

BAB V PENUTUP

5.1 Kesimpulan

Kesimpulan yang diperoleh dari penelitian ini ialah:

- A. Risiko – risiko keamanan teknologi informasi pada laboratorium komputer FIK UPNVJ ditemukan meliputi kerentanan fisik, kerentanan perangkat lunak, kerentanan jaringan, dan kelemahan atau kurangnya kesadaran pemahaman pengguna. Tingkat risiko yang ada keamanan informasi pada laboratorium komputer FIK UPNVJ cukup tinggi. Hal ini didasarkan pada temuan yang didapat melakukan observasi dan wawancara pada laboran laboratorium komputer, melakukan penilaian risiko pada aset laboratorium komputer, dan mengikuti panduan ISO 27001:2022 terkait kebijakan keamanan informasi.
- B. Dokumen kebijakan IT *Risk control* untuk laboratorium komputer FIK UPNVJ mencakup panduan untuk mengidentifikasi, mengelola risiko keamanan informasi, serta memuat tanggung jawab untuk pihak yang berwenang dan pengguna untuk mengikuti kebijakan keamanan dan menegakkan nilai disiplin dalam penerapan praktik keamanan.
- C. Rekomendasi dan solusi keamanan teknologi informasi laboratorium komputer didasarkan pada nilai kekurangan, tingkat risiko, dan kondisi langsung yang didapatkan di lapangan. Rekomendasi dan solusinya yaitu Meningkatkan keamanan terkait aset fisik laboratorium komputer, Meningkatkan aktivitas pemantauan terhadap aset fisik, menjalankan operasional keamanan informasi dengan peran yang memadai dan berkualifikasi, mengadakannya pelatihan terhadap pengguna dan pihak yang berwenang terkait untuk meningkatkan kesadaran pengguna terkait keamanan informasi, Memelihara aset laboratorium komputer dengan berkesinambungan dan beradaptasi dengan kemajuan teknologi informasi.

5.2 Saran

Berdasarkan penelitian yang telah dilakukan terkait Information Technology (IT) *Risk Control* dalam Laboratorium Komputer FIK UPNVJ dengan menggunakan ISO 27001:2022 memiliki cakupan yang luas untuk dikembangkannya lagi mengenai judul penulis ambil. Oleh karena itu, peneliti mencoba memberikan saran untuk penelitian selanjutnya sebagai berikut:

1. Bagi para peneliti selanjutnya sebaiknya dapat mengukur tingkat keamanan khususnya Sistem Manajemen Keamanan informasi menggunakan *Framework* yang lebih terkini dan terbaru untuk melindungi lebih efektif.
2. Bagi para peneliti selanjutnya dapat mengevaluasi dengan menambahkan responden dan *Annex* atau klausul ISO yang terbaru.
3. Dikarenakan peneliti memilih skala yang lingkupnya masih kecil dan masih umum menyeluruh dalam pemeriksaan keamanan informasi menggunakan ISO 27001. Maka diharapkan peneliti selanjutnya dapat membuat lingkup yang lebih besar dan spesifik serta menggunakan metode yang lebih efektif dan efisien.
4. Diharapkan juga untuk peneliti selanjutnya menggunakan rumus yang terbaru dan dapat mendapat nilai lebih spesifik untuk menentukan nilai risiko, ancaman, dan sebagainya