ABSTRAK

Perkembangan teknologi informasi (TI) semakin canggih dan meluas, penggunaan TI tersebut sudah menjadi kebutuhan dan tuntutan disetiap lembaga manapun. Pemanfaatan TI tidak terlepas dari perangkat keras *(hardware)* komputer untuk menunjang berjalannya sebuah sistem. Semakin canggih teknologi informasi terkadang tidak diikuti dengan penerapan keamanan yang memadai. Begitu pula Fakultas Teknik Universitas Pasundan belum menerapkan aturan mengenai keamanan *hardware*, sehingga organisasi atau perusahaan dihadapkan pada sejumlah ancaman yang dapat mengganggu aktifitas bahkan menyebabkan terhentinya proses bisnis.

Standar Operasional Prosedur (SOP) keamanan *hardware* disusun sebagai keamanan informasi untuk mencegah dan meminimalisir sejumlah ancaman yang dapat menimbulkan resiko di Fakultas Teknik Universitas Pasundan. Penyusunan SOP ini melalui berbagai tahapan seperti pemahaman studi literatur atau referensi, mengidentifikasi permasalahan yang terjadi terkait keamanan *hardware*, menganalisis keamanan *hardware* di tempat penelitian, melakukan penilaian resiko, melakukan analisa gap, dan penyusunan SOP yang disesuaikan dengan pendekatan standar keamanan informasi, yaitu ISO27001:2005 pada klausa A.9.2 mengenai keamanan peralatan. Tujuan dari standar pada klausa keamanan peralatan untuk mencegah kehilangan, kerusakan, pencurian atau ketidakberesan aset dan gangguan terhadap aktifitas organisasi atau perusahaan.

Penelitian ini menghasilkan rekomendasi Standar Operasional Prosedur Keamanan *Hardware* Berdasarkan Pendekatan ISO 27001:2005. SOP ini diharapkan dapat mengimbangi peningkatan pemanfaatan teknologi informasi dalam hal keamanan informasi di Fakultas Teknik Universitas Pasundan.

Kata Kunci : *Teknologi Informasi, Perangkat Keras (Hardware), Standar Operasional Prosedur (SOP), ISO27001.*

ABSTRACT

The development of information technology (IT) is becoming more sophisticated and extends, the IT usage has become a requirement and the demands of each of any institution. IT utilization can not be separated from the hardware to support the passage of a computer system. Increasingly sophisticated information technology are sometimes not followed by the application of adequate security. Similarly, Faculty of Engineering, University of Pasundan have not implemented rules regarding security hardware, so organizations or companies faced with a number of threats that could disrupt the activity even cause the cessation of the business process.

Standard Operating Procedure (SOP) security hardware is structured as security information to prevent and minimize the number of threats that could pose a risk in the Faculty of Engineering, University of Pasundan. the literature study or reference, identify the problems that occur related to security hardware, analyze the security of the hardware in the study, commit risk assessment, perform a gap analysis, and preparation of SOP customized approach to information security standards, namely ISO27001: 2005 in clause A.9.2 about the security equipment. The purpose of the standard equipment safety clause to prevent loss, damage, theft or irregularities assets and disruption to the activities of the organization or company.

This study generates recommendations Security Hardware Standard Operating Procedures Based Approach ISO 27001: 2005. SOP is expected to balance the increased use of information technology in terms of information security at the Faculty of Engineering, University of Pasundan.

Keywords: Information Technology, Hardware , Standard Operating Procedures (SOP), ISO27001.