

## ABSTRAK

Pengamanan data merupakan suatu cara khusus untuk mengamankan sebuah data atau informasi yang berada di dalam perangkat fisik yang bisa menunjang keamanan data yang dimiliki sebuah organisasi. Dalam hal ini penjagaan keamanan informasi berarti pula perlunya usaha organisasi dalam memperhatikan faktor keamanan dari keseluruhan piranti pendukung, jaringan dan fasilitas lain yang terkait langsung maupun tidak langsung dengan proses pengolahan data. DISDUKCAPIL tentunya didukung dengan perangkat fisik yang menunjang untuk melakukan segala aktivitas pelayanan masyarakat, namun DISDUKCAPIL dihadapkan pada sejumlah ancaman keamanan informasi dari berbagai sumber berupa intervensi manusia seperti pencurian, perusakan, aktivitas *wiretapping* dan sabotase terhadap perangkat fisik serta ancaman yang disebabkan oleh perangkat itu sendiri yang dapat mengganggu aktivitas bahkan menyebabkan proses bisnis terhenti.

Standar Operasional Prosedur (SOP) keamanan perangkat fisik pada SIAK disusun sebagai keamanan informasi untuk mencegah dan meminimalisir sejumlah ancaman yang dapat menimbulkan risiko di DISDUKCAPIL Kota Bandung. Penyusunan SOP ini melalui berbagai tahapan seperti pemahaman studi literatur atau referensi, mengidentifikasi risiko terkait keamanan perangkat fisik, menganalisis keamanan perangkat fisik di tempat penelitian, melakukan analisis GAP, melakukan penilaian risiko, dan penyusunan SOP yang disesuaikan dengan pendekatan standar keamanan informasi, yaitu ISO27001:2013 pada klausul A.11.2 mengenai *equipment*.

Penelitian ini menghasilkan rekomendasi Standar Operasional Prosedur Keamanan Perangkat Fisik pada SIAK Berdasarkan ISO27001:2013. SOP ini diharapkan dapat mengimbangi peningkatan pemanfaatan teknologi informasi dalam hal keamanan perangkat fisik di DISDUKCAPIL Kota Bandung.

**Kata Kunci :** Teknologi Informasi, Perangkat Fisik, Standar Operasional Prosedur (SOP), ISO27001, Penyusunan Standar Operasional Prosedur Perangkat Fisik berdasarkan ISO27001:2013.

## ABSTRACT

Data security is a special way to secure a data or information that is within the physical devices that can support the security of the data belonging to an organization. In this case the guardianship information security means also the need for the Organization's efforts in that regard for the safety factor of the overall network of supporters, and any other facility that is associated directly or indirectly with data processing. DISDUKCAPIL course is supported with physical devices that support to do all activities of community service, but the DISDUKCAPIL are exposed on a number of security threat information from various sources in the form of human intervention such as theft, tampering, wiretapping activity and sabotage of physical devices as well as the threats caused by the device itself which can interfere with the activity of even causing business process at a standstill.

Standard Operational Procedure (SOP) physical security devices on the SIAK conceived as a security information to prevent and minimize the number of threats that could pose a risk in the DISDUKCAPIL city of Bandung. Preparation of the SOP this through various phases such as the understanding of the study of literature or reference, identifying risks related to physical security devices, analyse the physical device security in place of research, conducting analyses of GAP, do penilian risks, and the preparation of the SOP that are adapted to the standard approach to information security, i.e. ISO27001:2013 on clause a. 11.2 regarding equipment.

This research resulted in the recommendation of the operational standards of physical Device security procedures on the SIAK based on ISO27001:2013. SOP is expected to offset the increased utilization of information technology in terms of the physical device security DISDUKCAPIL in Bandung.

**Keywords** : *Information technology, physical devices, Standard Operational procedures (SOP), ISO27001, preparation of Standard Operational procedure of physical devices based on ISO27001:2013.*