasi dan sistem karier.
(2) Penilaian kinerja Manggala Informatika dilakukan berdasarkan perencanaan kinerja pada tingkat individu dan tingkat unit atau organisasi, dengan memperhatikan target, capaian, hasil dan manfaat yang dicapai, serta perilaku PNS.
(3) Penilaian kinerja Manggala Informatika dilakukan secara objektif, terukur, akuntabel, partisipatif, dan transparan sesuai ketentuan peraturan perundang-undangan.

Pasal 20

Penilaian Kinerja sebagaimana dimaksud dalam Pasal 19 meliputi:

a. SKP; dan
b. Perilaku Kerja.

Bagian Kedua

SKP

Paragraf Kesatu

Umum

Pasal 21

(1) Pada awal tahun, Manggala Informatika wajib menyusun SKP.

(2) SKP merupakan target kinerja Manggala Informatika berdasarkan penetapan kinerja unit kerja yang bersangkutan.

(3) SKP untuk masing-masing jenjang jabatan diambil dari uraian kegiatan tugas jabatan sebagai turunan dari penetapan kinerja unit kerja.

Pasal 22

(1) Target kinerja sebagaimana dimaksud dalam Pasal 21 ayat (2) terdiri dari kinerja utama berupa target Angka Kredit dan/atau kinerja tambahan berupa tugas tambahan.

(2) Target Angka Kredit sebagaimana dimaksud pada ayat (1) diuraikan dalam bentuk kegiatan, tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

(3) Tugas tambahan sebagaimana dimaksud pada ayat (1) ditetapkan oleh pimpinan unit kerja berdasarkan penetapan kinerja unit kerja yang bersangkutan.

Pasal 23

(1) Target Angka Kredit dan tugas tambahan sebagaimana dimaksud dalam Pasal 22 ayat (1) sebagai dasar untuk penyusunan, penetapan, dan penilaian SKP.

(2) SKP yang disusun sebagaimana dimaksud pada ayat (1) harus disetujui dan ditetapkan oleh atasan langsung.

(3) Penilaian SKP sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

(4) Hasil penilaian SKP Manggala Informatika sebagaimana dimaksud pada ayat (2) ditetapkan sebagai capaian SKP.

Paragraf Kedua
Target Angka Kredit

Pasal 24

(1) Target Angka Kredit sebagaimana dimaksud dalam Pasal 23 ayat (1) bagi Manggala Informatika setiap tahun ditetapkan paling kurang:
   a. 12,5 (dua belas koma lima) untuk Manggala Informatika Ahli Pertama;
   b. 25 (dua puluh lima) untuk Manggala Informatika Ahli Muda;
   c. 37,5 (tiga puluh tujuh koma lima) untuk Manggala Informatika Ahli Madya; dan
   d. 50 (lima puluh) untuk Manggala Informatika Ahli Utama.

(2) Target Angka Kredit sebagaimana dimaksud pada ayat (1) huruf d, tidak berlaku bagi Manggala Informatika Ahli Utama yang memiliki pangkat tertinggi dalam jenjang jabatan yang didudukinya.

Paragraf 3
Angka Kredit Pemeliharaan

Pasal 25

(1) Manggala Informatika yang telah memenuhi syarat untuk kenaikan jenjang jabatan setingkat lebih tinggi tetapi belum tersedia lowongan pada jenjang jabatan yang akan diduduki, setiap tahun wajib memenuhi target Angka Kredit paling sedikit:
   a. 10 (sepuluh) untuk Manggala Informatika Ahli Pertama;
   b. 20 (dua puluh) untuk Manggala Informatika Ahli Muda; dan
   c. 30 (tiga puluh) untuk manggala Informatika Ahli Madya.

(2) Manggala Informatika Ahli Utama yang menduduki pangkat tertinggi dari jabatannya, setiap tahun sejak menduduki pangkatnya wajib mengumpulkan paling sedikit 25 (dua puluh lima) Angka Kredit.

Bagian Ketiga
Perilaku Kerja

Pasal 26

(1) Perilaku kerja meliputi aspek:
a. orientasi pelayanan;
b. komitmen;
c. inisiatif kerja;
d. kerja sama; dan
e. kepemimpinan.

(2) Aspek kepemimpinan sebagaimana dimaksud pada ayat (1) huruf e hanya dilakukan bagi jabatan fungsional yang karakteristik kegiatannya membutuhkan aspek kepemimpinan, yang ditetapkan oleh Instansi Pembina.

