KEMENTERIAN PERTAHANAN RI
PUSAT DATA DAN INFORMASI

STANDAR OPERASIONAL PROSEDUR
Nomor: SOP/16/VIII/2022/PUSDATIN

TENTANG
PROSEDUR AKUISISI PEMELIHARAAN TEKNOLOGI INFORMASI

DIKELUARKAN DI JAKARTA
TAHUN 2022

BAB I
TUJUAN

1. Tujuan

   Prosedur ini merupakan petunjuk dalam pelaksanaan akuisisi, pengembangan, dan pemeliharaan sistem informasi, yang memiliki tujuan :

   a. Memastikan bahwa keamanan adalah bagian yang utuh dari sistem informasi.

   b. Mencegah kesalahan atau modifikasi informasi dalam aplikasi.

   c. Memastikan keamanan *system files.*

   d. Memelihara keamanan perangkat lunak sistem aplikasi dan informasi

BAB II
RUANG LINGKUP

2. Ruang Lingkup

   Prosedur ini mencakup Manajemen akuisisi, pengembangan, dan pemeliharaan sistem informasi yang berkaitan dengan sistem manajemen Keamanan Informasi pada semua tingkatan dan fungsi di Pusdatin Kemhan RI. Prosedur ini mengatur tahapan:

   a. Spesifikasi kebutuhan perangkat informasi.

   b. Pengolahan data aplikasi.

   c. Pengendalian perangkat lunak pada sistem operasional.

   d. Perlindungan terhadap sistem pengujian data.

   e. Pengendalian akses ke kode program.

   f. Anti *malicious code.*

BAB III
DEFINISI

3. Definisi

a. *Security Hole* adalah kelemahan-kelemahan *security* 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 maupun akses terhadap aset fisik.

c. Aplikasi *Third Party* adalah aplikasi perangkat lunak yang dibuat oleh pihak di luar perusahaan.

d. Insiden adalah terganggunya sebagian atau keseluruhan aktivitas Pusdatin Kemhan RI akibat terjadinya sesuatu yang tidak dikehendaki.

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

f. *Malicious Code* adalah program atau kode berbahaya yang digunakan untuk menyusup atau mengganggu kinerja perangkat lunak atau komputer.

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

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

BAB IV
PROSEDUR DAN TANGGUNG JAWAB

4. Prosedur dan Tanggung Jawab

a. Spesifikasi Kebutuhan Perangkat Informasi

Kabid Infratik memastikan Spesifikasi kebutuhan perangkat pengolah informasi yang dikembangkan baik oleh internal Pusdatin Kemhan atau pihak ketiga harus didokumentasikan secara formal.

b. Pengolahan Data Aplikasi

1) Kabid Banglolasisfohan memastikan diterapkannya masukan rangkap *(dual input)* atau mekanisme pengecekan masukan lainnya
untuk mendeteksi kesalahan berikut:

a) Di luar rentang/batas nilai-nilai yang diperbolehkan.

b) Karakter tidak valid dalam *field data*.

c) Data hilang atau tidak lengkap.

d) Melebihi batas atas dan bawah volume data, dan

e) Data yang tidak diotorisasi dan tidak konsisten.

2) Kabid Banglolasisfohan memastikan diterapkannya Pengkajian secara berkala terhadap isi *field* kunci *(key field)* atau file data untuk
mengkonfirmasi keabsahan dan integritas data.

3) Kabid Infratik memastikan diperiksanya dokumen *hard copy* untuk memastikan tidak adanya perubahan data masukan yang tidak melalui otorisasi.

4) Kabid Infratik memastikan ditampilkannya pesan yang sesuai dalam menanggapi kesalahan validasi.

5) Kabid Infratik memastikan diterapkannya aturan untuk menguji kewajaran dari data masukan.

6) Kabid Infratik memastikan di uraikannya tanggung jawab dari semua pegawai yang terkait dalam proses perekaman data.

7) Kabid Infratik memastikan Sistem mampu membuat dan mengeluarkan catatan aktivitas terkait proses perekaman data.

