KEMENTERIAN PERTAHANAN RI
PUSAT DATA DAN INFORMASI

STANDAR OPERASIONAL PROSEDUR
Nomor: SOP/04/VIII/2022/PUSDATIN

TENTANG
PROSEDUR KESESUAIAN TERHADAP PERSYARATAN

DIKELUARKAN DI JAKARTA
TAHUN 2022

BAB I
TUJUAN

1. Tujuan

   Prosedur ini merupakan pedoman dalam pemenuhan kesesuaian terhadap persyaratan yang berlaku, yang memiliki tujuan:

   a. Mencegah pelanggaran terhadap berbagai peraturan yang berlaku.

   b. Memastikan pemenuhan sistem terhadap kebijakan keamanan dan standar organisasi.

   c. Memaksimalkan efektivitas dari hasil proses audit.

BAB II
RUANG LINGKUP

2. Ruang Lingkup

   Prosedur ini mencakup manajemen pemenuhan kesesuaian terhadap persyaratan yang berlaku yang berkaitan dengan Sistem Manajemen Keamanan Informasi pada semua tingkatan dan fungsi di Pusdatin Kemhan RI.

   a. Prosedur ini mengatur tahapan.

   b. Identifikasi Perundangan dan Persyaratan.

   c. Kepatuhan terhadap Hak Kekayaan Intelektual.

   d. Kepatuhan terhadap berbagai Kebijakan Organisasi.

   e. Kepatuhan terkait Audit Sistem Informasi.

   f. Tindaklanjut Ketidakpatuhan.

BAB III
DEFINISI

3. Definisi

   a. Kerentanan keamanan adalah kelamahan-kelemahan keamanan terhadap sistem yang ada, baik sistem IT, sistem fisik, maupun sistem manajemen.

   b. Keamanan Fisik adalah keamanan yang berkaitan dengan aset fisik. Hal ini termasuk berkaitan dengan penanganan aset fisik mupun akses terhadap aset fisik.

   c. Aplikasi Pihak Ketiga adalah aplikasi perangkat lunak yang dibuat oleh pihak di luar.

   d. Insiden adalah terganggunya sebagian atau keseluruhan aktifitas akibat terjadinya sesuatu yang tidak dikehendaki.

   e. Kelemahan adalah hal-hal yang berpotensi menyebabkan terjadinya insiden.

   f. Pelapor adalah Setiap pihak yang menemukan kelemahan gangguan / insiden keamanan informasi.

   g. Insiden Informasi (Information Security Incident) adalah insiden yang disebabkan oleh masalah keamanan informasi.

BAB IV
PROSEDUR DAN TANGGUNG JAWAB

4. Prosedur dan Tanggung Jawab

   a. Identifikasi perundangan dan persyaratan.

      1) Tim Satgas SMKI melakukan identifikasi terhadap undang-undang yang berlaku dan persyaratan kontrak terkait Keamanan Informasi.

      2) Tim Satgas SMKI memastikan semua persyaratan legislatif, hukum, peraturan, kontrak, dan persyaratan organisasi yang relevan dipenuhi.

      3) Tim Satgas SMKI memastikan persyaratan-persyaratan tersebut secara eksplisit diidentifikasi, didokumentasikan,

dan terus *up to date* untuk setiap sistem informasi dan organisasi.

b. Kepatuhan terhadap Hak Kekayaan Intelektual.

1) Tim Satgas SMKI memastikan mendapatkan perangkat lunak hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan hak cipta tidak dilanggar.

2) Tim Satgas SMKI memastikan mendapatkan perangkat lunak hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan hak cipta tidak dilanggar.

3) Tim Satgas SMKI memelihara daftar aset informasi sesuai persyaratan untuk melindungi hak kekayaan intelektual.

4) Tim Satgas SMKI, Kabid dan Kabag terkait memelihara bukti kepemilikan lisensi, master disk, buku manual dan lain sebagainya.

5) Tim Satgas SMKI, Kabid dan Kabag terkait menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki.

6) Tim Satgas SMKI melakukan pemeriksaan bahwa hanya perangkat lunak dan produk berlisensi yang dipasang.

7) Kabid dan Kabag terkait memastikan semua pegawai pada bidang/bagiannya masing-masing patuh terhadap syarat dan kondisi untuk perangkat lunak dan informasi yang didapat dari jaringan publik.

8) Kabid dan Kabag terkait memastikan semua pegawai bidang/bagiannya masing-masing tidak melakukan duplikasi, konversi ke format lain atau mengambil dari rekaman komersial (film atau audio), selain yang diperbolehkan oleh Undang-Undang Hak Cipta.