(3) Perilaku kerja ditetapkan berdasarkan standar perilaku kerja dalam Jabatan Fungsional Manggala Informatika dan dinilai sesuai dengan ketentuan peraturan perundang-undangan.

BAB VIII
PENILAIAN DAN PENETAPAN ANGKA KREDIT

Bagian Kesatu
Penilaian dan Penetapan Angka Kredit

Pasal 27

(1) Capaian SKP Manggala Informatika sebagaimana dimaksud dalam Pasal 23 ayat (4) disampaikan kepada Tim Penilai untuk dilakukan penilaian sebagai capaian Angka Kredit.

(2) Capaian Angka Kredit Manggala Informatika sebagaimana dimaksud pada ayat (1), ditetapkan paling tinggi 150% (seratus lima puluh persen) dari target Angka Kredit minimal sebagaimana dimaksud dalam Pasal 24.

(3) Dalam hal telah memenuhi Angka Kredit yang dipersyaratkan untuk kenaikan pangkat/jabatan, capaian Angka Kredit Manggala Informatika sebagaimana dimaksud pada ayat (1) diusulkan kepada pejabat yang memiliki kewenangan menetapkan Angka Kredit untuk ditetapkan dalam PAK.

(4) PAK sebagaimana dimaksud pada ayat (3) digunakan sebagai dasar kenaikan pangkat/jabatan setingkat lebih tinggi tercantum dalam Lampiran III sampai dengan Lampiran V yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

Pasal 28

(1) Untuk mendukung objektivitas dalam penilaian kinerja, Manggala Informatika mendokumentasikan hasil kerja yang diperoleh sesuai dengan SKP yang ditetapkan setiap tahunnya.

(2) Dalam hal sebagai bahan pertimbangan dalam pelaksanaan penilaian Angka Kredit, Tim Penilai dapat meminta laporan pelaksanaan kegiatan dan bukti fisik hasil kerja Manggala Informatika.

(3) Hasil penilaian dan PAK Manggala Informatika sebagaimana dimaksud dalam Pasal 27 ayat (3) dan ayat (4) dapat digunakan sebagai bahan pertimbangan dalam penilaian kinerja Manggala Informatika.

Bagian Kedua

Pejabat Yang Mengusulkan Angka Kredit

Pasal 29

Usul Penetepan Angka Kredit Manggala Informatika diajukan oleh:

a. Pejabat Pimpinan Tinggi Madya kepada Pejabat Pimpinan Tinggi Madya yang membidangi kepegawaian untuk Angka Kredit Manggala Informatika Ahli Utama di lingkungan Badan Siber dan Sandi Negara;
b. Pejabat Pimpinan Tinggi Pratama kepada Pejabat Pimpinan Tinggi Madya yang membidangi kepegawaian pada Badan Siber dan Sandi Negara untuk Angka Kredit Manggala Informatika Ahli Madya di lingkungan Badan Siber dan Sandi Negara, Instansi Pusat, atau Pemerintah Daerah Provinsi;
c. Pejabat Administrator kepada Pejabat Administrator yang membidangi kepegawaian untuk Angka Kredit Manggala Informatika Ahli Pertama dan Manggala Informatika Ahli Muda di lingkungan Badan Siber dan Sandi Negara;
d. Pejabat Administrator kepada Pejabat Pimpinan Tinggi Pratama yang membidangi kepegawaian untuk Angka Kredit Manggala Informatika Ahli Pertama dan Manggala Informatika Ahli Muda di lingkungan Instansi Pusat dan Instansi Daerah;

Bagian Ketiga

Pejabat yang Berwenang Menetapkan Angka Kredit

Pasal 30

PyB menetapkan Angka Kredit yaitu:

a. Pejabat Pimpinan Tinggi Utama atau Pejabat Pimpinan Tinggi Madya yang mendapat pendelegasian wewenang untuk Angka Kredit Manggala Informatika Ahli Utama di lingkungan Badan Siber dan Sandi Negara;
b. Pejabat Pimpinan Tinggi Madya yang membidangi

pembinaan jabatan fungsional pada Badan Siber dan Sandi Negara untuk Angka Kredit Manggala Informatika Ahli Madya di lingkungan Badan Siber dan Sandi Negara, Instansi Pusat, atau Pemerintah Daerah Provinsi;

c. Pejabat Pimpinan Tinggi Pratama yang membidangi kepegawaian untuk Angka Kredit Manggala Informatika Ahli Pertama dan Manggala Informatika Ahli Muda di lingkungan Badan Siber dan Sandi Negara, Instansi Pusat dan Instansi Daerah;

Bagian Keempat

Tim Penilai

Pasal 31

(1) Dalam menjalankan tugasnya, pejabat sebagaimana dimaksud dalam Pasal 30 dibantu oleh Tim Penilai.

