# INFORMATION SECURITY POLICY AND SOP AS THE ACCESS CONTROL DOCUMENT OF PT. JUI SHIN INDONESIA USING ISO/IEC 27002:2013

**Muhammad Sukmaji[1*]; Rahmat Yasirandi[2]; Muhammad Al Makky[3]**
[1, 2, 3] School of Computing
Telkom University, Bandung, Indonesia
[1]muhammadsukmaji@student.telkomuniversity.ac.id; [2]batanganhitam@telkomuniversity.ac.id;
[3]malmakky@telkomuniversity.ac.id

(*) Corresponding Author

***Abstract***— PT. Jui Shin Indonesia as the research population is a company engaged in the ceramics, granite, and cement industry. The existence of important assets owned by the company can not be denied the threat that will occur in these important assets. The importance of a company's assets, then the company must maintain the security of assets with various efforts. The security that must be maintained in this study is the security of information related to accessing control of important assets of the company. The purpose of this research is to analyze and design policy documents and SOP (Standard Operating Procedure) access control related to information security. This is done to minimize the risk that occurs in important assets of the company. The method used in this study is the OCTAVE method as a method of identification against risks that will occur in important assets of the company and the FMEA method as a method of risk analysis against the risk that has been identified through the OCTAVE method. The final result of this study is the creation of policy documents and access control SOPs related to information security which refers to the ISO/IEC 27002:2013 framework that focuses on clause 9. Access Control. Based on the results of the study, the researchers received proposals for policy document-making and SOPs as much as, namely, 17 for policy document-making and 18 for the creation of SOP documents.

**Keywords:** information security, access control, policy, SOP, ISO/IEC 27002:2013.

***Abstrak***—*PT. Jui Shin Indonesia yang menjadi objek penelitian saat ini adalah perusahaan yang bergerak di bidang industri keramik, granit, dan semen. Adanya aset penting yang dimiliki perusahaan maka tidak bisa dipungkiri akan adanya ancaman yang akan terjadi pada aset penting tersebut. Pentingnya aset sebuah perusahaan, maka perusahaan harus menjaga keamanan aset dengan berbagai macam upaya. Keamanan yang harus dijaga pada penelitian ini yaitu keamanan informasi terkait kontrol akses terhadap aset penting perusahaan. Tujuan penelitian ini yaitu menganalisis dan merancang dokumen kebijakan dan SOP (Standard Operating Procedure) kontrol akses terkait keamanan informasi. Hal tersebut dilakukan untuk meminimalisir risiko yang terjadi pada aset penting perusahaan. Metode yang digunakan dalam penelitian ini yaitu, metode OCTAVE sebagai metode identifikasi terhadap risiko yang akan terjadi pada aset penting perusahaan dan metode FMEA sebagai metode analisis risiko terhadap risiko yang sudah diidentifikasi melalui metode OCTAVE. Hasil akhir dari penelitian ini yaitu pembuatan dokumen kebijakan dan SOP kontrol akses terkait keamanan informasi yang mengacu pada kerangka kerja ISO/IEC 27002:2013 yang berfokus pada klausul 9. Access Control. Berdasarkan hasil penelitian, maka peneliti mendapatkan usulan pembuatan dokumen kebijakan dan SOP sebanyak yaitu, 17 untuk pembuatan dokumen kebijakan dan 18 untuk pembuatan dokumen SOP.*

***Kata Kunci****: keamanan informasi, kontrol akses, kebijakan, SOP, ISO/IEC 27002:2013.*

## INTRODUCTION

The current development of the business is inseparable from the important role of information technology. Information technology is one of the very important components in supporting the sustainability of the organization's business, wherein information technology there are important information assets of the organization (Saputra, 2016). Many organizations already realize that information assets have the potential to provide a competitive advantage as well as support the success of the organization (Anarkhi, Ali, & Kurnia, 2013). The importance of the value of information so that the presentation of such information is limited to certain people to access the desired information (Arsin, Yamin, &

Surimi, 2017). Information contained in the organization can be employee data, stakeholders, and other confidential organization data.

Thus, the importance of access to information assets causes every organization to strive to maintain the security of information it has and no exception to the security of information technology owned by the company under research today, namely a manufacturing company named PT. Jui Shin Indonesia.

Based on a survey from the Cyber Security Breaches Survey 2020 in the fifth series shows that cybersecurity attacks have grown and become more frequent. Almost half of businesses (46%) and a quarter of charities (26%) reported cybersecurity breaches or attacks in the last 12 months. Like in previous years. This is higher among medium-sized businesses (68%), large businesses (75%), and high-income charities (57%). This indicates that the organization's awareness of information security is not per the security that has been done by the organization in handling the importance of information security management (Department for Digital Culture Media & Sport, 2020)

PT. Jui Shin Indonesia which is the object of research today is a company engaged in the ceramics, granite, and cement industries located in the city of Medan, North Sumatra. This company has utilized information technology as a supporter of business processes run, some information technology that is utilized by the company such as servers, networks, and application systems (Sadzah, 2018). utilization of technology used by the company does not cover the possibility of problems in information security such as loss of company data caused by errors in granting access rights even systems that are capable of manipulation by irresponsible persons.