9) Kabid dan Kabag terkait memastikan semua pegawai bidang/bagiannya masing-masing tidak menyalin secara penuh atau sebagian buku, artikel, laporan, atau dokumen lainnya, selain yang diizinkan oleh Undang-Undang Hak Cipta.

c. Kepatuhan terhadap berbagai Kebijakan Organisasi.

1) Tim Satgas SMKI memastikan kebijakan Sistem Manajemen Keamanan Informasi dilakukan dengan baik dan berkesinambungan.

2) Tim Satgas SMKI memastikan kebijakan *clear desk clear screen* ditetapkan dan diterapkan dengan baik dan berkesinambungan. Kebijakan *clear desk clear screen* ditujukan untuk layar monitor, kertas, fasilitas pengolahan informasi, dan media penyimpanan lainnya.

3) Tim Satgas SMKI memastikan adanya Kebijakan Perlindungan terhadap catatan (rekaman). Catatan harus dilindungi dari kerugian, kerusakan, dan pemalsuan sesuai dengan perundangan, peraturan, kontrak, dan kebutuhan bisnis.

4) Tim Satgas SMKI memastikan adanya kebijakan privasi dan perlindungan informasi pribadi. Privasi dan perlindungan informasi pribadi harus dipastikan sebagaimana disyaratkan dalam perundangan dan peraturan yang berlaku.

5) Tim Satgas SMKI memastikan adanya kebijakan peraturan kontrol kriptografi. Pengendalian Kriptografi harus digunakan sesuai dengan semua kontrak yang relevan, perundangan, dan peraturan yang berlaku.

d. Kepatuhan terkait audit Sistem Manajemen Keamanan Informasi.

1) Tim Satgas SMKI merencanakan pelaksanaan audit Sistem Manajemen Keamanan Informasi yang dilakukan secara berkala atau minimal satu (1) tahun sekali.

2) Koordinator Pelaksana Tim Satgas SMKI menentukan persyaratan audit Sistem Manajemen Keamanan Informasi dan Tim Auditor beserta Ketua Tim Auditor.

3) Pemeriksaan audit oleh Tim Auditor Internal harus mengikuti prosedur Audit Internal Nomor: SOP/25/VIII/2022/ PUSDATIN serta menggunakan formulir Rekapitulasi Pertanyaan dan Temuan Audit Internal Nomor: LI/25C/ VIII/2022/PUSDATIN serta Formulir Evaluasi Kesesuaian Terhadap Persyaratan Nomor: LI/04B/VIII/2022/PUSDATIN.

4) Ketua Satgas SMKI menyetujui persyaratan yang diajukan berikut Ruang Lingkup Auditnya.

5) Ketua Satgas SMKI membatasi proses audit dan memberikan perlakuan khusus pada proses-proses yang dianggap perlu. Proses tersebut antara lain:

   a) Pemeriksaan pada perangkat lunak dan data yang harus dibatasi untuk akses baca saja *(read-only).*

   b) Pemeriksaan pada salinan dari sistem *file* yang diisolasi, yang harus dihapus bila audit telah selesai, atau diberikan perlindungan yang tepat jika ada kewajiban untuk menyimpan file tersebut di bawah persyaratan dokumentasi audit.

6) Auditor Internal Satgas SMKI atau Ketua Tim Auditor yang sudah ditentukan dan ditetapkan oleh Kapusdatin Kemhan RI memastikan Sumber daya untuk melakukan pemeriksaan telah teridentifikasi dan tersedia.

7) Satgas SMKI atau Ketua Tim Auditor memastikan semua akses harus dipantau dan dicatat untuk menghasilkan jejak audit, dan untuk data dan sistem informasi sensitif harus mempertimbangkan pencatatan waktu *(time stamp)* pada jejak audit.

8) Satgas SMKI atau Ketua Tim Auditor memastikan semua prosedur, persyaratan, dan tanggung jawab didokumentasi kan.

e. Tindak Lanjut Ketidakpatuhan

Jika ditemukan ketidakpatuhan, Satgas SMKI melakukan:

1) meminta Kabid/Kabag terkait untuk melakukan tindakan perbaikan yang sesuai. Tindakan Perbaikan harus dirumuskan dengan menggunakan formulir Permintaan Tindakan Perbaikan dan Pencegahan Nomor: LI/24A/VIII /2022/PUSDATIN.

2) mengkaji tindakan perbaikan yang telah dilakukan untuk memastikan ketidakpatuhan sudah diperbaiki sesuai persyaratan yang berlaku agar ketidakpatuhan tidak terulang kembali.