(2) Tim Penilai sebagaimana dimaksud pada ayat (1) memiliki tugas:
   a. mengevaluasi keselarasan hasil penilaian yang dilakukan oleh pejabat penilai;
   b. memberikan penilaian Angka Kredit berdasarkan nilai capaian tugas jabatan;
   c. memberikan rekomendasi kenaikan pangkat dan/atau jenjang jabatan;
   d. memberikan rekomendasi mengikuti uji kompetensi;
   e. melakukan pemantauan terhadap hasil penilaian capaian tugas jabatan;
   f. memberikan pertimbangan penilaian SKP; dan
   g. memberikan bahan pertimbangan kepada Pejabat yang Berwenang dalam pengembangan PNS, pengangkatan dalam jabatan, pemberian tunjangan dan sanksi, mutasi, serta keikutsertaan Pejabat Fungsional dalam pendidikan dan pelatihan.

(3) Tim Penilai Manggala Informatika terdiri atas:
   a. Tim Penilai Pusat, bagi:
      1) Pejabat Pimpinan Tinggi Madya yang

membidangi kepegawaian untuk Angka Kredit Manggala Informatika Ahli Utama di lingkungan Badan Siber dan Sandi Negara; dan

2) Pejabat Pimpinan Tinggi Madya yang membidangi kepegawaian untuk Angka Kredit Manggala Informatika Ahli Madya di lingkungan Badan Siber dan Sandi Negara, Instansi Pusat dan Pemerintah Daerah Provinsi;

b. Tim Penilai Instansi bagi Pejabat Pimpinan Tinggi Pratama yang membidangi kepegawaian untuk Angka Kredit Manggala Informatika Ahli Pertama dan Manggala Informatika Ahli Muda di lingkungan Badan Siber dan Sandi Negara dan Instansi Pusat;

c. Tim Penilai Provinsi bagi Pejabat Pimpinan Tinggi Pratama yang membidangi kepegawaian untuk Angka Kredit Manggala Informatika Ahli Pertama dan Manggala Informatika Ahli Muda di lingkungan Pemerintah Daerah Provinsi; dan

d. Tim Penilai Kabupaten/Kota bagi Pejabat Pimpinan Tinggi Pratama untuk Angka Kredit Manggala Informatika Ahli Pertama dan Manggala Informatika Ahli Muda di lingkungan Pemerintah Daerah Kabupaten/Kota.

Pasal 32

(1) Tim Penilai sebagaimana dimaksud dalam Pasal 31 terdiri atas pejabat yang berasal dari unsur teknis yang membidangi Jabatan Fungsional Manggala Informatika, unsur kepegawaian, dan Manggala Informatika.

(2) Susunan keanggotaan Tim Penilai sebagai berikut:
   a. seorang Ketua merangkap anggota;
   b. seorang Sekretaris merangkap anggota; dan
   c. paling sedikit 3 (tiga) orang anggota.

(3) Susunan Anggota sebagaimana dimaksud pada ayat (2) harus berjumlah ganjil.

(4) Ketua Tim Penilai sebagaimana dimaksud pada ayat (2) huruf a, paling rendah Pejabat Administrator atau Manggala Informatika Ahli Madya;

(5) Sekretaris Tim Penilai sebagaimana dimaksud pada ayat (2) huruf b, harus berasal dari unsur kepegawaian.

(6) Anggota Tim Penilai sebagaimana dimaksud pada ayat (2) huruf c, paling sedikit 2 (dua) orang dari Manggala Informatika.

(7) Syarat untuk menjadi anggota Tim Penilai, yaitu:
   a. menduduki jabatan/pangkat paling rendah sama dengan jabatan/pangkat Manggala Informatika yang dinilai;
   b. memiliki keahlian serta kemampuan untuk menilai Angka Kredit Manggala Informatika; dan
   c. aktif melakukan penilaian Angka Kredit Manggala Informatika.