8) Kabid Infratik memastikan diterapkannya penyusunan daftar pemeriksaan *(check list)* yang sesuai, mendokumentasikan proses pemeriksaan, dan menyimpan hasilnya secara aman.

Proses pemeriksaan mencakup, tetapi tidak terbatas pada:

a) Pengendalian session atau batch, untuk mencocokkan data setelah perubahan transaksi.

b) Pengendalian balancing untuk memeriksa data sebelum dan sesudah transaksi.

c) Validasi data masukan yang dihasilkan sistem.

d) Keutuhan dan keaslian data yang diunduh/ diunggah *(download/ upload)*.

e) Aplikasi berjalan sesuai dengan rencana dan waktu yang ditentukan.

f) Program dijalankan dalam urutan yang benar dan menghentikan sementara jika terjadi kegagalan sampai masalah diatasi. Dan

g) Sistem mampu membuat dan mengeluarkan catatan aktivitas pengelolaan internal.

9) Kabid Infratik memastikan diterapkannya Pemeriksaan data keluaran dengan mempertimbangkan, tetapi tidak terbatas pada:

a) Kewajaran dari data keluaran yang dihasilkan.

b) Pengendalian rekonsiliasi data untuk memastikan kebenaran pengolahan data.

c) Menyediakan informasi yang cukup untuk pengguna atau sistem pengolahan informasi untuk menentukan akurasi, kelengkapan, ketepatan, dan klasifikasi informasi.

d) Aturan untuk menindaklanjuti validasi data keluaran.

e) Menguraikan tanggung jawab dari semua pegawai yang terkait proses data keluaran. Dan

f) Sistem mampu membuat dan mengeluarkan catatan aktivitas dalam proses validasi data keluaran.

c. Pengendalian Perangkat Lunak Pada Sistem Operasional

1) Kabid Infratik memastikan bahwa Proses pemutakhiran perangkat lunak operasional, aplikasi, *library program* hanya boleh dilakukan oleh system administrator terlatih setelah melalui proses otorisasi.

2) Kabid Infratik memastikan bahwa Sistem operasional hanya berisi program aplikasi *executable* yang telah diotorisasi, tidak boleh berisi kode program atau compiler.

3) Kabid Infratik memastikan bahwa Aplikasi dan perangkat lunak sistem operasi hanya dapat diimplementasikan setelah melewati proses pengujian yang ekstensif.

4) Kabid Infratik memastikan bahwa Sistem pengendalian konfigurasi harus digunakan untuk mengendalikan seluruh perangkat lunak yang telah diimplementasikan beserta dokumentasi sistem.

5) Kabid Infratik memastikan bahwa Strategi *rollback* harus tersedia sebelum suatu perubahan diimplementasikan.

6) Kabid Infratik memastikan bahwa Catatan audit harus dipelihara kemutakhiran *library program* operasional.

7) Kabid Infratik memastikan bahwa Versi terdahulu dari suatu aplikasi harus tetap disimpan untuk keperluan kontingensi.

8) Kabid Infratik memastikan bahwa Versi lama dari suatu perangkat lunak harus diarsip, bersama dengan informasi terkait dan prosedur, parameter, konfigurasi rinci dan perangkat lunak pendukung.

d. Perlindungan Terhadap Sistem Pengujian Data

1) Kabid Infratik memastikan bahwa aturan pengendalian akses, yang berlaku pada sistem aplikasi operasional, harus berlaku juga pada sistem aplikasi pengujian.

2) Kabid Infratik memastikan bahwa proses otorisasi setiap kali informasi/ data operasional digunakan pada sistem pengujian.

3) Kabid Infratik memastikan bahwa Penghapusan informasi/ data operasional yang digunakan pada sistem pengujian segera dilakukan setelah proses pengujian selesai.

4) Kabid Infratik memastikan bahwa Pencatatan terhadap jejak audit penggunaan informasi/ data operasional dilakukan.

e. Pengendalian Akses ke Kode *Program*

1) Kabid Infratik memastikan bahwa Kode program tidak boleh disimpan pada sistem operasional.

