LAPORAN INDIVIDU EVALUASI IMPLEMENTASI SPBE

EVALUASI IMPLEMENTASI SPBE PADA ASPEK KEAMANAN DAN MANAJEMEN ASET TIK DI KANTOR WILAYAH KEMENTERIAN HUKUM KALIMANTAN TENGAH

DISUSUN:

NAMA : SALSABILLA ARYANING PUTRI
NIP : 200104062025062015
JABATAN : PRANATA KOMPUTER AHLI PERTAMA
SATUAN KERJA : KANTOR WILAYAH KEMENTERIAN HUKUM KALIMANTAN TENGAH

PELATIHAN TEKNIS TATA KELOLA DAN MANAJEMEN SPBE
PUSAT DATA DAN TEKNOLOGI INFORMASI
BALAI PELATIHAN HUKUM SEMARANG
KEMENTERIAN HUKUM REPUBLIK INDONESIA
2026

PENGANTAR

SPBE memanfaatkan TIK untuk mendukung pelaksanaan tugas pemerintahan secara aman, efektif, dan berkelanjutan.

Di Kanwil Kementerian Hukum Kalimantan Tengah, pengelolaan SPBE telah didukung oleh:

- Inventarisasi aset TIK
- Monitoring keamanan jaringan & hak akses
- Dokumen Manajemen Risiko, Keamanan Informasi, dan Aset TIK

Fokus Evaluasi:
Melihat penguatan pada Keamanan dan Manajemen Aset TIK, khususnya:

- Data aset & pengguna
- Akun/email kantor
- Recovery perangkat
- Backup & keberlangsungan data

PELAKSANAAN KEGIATAN

01.

Pelaksanaan Kegiatan
Evaluasi dilakukan melalui pengumpulan dokumen, identifikasi kondisi SPBE, pemetaan keamanan dan aset TIK, serta analisis kesenjangan untuk menghasilkan rekomendasi dan rencana tindak lanjut penguatan SPBE.

02.

Tahapan Kegiatan:

1. Identifikasi kondisi SPBE
2. Inventarisasi informasi & dokumen
3. Identifikasi keamanan & aset TIK
4. Identifikasi risiko
5. Penentuan kondisi yang diharapkan
6. Analisis kesenjangan
7. Rekomendasi & tindak lanjut

03.

Objek evaluasi:
Implementasi SPBE pada aspek Keamanan dan Manajemen Aset TIK untuk mendukung keamanan serta keberlangsungan pelaksanaan tugas kedinasan berbasis elektronik.

04.

Batasan Evaluasi
Evaluasi berfokus pada Keamanan dan Manajemen Aset TIK berdasarkan dokumen dan kondisi internal yang tersedia, tanpa mencakup pengujian teknis mendalam maupun pengujian pemulihan data dan perangkat secara menyeluruh.

KONDISI SAAT INI

Evaluasi difokuskan pada dua area yang saling berkaitan, yaitu Keamanan dan Manajemen Aset TIK. Fokus tersebut dipilih karena pengelolaan perangkat kedinasan tidak hanya membutuhkan pencatatan aset secara fisik, tetapi juga membutuhkan pengendalian akses, kesiapan pemulihan perangkat, dan perlindungan terhadap data yang digunakan dalam pelaksanaan pekerjaan.

01

Manajemen Aset TIK
Inventarisasi aset TIK telah dilakukan.
Data aset menjadi dasar pemetaan dan perencanaan kebutuhan.
Perlu diperkuat dengan informasi pengguna, akun, recovery, dan backup.

02

Keamanan Perangkat & Akses
Monitoring keamanan jaringan dan hak akses telah berjalan.
Screening perangkat end user telah dilakukan.
Perlu penguatan pengelolaan akun dan kesiapan recovery perangkat.

03

Backup & Keberlangsungan Data
Media penyimpanan digital telah tersedia.
Mekanisme backup perlu diperjelas terkait data, frekuensi, lokasi, penanggung jawab, dan pemulihan.
Perlu memastikan backup berkala dan dapat dipulihkan.

GAP ANALYSIS

Area	Kondisi Saat Ini	Kondisi Diharapkan	Gap/Risiko
Aset TIK	Inventaris perangkat telah tersedia.	Inventaris mutakhir dan terhubung dengan pengguna serta informasi pengelolaan digital.	Data aset masih perlu diperkuat dengan informasi pengguna, akun, recovery, dan backup.
Akun perangkat	Akun/email kantor digunakan pada perangkat, tetapi belum terlihat sebagai bagian dari inventaris aset secara terpusat.	Akun terkait perangkat terdokumentasi dan dikelola pihak berwenang.	Kesulitan identifikasi akun ketika terjadi gangguan akses; risiko pengelolaan akses.
Recovery	Mekanisme recovery perangkat perlu diperjelas dan didokumentasikan.	Tersedia prosedur recovery dan informasi recovery yang aman.	Gangguan perangkat berpotensi lebih lama apabila recovery tidak siap.
Backup data	Media penyimpanan digital tersedia, tetapi mekanisme backup belum terstandar/terverifikasi.	Backup data penting berkala dan dapat dipulihkan.	Risiko kehilangan data ketika perangkat rusak, terkunci, atau di-reset.
Monitoring	Monitoring jaringan dan hak akses telah berjalan.	Monitoring juga mencakup kesiapan recovery dan keberlangsungan data.	Ketahanan operasional perangkat perlu diperkuat.