(8) Apabila jumlah anggota Tim Penilai sebagaimana dimaksud pada ayat (6) tidak dapat dipenuhi dari Manggala Informatika, anggota Tim Penilai dapat diangkat dari PNS lain yang memiliki kompetensi untuk menilai hasil kerja Manggala Informatika.

(9) Pembentukan dan susunan anggota Tim Penilai ditetapkan oleh:
   a. Pejabat Pimpinan Tinggi Madya yang membidangi kepegawaian untuk Tim Penilai Pusat;
   b. Pejabat Pimpinan Tinggi Madya yang membidangi kepegawaian untuk Tim Penilai Instansi di lingkungan Instansi Pusat;
   c. Pejabat Pimpinan Tinggi Madya yang membidangi kepegawaian untuk Tim Penilai Provinsi; dan
   d. Pejabat Pimpinan Tinggi Pratama yang membidangi kesekretarian untuk Tim Penilai Kabupaten/Kota.

(10) Dalam hal Instansi Pemerintah belum membentuk Tim Penilai, Penilaian Angka Kredit dapat dilaksanakan oleh Tim Penilai pada Instansi Pemerintah lain terdekat atau instansi pembina.

Pasal 33

Tata kerja Tim Penilai dan tata cara penilaian Angka Kredit Jabatan Fungsional Manggala Informatika ditetapkan oleh Kepala Badan Siber dan Sandi Negara selaku Pimpinan Instansi Pembina Jabatan Fungsional Manggala Informatika.

BAB IX

KENAIKAN PANGKAT DAN KENAIKAN JABATAN

Bagian Kesatu

Kenaikan Pangkat

Pasal 34

(1) Kenaikan pangkat dapat dipertimbangkan apabila capaian Angka Kredit telah memenuhi Angka Kredit Kumulatif yang dipersyaratkan.

(2) Jumlah Angka Kredit Kumulatif yang harus dipenuhi untuk kenaikan pangkat dan/atau jenjang Jabatan Fungsional Manggala Informatika, untuk:

a. Manggala Informatika dengan pendidikan sarjana atau diploma empat tercantum dalam Lampiran III yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

b. Manggala Informatika dengan pendidikan magister tercantum dalam Lampiran IV yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

c. Manggala Informatika dengan pendidikan doktor tercantum dalam Lampiran V yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

Pasal 35

(1) Dalam hal untuk kenaikan pangkat sebagaimana dimaksud dalam Pasal 34 ayat (1), Manggala Informatika dapat melaksanakan kegiatan penunjang, meliputi:

a. pengajar/pelatih pada diklat fungsional/teknis di bidang Sistem Manajemen Keamanan Informasi;

b. keanggotaan dalam tim penilai;
c. perolehan penghargaan/tanda jasa;
d. melaksanakan tugas lain yang mendukung pelaksanaan tugas Jabatan Fungsional; atau
e. perolehan gelar/ijazah lain.

(2) Kegiatan penunjang sebagaimana dimaksud pada ayat (1), diberikan kumulatif Angka Kredit paling tinggi 20% dari Angka Kredit yang dipersyaratkan untuk kenaikan pangkat tercantum dalam Lampiran III sampai dengan Lampiran V yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

(3) Angka Kredit sebagaimana dimaksud pada ayat (2) diberikan untuk satu kali kenaikan pangkat.

Bagian Kedua
Kenaikan Jenjang Jabatan

Pasal 36

(1) Kenaikan jenjang Jabatan Fungsional Manggala Informatika satu tingkat lebih tinggi wajib memenuhi Angka Kredit yang ditetapkan tercantum dalam Lampiran III sampai dengan Lampiran V yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

(2) Kenaikan jenjang Jabatan Fungsional Manggala Informatika sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan ketersediaan lowongan kebutuhan jabatan.

(3) Selain memenuhi syarat kinerja, Manggala Informatika yang akan dinaikkan jabatannya setingkat lebih tinggi harus mengikuti dan lulus uji kompetensi dan persyaratan lain.

(4) Syarat kinerja dan persyaratan lain sebagaimana dimaksud pada ayat (3) diatur oleh instansi pembina.

Pasal 37

(1) Dalam hal untuk kenaikan jenjang sebagaimana dimaksud dalam Pasal 36 ayat (1), Manggala Informatika dapat melaksanakan kegiatan pengembangan profesi.