BAB IV
DOKUMEN PENDUKUNG

4 Dokumen Pendukung

a. Prosedur Komunikasi Internal dan Eksternal Manajemen Sistem Nomor: SOP/02/VIII/2022/PUSDATIN.

b. Prosedur Manajemen Perubahan Nomor: SOP/03/VIII/2022/ PUSDATIN.

c. Prosedur Audit Internal Nomor: SOP/25/VIII/2022/PUSDATIN.

d. Prosedur Tindakan Perbaikan dan Pencegahan Nomor: SOP/24/ VIII/2022/PUSDATIN.

BAB V
REKAMAN PENDUKUNG

5 Rekaman Pendukung

a. Formulir Sasaran Keamanan Informasi Nomor: LI/04A/VIII/2022 /PUSDATIN.

b. Formulir Evaluasi Kesesuaian Terhadap Persyaratan Nomor: LI/04B/VII/2022/PUSDATIN.

c. Formulir Rekapitulasi Temuan Audit Internal Nomor: LI/25D /VII/2022/PUSDATIN.

d. Formulir Permintaan Tindakan Perbaikan dan Pencegahan Nomor: LI/24A/VIII/2022/PUSDATIN.

BAB VI
RUJUKAN

6 Rujukan

a. Sistem Manajemen Keamanan Informasi ISO 27001:2013 klausul 4. *Context of the Organization.*

b. Sistem Manajemen Keamanan Informasi ISO 27001:2013 klausul 4.1 *Understanding the Organization and its context.*

c. Sistem Manajemen Keamanan Informasi ISO 27001:2013 klausul 4.2 *Understanding the needs and expectations of interested parties*.

d. Sistem Manajemen Keamanan Informasi ISO 27001:2013 klausul 4.3 *Determining the Scope of the Information Security Management System.*

e. Sistem Manajemen Keamanan Informasi ISO 27001:2013 klausul 4.4 *Information Security Management System.*

f. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.5 *Information Security Policies.*

g. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.5.1 *Management direction for information Security.*

h. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.5.1.1 *Policies for Information Security.*

i. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.5.1.2 *Review of the Policies for Information Security.*

j. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.7.2.1 *Management Responsibilities.*

k. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.11.2.9 *Clear Desk and Clear Screen Policy.*

l. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.18 *Compliance.*

m. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.18.1 *Compliance with Legal and Contractual Requirements.*

n. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.18.1.1 *Identification of Applicable Legislation and Ccontractual Requirements.*

o. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.18.1.2 *Intellectual Property Rights.*

p. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.18.1.3 *Protection of Records.*

q. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.18.1.4 *Privacy and Protection of Personally Identifiable Information.*

r. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.18.1.5 *Regulation of Cryptographic Controls.*

s. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.18.2 *Information Security Reviews.*

t. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.18.2.1 *Independent Review of Information Security.*

u. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.18.2.2 *Compliance with Security Policies and Standards.*

BAB VII
PENUTUP

7 Penutup

a. Demikian SOP Kesesuaian Terhadap Persyaratan ini di buat, sebagai acuan dalam pengamanan informasi di Pusdatin.

b. Pedoman ini berlaku sejak di tandatangani dan ketentuan yang belum tercantum dalam pedoman ini akan diatur lebih lanjut dengan memperhatikan perkembangan Sistem Manajemen Keamanan Informasi.

c. Dokumen asli dari prosedur ini dipelihara dan dikendalikan oleh Dokumen Kontrol di Bidang Pamsisinfosan Pusdatin Kemhan RI.

d. Penggunaan dokumen asli ataupun dokumen salinan harus mengikuti aturan yang tertulis pada Dokumen Prosedur Pengendalian Dokumen Nomor: SOP/22/VIII/2022/PUSDATIN.

Dikeluarkan di Jakarta
Pada tanggal Agustus 2022

Kepala Pusat Data dan Informasi,

Rionardo
Brigadir Jenderal TNI

Lampiran

a. Formulir Sasaran Keamanan Informasi Nomor: LI/04A/VI/2022/ PUSDATIN.

b. Formulir Evaluasi Kesesuaian Terhadap Persyaratan Nomor: LI/04B/ VI/2022/PUSDATIN.

c. Formulir Rekapitulasi Temuan Audit Internal Nomor:LI/25D/VI/2022/ PUSDATIN.

d. Formulir Permintaan Tindakan Perbaikan dan Pencegahan Nomor: LI/24A/VI/2022/PUSDATIN.