2) Kabid Infratik memastikan bahwa Pengelolaan kode program dan *library* harus mengikuti aturan yang telah ditetapkan.

3) Kabid Infratik memastikan bahwa Pengelola Teknologi Informasi dan Komunikasi tidak boleh memiliki akses yang tidak terbatas ke kode program dan *library*.

4) Kabid Infratik memastikan bahwa Proses pemutakhiran kode program dan item terkait, serta pemberian kode program kepada programmer hanya dapat dilakukan setelah melalui proses otorisasi.

5) Kabid Infratik memastikan bahwa Daftar program disimpan dalam secure areas.

6) Kabid Infratik memastikan bahwa Catatan audit dari seluruh akses ke kode program dan *library* dipelihara

f. *Anti Malicious Code*

1) Kabid Pamsisinfosan melakukan Identifikasi Sistem Anti *Malicious Code.*

2) Sistem Anti *Malicious Code* yang digunakan adalah:

a) *Firewall*

b) *Antivirus system* versi terbaru digunakan pada perangkat *Server dan Client.*

3) Sistem Anti *Malicious Code* digunakan pula pada removable media, yaitu :

a) *Antivirus system* versi terbaru digunakan pada Flash Disk.

b) *Antivirus system* versi terbaru digunakan pada External HD.

4) Otorisasi telah ditentukan pada Akses Jaringan, yaitu :

a) *File Server* diberikan pada seluruh pengguna umum berupa *"read only-edit-create-delete" .*

b) *Shared Folder* diberikan pada pengguna tertentu berupa *"read only-edit-create-delete" .*

5) Jika dilakukan, Kabid Pamsisinfosan memastikan Perubahan Sistem Anti Malicious Code dilakukan dengan benar. Kriteria Sistem
Anti *Malicious Code* yang digunakan harus:

a) Mampu melakukan pembaruan *(update virus definitions).*

b) Mampu *Scanning* semua jenis File.

c) Mampu menghapus atau karantina File terinfeksi.

d) Memberikan informasi lengkap *Malicious Code* yang ditemukan.

e) Mampu memantau dan melaporkan secara lengkap hasil Scan.

BAB VI
DOKUMEN PENDUKUNG

6) Dokumen Pendukung

a. Prosedur Manajemen Perangkat Pengolah Data Bergerak Nomor: SOP/10/VIII/2022/PUSDATIN.

b. Prosedur Pemeliharaan Dan Perbaikan Perangkat Teknologi Informasi Nomor: SOP/13/VIII/2022/PUSDATIN.

c. Prosedur *Disposal,Reuse,Removal* Perangkat Teknologi Informasi Nomor: SOP/14/VIII/2022/PUSDATIN.

d. Prosedur Pengembangan Sistem Teknologi Informasi Nomor: SOP/17/VIII/2022/PUSDATIN.

BAB VII
RUJUKAN

7) Rujukan

a. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Klausul 8. *Operation.*

b. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Klausul 8.1 *Operational Planning And Control.*

c. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.4.4 *Use Of Privileged Utility Programs.*

d. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.9.4.5 *Access Control To Program Source Code.*

e. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.12.5 *Control Of Operational Software.*

f. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.12.5.1 *Installation Of Software On Operational Systems.*

g. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.12.6 *Technical Vulnerability Management.*

h. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.12.6.1 *Management Of Technical Vulnerabilities.*

i. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.12.6.2 *Restrictions On Software Installation.*

j. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.14.2.1 *Secure Development Policy.*

k. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.14.2.5 *Secure System Engineering Principles.*

l. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.14.2.6 *Secure Development Environment.*

m. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.14.2.7 *Outsourced Development.*

n. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.14.2.8 *System Security Testing.*

o. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.14.2.9 *System Acceptance Testing.*

p. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.14.3 *Test Data.*

q. Sistem Manajemen Keamanan Informasi ISO 27001:2013 Annex A.14.3.1 *Protection Of Test Data.*

BAB VIII
PENUTUP

8 Penutup

a. Demikian SOP Akuisisi Pemeliharaan Tekhologi Informasi 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