(2) Kegiatan pengembangan profesi sebagaimana dimaksud pada ayat (1) meliputi:
   a. perolehan ijazah/gelar pendidikan formal di bidang Sistem Manajemen Keamanan Informasi;
   b. penyusunan Karya Tulis/Karya Ilmiah di bidang Sistem Manajemen Keamanan Informasi;
   c. penerjemahan/penyaduran buku dan karya ilmiah di bidang Sistem Manajemen Keamanan Informasi;
   d. penyusunan pedoman/petunjuk teknis di bidang Sistem Manajemen Keamanan Informasi; dan
   e. pelatihan/pengembangan kompetensi di bidang Sistem Manajemen Keamanan Informasi.

(3) Kegiatan pengembangan profesi sebagaimana dimaksud pada ayat (2) diberikan Angka Kredit tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini

(4) Bagi Manggala Informatika yang akan naik ke jenjang jabatan Ahli Madya dan Ahli Utama, Manggala Informatika wajib melaksanakan kegiatan pengembangan profesi Jabatan Fungsional Manggala Informatika, dengan Angka Kredit pengembangan profesi yang disyaratkan sebagai berikut:
   a. 6 (enam) bagi Manggala Informatika Ahli Muda yang akan naik jabatan setingkat lebih tinggi menjadi Manggala Informatika Ahli Madya.
   b. 12 (dua belas) bagi Manggala Informatika Ahli Madya yang akan naik jabatan setingkat lebih tinggi menjadi Manggala Informatika Ahli Utama.

Pasal 38

(1) Manggala Informatika yang secara bersama-sama membuat Karya Tulis/Karya Ilmiah di bidang keamanan informasi, diberikan Angka Kredit dengan ketentuan sebagai berikut:
    a. apabila terdiri dari 2 (dua) orang penulis maka pembagian Angka Kredit yaitu 60% (enam puluh persen) bagi penulis utama dan 40% (empat puluh persen) bagi penulis pembantu;
    b. apabila terdiri dari 3 (tiga) orang penulis maka pembagian Angka Kredit yaitu 50% (lima puluh persen) bagi penulis utama dan masing-masing 25% (dua puluh lima persen) bagi penulis pembantu;
    c. apabila terdiri dari 4 (empat) orang penulis maka pembagian Angka Kredit yaitu 40% (empat puluh persen) bagi penulis utama dan masing-masing 20% (dua puluh persen) bagi penulis pembantu; dan
    d. apabila tidak terdapat atau tidak dapat ditentukan penulis utama dan penulis pembantu maka pembagian Angka Kredit dibagi sebesar proporsi yang sama untuk setiap penulis.
(2) Jumlah penulis pembantu sebagaimana dimaksud pada ayat (1), paling banyak 3 (tiga) orang.

Bagian Ketiga

Mekanisme Kenaikan Pangkat dan Jenjang

Pasal 39

Persyaratan dan mekanisme kenaikan pangkat dan jenjang jabatan bagi Manggala dilakukan sesuai dengan peraturan perundang-undangan.

Pasal 40

Dalam hal target Angka Kredit yang disyaratkan untuk kenaikan pangkat/jabatan setingkat lebih tinggi bagi tidak

tercapai, Manggala Informatika tidak diberikan kenaikan pangkat/jabatan.

Pasal 41

Manggala Informatika yang memiliki Angka Kredit melebihi Angka Kredit yang disyaratkan untuk kenaikan pangkat setingkat lebih tinggi, kelebihan angka kredit tersebut dapat diperhitungkan untuk kenaikan pangkat berikutnya dalam satu jenjang Jabatan Fungsional.

BAB X

KEBUTUHAN PNS DALAM JABATAN FUNGSIONAL MANGGALA INFORMATIKA

Pasal 42

(1) Penetapan kebutuhan PNS dalam Jabatan Fungsional Manggala Informatika dihitung berdasarkan beban kerja yang ditentukan dari indikator:
    a. ruang lingkup penyelenggaraan sistem elektronik;
    b. luas wilayah pelayanan sistem elektronik; dan
    c. kompleksitas sistem elektronik;
(2) Pedoman perhitungan kebutuhan Jabatan Fungsional Manggala Informatika diatur oleh Kepala Badan Siber dan Sandi Negara selaku Pimpinan Instansi Pembina setelah mendapat persetujuan Menteri.

Pasal 43

Pengangkatan dalam Jabatan Fungsional Manggala Informatika berdasarkan Peraturan ini tidak dapat dilakukan sebelum pedoman penghitungan kebutuhan Jabatan Fungsional Manggala Informatika ditetapkan.