KONDISI YANG DIHARAPKAN

- Data aset TIK mutakhir dan dapat ditelusuri sampai pengguna serta informasi pengelolaan digital perangkat.
- Akun/email kantor yang digunakan pada perangkat kedinasan terdokumentasi dan dikelola melalui mekanisme resmi.
- Informasi recovery perangkat tersedia melalui mekanisme yang aman dan hanya dapat diakses oleh pihak yang berwenang.
- Prosedur penanganan perangkat terkunci atau rusak tersedia, yang mencakup verifikasi, recovery, backup, dan eskalasi.
- Data kerja penting memiliki backup secara berkala pada media atau layanan yang ditetapkan organisasi.
- Keberhasilan backup dapat diverifikasi dan proses pemulihan data dapat diuji secara berkala.
- Perubahan pengguna, perangkat, akun, kerusakan, penggantian, dan pemindahan aset dicatat serta diperbarui secara berkala.

REKOMENDASI & TINDAK LANJUT

- Memutakhirkan data aset TIK secara berkala, termasuk informasi pengguna dan status perangkat.
- Mendata akun/email kantor dan mengelolanya melalui mekanisme yang aman.
- Mengelola informasi recovery perangkat secara aman dan terbatas.
- Menyusun/menyempurnakan SOP penanganan gangguan perangkat, termasuk recovery, backup, dan eskalasi.
- Melaksanakan backup data secara berkala pada media/layanan resmi.
- Melakukan uji pemulihan data untuk memastikan backup dapat digunakan.
- Melakukan monitoring dan evaluasi berkala terhadap aset, akun, keamanan, recovery, dan backup.

No.	Rencana Tindak Lanjut	Output	Waktu Pelaksanaan
1	Melakukan pemutakhiran data aset TIK dan informasi pengguna perangkat	Data aset TIK yang mutakhir	0–30 hari
2	Melakukan pendataan dan pemetaan akun/email kantor dengan perangkat atau layanan yang digunakan	Daftar/pemetaan akun dan perangkat	0–30 hari
3	Menetapkan mekanisme pengelolaan recovery perangkat	Mekanisme dan dokumentasi recovery	0–60 hari
4	Menyusun atau menyempurnakan SOP penanganan gangguan perangkat	SOP penanganan gangguan perangkat	0–60 hari
5	Menetapkan dan melaksanakan backup data kerja secara berkala	Backup data dan dokumentasi pelaksanaan	0–90 hari
6	Melakukan uji pemulihan terhadap data yang telah dibackup	Bukti uji pemulihan data	0–90 hari
7	Melakukan monitoring dan evaluasi terhadap pelaksanaan pengelolaan aset, keamanan, recovery, dan backup	Laporan monitoring dan tindak lanjut	Berkala

KESIMPULAN & PENUTUP

Evaluasi menunjukkan bahwa pengelolaan SPBE telah memiliki dasar pada aspek Keamanan dan Manajemen Aset TIK, namun masih perlu penguatan pada pemutakhiran aset, pengelolaan akun, recovery perangkat, serta backup dan pemulihan data. Rekomendasi yang disusun diharapkan dapat mendukung perbaikan secara bertahap sehingga keamanan aset dan data semakin terjaga serta penyelenggaraan SPBE berjalan efektif, aman, dan berkelanjutan.

01

Pengelolaan SPBE telah memiliki dasar yang cukup, melalui inventarisasi aset TIK, pengelolaan keamanan jaringan, hak akses, serta dokumen terkait keamanan dan manajemen aset TIK.

02

Masih terdapat aspek yang perlu diperkuat, terutama dalam keterhubungan data aset dengan pengguna dan akun, kesiapan recovery perangkat, serta pengelolaan backup data.

03

Keberlangsungan data perlu menjadi perhatian, dengan memastikan data penting dibackup secara berkala dan dapat dipulihkan apabila terjadi gangguan pada perangkat.

04

Penguatan tata kelola dan dokumentasi diperlukan agar pengelolaan aset, keamanan, recovery, dan backup dapat dilakukan secara lebih tertib, aman, dan berkelanjutan.

TERIMA KASIH