

## **BAB V**

### **KESIMPULAN DAN SARAN**

#### **5.1. Kesimpulan**

Berdasarkan audit keamanan informasi pada Sistem Informasi Anggota KPU dan Badan Adhoc di KPU Kota Cimahi menggunakan standar ISO 27001:2013, terdapat beberapa area yang memerlukan perbaikan dalam Standard Operating Procedure (SOP) untuk meningkatkan keamanan dan efektivitas sistem. Kesimpulan dari audit ini mengindikasikan beberapa langkah perbaikan yang perlu diterapkan:

1. Peningkatan Kontrol Akses: SOP perlu diperbaiki dengan pengetatan kontrol akses terhadap sistem informasi. Hanya personel yang berwenang dan terlatih yang diizinkan mengakses data sensitif. Penggunaan autentikasi multi-faktor juga disarankan untuk memperkuat keamanan.
2. Manajemen Risiko yang Lebih Ketat: SOP harus mencakup proses identifikasi, evaluasi, dan mitigasi risiko secara rutin. Setiap potensi ancaman keamanan informasi harus diidentifikasi dan ditangani sebelum berdampak signifikan.
3. Peningkatan Kesadaran Keamanan Informasi: Program pelatihan dan kesadaran keamanan informasi bagi seluruh staf perlu dimasukkan ke dalam SOP untuk memastikan bahwa semua personel memahami pentingnya menjaga keamanan informasi.
4. Pemantauan dan Audit Berkala: SOP harus mencakup jadwal pemantauan dan audit keamanan informasi secara berkala untuk memastikan bahwa kebijakan keamanan yang diimplementasikan tetap efektif dan relevan dengan perkembangan teknologi.
5. Pengelolaan Insiden Keamanan Informasi: SOP perlu mencakup prosedur yang jelas untuk melaporkan, mengelola, dan menyelesaikan insiden keamanan informasi dengan cepat dan efisien, termasuk proses dokumentasi dan pembelajaran dari insiden yang terjadi.

Dengan mengimplementasikan perbaikan ini, KPU Kota Cimahi dapat meningkatkan keamanan dan integritas data, memastikan kepatuhan terhadap standar ISO 27001:2013, serta meminimalkan risiko yang terkait dengan pengelolaan sistem informasi.

## **5.2. Saran**

Saran Perbaikan Berdasarkan Audit Keamanan Informasi Menggunakan ISO 27001:2013 di KPU Kota Cimahi :

1. Perlu melakukan peningkatan kontrol akses terapkan mekanisme kontrol akses yang lebih ketat, termasuk penggunaan autentikasi multi-faktor untuk semua pengguna, serta pembatasan akses berdasarkan peran dan kebutuhan.
2. Pengembangan kebijakan manajemen risiko, implementasikan prosedur manajemen risiko yang lebih komprehensif dengan identifikasi, evaluasi, dan mitigasi risiko yang berkelanjutan. Buat daftar risiko yang selalu diperbarui dan lakukan penilaian risiko secara berkala di KPU Kota Cimahi
3. Perlunya dilakukan pelatihan keamanan informasi tingkatkan program pelatihan untuk seluruh staf, terutama yang berhubungan langsung dengan pengelolaan sistem informasi. Pastikan staf memahami pentingnya kebijakan keamanan dan cara menghindari ancaman keamanan.