BAB XI

KOMPETENSI

Bagian Kesatu

Standar Kompetensi

Pasal 44

(1) PNS yang menduduki Jabatan Fungsional Manggala Informatika harus memenuhi standar kompetensi sesuai dengan jenjang jabatan.

(2) Kompetensi Manggala Informatika meliputi:
   a. kompetensi teknis;
   b. kompetensi manajerial; dan
   c. kompetensi sosial kultural.

(3) Rincian standar kompetensi setiap jenjang jabatan dan tata cara pelaksanaan uji kompetensi sebagaimana dimaksud pada ayat (1) dan ayat (2) disusun oleh instansi pembina.

Bagian Kedua

Pengembangan Kompetensi

Pasal 45

(1) Untuk meningkatkan kompetensi dan profesionalisme Manggala Informatika diikutsertakan pada pelatihan.

(2) Pelatihan yang diberikan bagi Manggala Informatika sebagaimana dimaksud pada ayat (1) disesuaikan dengan hasil analisis kebutuhan pelatihan dan penilaian kinerja.

(3) Pelatihan yang diberikan kepada Manggala Informatika sebagaimana dimaksud pada ayat (1), antara lain dalam bentuk:
   a. pelatihan fungsional; dan
   b. pelatihan teknis bidang Sistem Manajemen Keamanan Informasi.

(4) Selain pelatihan sebagaimana dimaksud pada ayat (3), Manggala Informatika dapat mengembangkan kompetensinya melalui program pengembangan kompetensi lainnya.

(5) Program pengembangan kompetensi sebagaimana dimaksud pada ayat (4) meliputi:
   a. mempertahankan keahlian sebagai Manggala Informatika *(maintain rating)*;
   b. seminar;
   c. lokakarya (*workshop*); atau
   d. konferensi.

(6) Ketentuan mengenai pelatihan dan pengembangan kompetensi serta pedoman penyusunan analisis kebutuhan pelatihan fungsional Manggala Informatika sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur oleh instansi pembina.

BAB XII
PEMBERHENTIAN DARI JABATAN

Pasal 46

(1) Manggala Informatika diberhentikan dari jabatannya apabila:
   a. mengundurkan diri dari Jabatan;
   b. diberhentikan sementara sebagai PNS;
   c. menjalani cuti di luar tanggungan Negara;
   d. menjalani tugas belajar lebih dari 6 (enam) bulan;
   e. ditugaskan secara penuh pada Jabatan Pimpinan Tinggi, Jabatan Administrator, Jabatan Pengawas, dan Jabatan Pelaksana;
   f. tidak memenuhi persyaratan jabatan.

(2) Pengunduran diri sebagaimana dimaksud pada ayat (1) huruf a dapat dipertimbangkan dalam hal memiliki alasan pribadi yang tidak mungkin untuk melaksanakan tugas Jabatan Fungsional Manggala Informatika.

(3) Kriteria tidak memenuhi persyaratan jabatan sebagaimana dimaksud pada ayat (1) huruf f dapat dipertimbangkan dalam hal:
   a. tidak memenuhi kualifikasi pendidikan yang dipersyaratkan untuk menduduki Jabatan Fungsional Manggala Informatika; atau
   b. tidak memenuhi standar kompetensi yang ditentukan pada jabatan fungsional yang diduduki.

(4) Manggala Informatika yang diberhentikan karena alasan sebagaimana dimaksud pada ayat (1) huruf b sampai dengan huruf e dapat diangkat kembali sesuai dengan jenjang jabatan terakhir apabila tersedia kebutuhan Jabatan Fungsional Manggala Informatika.

(5) Pengangkatan kembali dalam Jabatan Fungsional Manggala Informatika sebagaimana dimaksud pada ayat (4), dilakukan dengan menggunakan Angka Kredit terakhir yang dimiliki dan dapat ditambah dengan Angka Kredit dari penilaian pelaksanaan tugas di bidang Sistem Manajemen Keamanan Informasi selama diberhentikan.

(6) Terhadap Manggala Informatika sebagaimana dimaksud pada ayat (1) huruf a dan huruf f dilaksanakan pemeriksaan dan mendapatkan ijin dari Pejabat yang Berwenang sebelum ditetapkan pemberhentiannya.

(7) Manggala Informatika sebagaimana dimaksud pada ayat (6) tidak dapat diangkat kembali dalam Jabatan Fungsional Manggala Informatika.

Pasal 47

Manggala Informatika yang diberhentikan karena ditugaskan pada jabatan sebagaimana dimaksud dalam Pasal 46 ayat (1) huruf e, dapat disesuaikan pada jenjang sesuai dengan pangkat terakhir pada jabatannya paling kurang 1 (satu) tahun setelah diangkat kembali pada jenjang terakhir yang didudukinya, setelah mengikuti dan lulus uji kompetensi apabila tersedia kebutuhan.

Pasal 48

Pemberhentian dari Jabatan Fungsional Manggala Informatika dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB XIII

TUGAS INSTANSI PEMBINA

Pasal 49

(1) Instansi Pembina berperan sebagai pengelola Jabatan Fungsional Manggala Informatika yang bertanggung jawab untuk menjamin terwujudnya standar kualitas dan profesionalitas jabatan.

(2) Instansi Pembina mempunyai tugas sebagai berikut:
   a. menyusun pedoman formasi Jabatan Fungsional Manggala Informatika;
   b. menyusun Standar Kompetensi Jabatan Fungsional Manggala Informatika;
   c. menyusun petunjuk pelaksanaan dan petunjuk teknis Jabatan Manggala Informatika;
   d. menyusun standar kualitas hasil kerja dan pedoman penilaian kualitas hasil kerja Manggala Informatika;
   e. menyusun pedoman penulisan Karya Tulis/Karya Ilmiah yang bersifat inovatif di bidang Sistem Manajemen Keamanan Informasi;
   f. menyusun kurikulum pelatihan Jabatan Fungsional Manggala Informatika;
   g. menyelenggarakan pelatihan Jabatan Fungsional Manggala Informatika;
   h. membina penyelenggaraan pelatihan fungsional Manggala Informatika pada lembaga pelatihan;
   i. menyelenggarakan uji kompetensi Jabatan Fungsional Manggala Informatika;
   j. menganalisis kebutuhan pelatihan fungsional di bidang tugas Jabatan Fungsional Manggala Informatika;

k. melakukan sosialisasi petunjuk pelaksanaan dan petunjuk teknis Jabatan Fungsional Manggala Informatika;
l. mengembangkan sistem informasi Jabatan Fungsional Manggala Informatika;
m. memfasilitasi pelaksanaan tugas pokok Jabatan Fungsional Manggala Informatika;
n. memfasilitasi pembentukan organisasi profesi Jabatan Fungsional Manggala Informatika;
o. memfasilitasi penyusunan dan penetapan kode etik profesi dan kode perilaku Jabatan Fungsional Manggala Informatika;
p. melakukan akreditasi pelatihan fungsional dengan mengacu kepada ketentuan yang telah ditetapkan oleh Lembaga Administrasi Negara;
q. melakukan pemantauan dan evaluasi penerapan Jabatan Fungsional Manggala Informatika; dan
r. melakukan koordinasi dengan instansi pengguna dalam rangka pembinaan karier Manggala Informatika; dan
s. menyusun informasi faktor jabatan untuk evaluasi jabatan.

(3) Uji kompetensi sebagaimana dimaksud pada ayat (2) huruf i dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

(4) Uji kompetensi sebagaimana dimaksud pada ayat (3) dapat dilakukan oleh Instansi Pemerintah pengguna Jabatan Fungsional Manggala Informatika setelah mendapat akreditasi dari instansi pembina.

(5) Instansi pembina dalam melaksanakan tugas pembinaan sebagaimana dimaksud pada ayat (2) huruf a, huruf b, huruf c, huruf d, huruf e, huruf i, huruf k, huruf l, huruf m, huruf n, huruf o, huruf q, huruf r, dan huruf s menyampaikan hasil pelaksanaan pembinaan Jabatan Fungsional Manggala Informatika secara berkala sesuai dengan perkembangan pelaksanaan pembinaan kepada

Menteri dengan tembusan Kepala Badan Kepegawaian Negara.

(6) Instansi pembina menyampaikan secara berkala setiap tahun pelaksanaan tugas sebagaimana dimaksud pada ayat (2) huruf f, huruf g, huruf h, huruf j, dan huruf p kepada Menteri dengan tembusan Kepala Lembaga Administrasi Negara.

(7) Ketentuan lebih lanjut mengenai penyelenggaraan uji kompetensi Jabatan Fungsional Manggala Informatika sebagaimana dimaksud pada ayat (2) huruf i diatur oleh instansi pembina.

BAB XIV
PEMINDAHAN KEDALAM JABATAN LAIN DAN LARANGAN RANGKAP JABATAN

Pasal 50

Untuk kepentingan organisasi dan pengembangan karir, Manggala Informatika dapat dipindahkan ke dalam jabatan lain sesuai dengan ketentuan peraturan perundang-undangan dengan persetujuan PPK .

Pasal 51

Dalam rangka optimalisasi pelaksanaan tugas dan pencapaian kinerja organisasi, Manggala Informatika dilarang rangkap Jabatan dengan Jabatan Pimpinan Tinggi, Jabatan Administrator, Jabatan Pengawas, atau Jabatan Pelaksana.

BAB XV
ORGANISASI PROFESI

Pasal 52

(1) Jabatan Fungsional Manggala Informatika wajib memiliki 1 (satu) organisasi profesi.

(2) Manggala Informatika wajib menjadi anggota organisasi profesi Jabatan Fungsional Manggala Informatika.

(3) Pembentukan organisasi profesi Jabatan Fungsional Manggala Informatika sebagaimana dimaksud pada ayat (1) difasilitasi oleh Instansi Pembina.

(4) Organisasi profesi Jabatan Fungsional Manggala Informatika sebagaimana dimaksud pada ayat (1) wajib menyusun kode etik dan kode perilaku profesi.

(5) Organisasi profesi Jabatan Fungsional Manggala Informatika mempunyai tugas:
a. menyusun kode etik dan kode perilaku profesi;
b. memberikan advokasi; dan
c. memeriksa dan memberikan rekomendasi atas pelanggaran kode etik dan kode perilaku profesi.

(6) Kode etik dan kode perilaku profesi sebagaimana dimaksud pada ayat (4) dan ayat (5) huruf a, ditetapkan oleh organisasi profesi Jabatan Fungsional Manggala Informatika setelah mendapat persetujuan dari pimpinan Instansi Pembina.

(7) Ketentuan lebih lanjut mengenai syarat dan tata cara pembentukan organisasi profesi Jabatan Fungsional Manggala Informatika dan hubungan kerja Instansi pembina dengan organisasi profesi Jabatan Fungsional Manggala Informatika diatur lebih lanjut oleh Kepala Badan Siber dan Sandi Negara selaku Pimpinan Instansi Pembina.

Pasal 53

(1) Hubungan kerja antara Instansi Pembina dengan organisasi profesi Jabatan Fungsional Manggala Informatika bersifat koordinatif dan fasilitatif untuk penyelenggaraan tugas dan fungsi pembinaan Jabatan Fungsional Manggala Informatika.

(2) Ketentuan mengenai hubungan kerja instansi pembina dengan organisasi profesi Jabatan Fungsional Manggala Informatika diatur oleh instansi pembina sesuai ketentuan peraturan perundang-undangan.

BAB XVI

KETENTUAN PENUTUP

Pasal 54

Pengangkatan dalam Jabatan Fungsional Manggala Informatika melalui penyesuaian (*inpassing*) sebagaimana dimaksud dalam Pasal 16 dilaksanakan 1 (satu) kali untuk paling lama 2 (dua) tahun sejak Peraturan Menteri ini diundangkan.

Pasal 55

Pembentukan Organisasi Profesi sebagaimana dimaksud dalam Pasal 52 ayat (3) dilaksanakan paling lama 5 (lima) tahun sejak Peraturan Menteri ini diundangkan.

Pasal 56

Ketentuan lebih lanjut mengenai pelaksanaan Jabatan Fungsional Manggala Informatika diatur dengan Peraturan Badan Siber dan Sandi Negara dan Peraturan Badan Kepegawaian Negara sesuai dengan kewenangan masing-masing.

Pasal 57

Peraturan Menteri ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Menteri ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 20 Maret 2020

MENTERI PENDAYAGUNAAN APARATUR NEGARA DAN REFORMASI BIROKRASI REPUBLIK INDONESIA,

ttd

TJAHJO KUMOLO

Diundangkan di Jakarta
pada tanggal 30 Maret 2020

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd

WIDODO EKATJAHJANA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2020 NOMOR 295

Salinan Sesuai Dengan Aslinya
KEMENTERIAN PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI
Kepala Biro Hukum, Komunikasi, dan Informasi Publik,

Andi Rahadian