Thus, companies are obliged to prevent the risks that will occur to any important information assets of the company, such as illegal access and manipulation of data, companies need to have a control that can limit what information can see and access. The control that the company has over the right of access to information assets can minimize losses caused by misuse of access rights and destruction of the company's application system. This aims to maintain information assets so that the information owned is guaranteed confidentiality, integrity, and availability (Fahrurozi, Tarigan, Tanjung, & Mutijarsa, 2020).

Given the possible risks that will occur to companies regarding the security of information related to accessing control, the company needs support to maintain information security by designing policy documents and SOP (Standard Operating Procedure) regarding access control of important information assets of the company. This is done to minimize and avoid the risks that will occur, so as not to interfere with the sustainability of the company's business processes. SOP can be useful to define all concepts, techniques, and requirements in carrying out a process written into a document that can be directly used by employees and employees concerned in carrying out tasks in their business processes (Rachmawan, Pribadi, & Wahyu, 2017).

While the policy document is a security infrastructure that must be owned by a company that wants to protect its most important information assets (Sudirman, 2019). Related to the discussion of policy documents and SOP, there is some previous research related to the implementation in the design of policy documents and SOP, especially in Indonesia.

Several related studies have been able to prove how ISO/IEC 27002:2013 works. Companies and organizations that have created policies and SOPs have stated that they can mitigate any risks that are found. Some of these case studies include the Savings and Loans Cooperative (Andriana, Sembiring, & Hartomo, 2020), STIE Perbanas (Fatimah, 2016), CV Cempaka Tulungagung (Rachmawan et al., 2017), Communications and Information Office of East Java Province (Pratiwi, 2019). In the methodology, all related research is applying the FMEA method as a risk measurement tool and OCTAVE as a method for identifying and classifying risks. Based on the results that have been carried out in several reference studies, all of it describes how ISO/IEC 27002:2013 has become the comprehensive guideline. Especially regarding access control, ISO/IEC 27002:2013 in clause 9 has been explained in a complete way.

This study raised the fact that PT. Jui Shin Indonesia is still unable to optimize the security process for its IT assets. If the comparison of company's condition between the existing and the expected ideal conditions, it is clear that there are still several steps that need to be taken. So it is clear that there is still a clear gap as a research problem in this research.

In designing policy documents and access control SOP on information security that suit the needs of the company, the initial stage that needs to be done is by identifying the assets owned using the OCTAVE method and to help identify the risks that each asset has (Hom, Anong, Rii, Choi, & Zelina, 2020). OCTAVE method is a technique and method used to assess and plan the security of information systems based on risk identification by using a comprehensive, systematic, directed, and self-directed approach (Jufri, Hendayun, & Suharto, 2017). All defined risks are then analyzed and assessed to determine their priority level using the FMEA method.

FMEA is one of the real efforts that can be made to know the state of the level of insecurity of the information system, identify potential causes of various forms of failure, and sort the priority of failure based on the value of RPN (Risk Priority Number) (Liu, Wang, Li, & Hu, 2019). The results of the risk assessment will be the basis for the creation of policy documents and SOP. The documents that have been created will then be mapped with the control that refers to clause 9. Access Control at ISO/IEC 27002:2013. These results are per the principles of the ISO/IEC 27002:2013 framework which gives users the option to select and implement controls that suit the needs of their organization (International Organization for Standardization, 2013).

## MATERIALS AND METHODS

This research is divided into three stages, namely the data collection stage, the risk assessment stage, and the control determination stage. The stages of this research are explained sequentially.

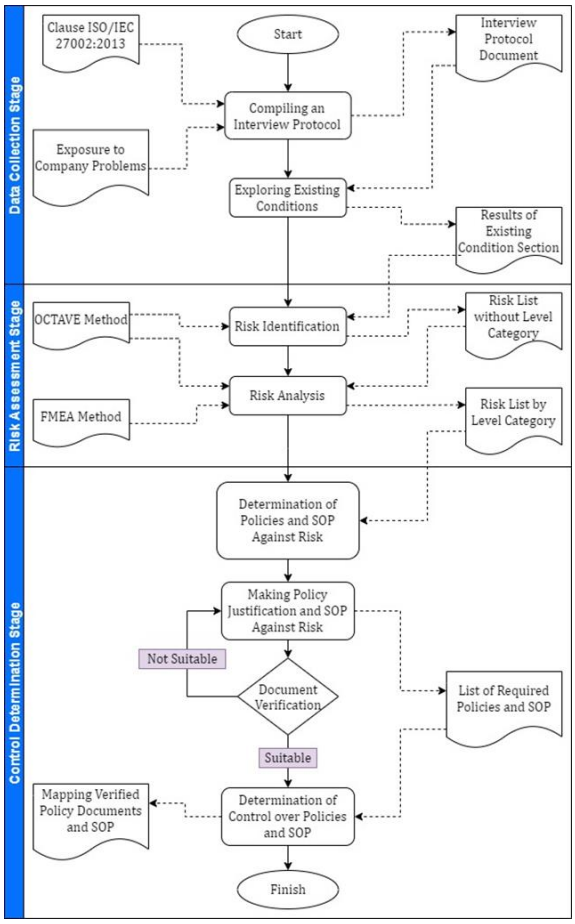


Figure 1. Research Methodology Steps

Here is a description of the research methodology step based on figure 1:

1. Data Collection Stage

This stage is the first step to fulfilling the preparation of this research. There are several processes underway at this stage. Here's an explanation of each process at the data collection stage.

a. Compiling an Interview Protocol

In compiling the interview protocol two inputs affect and become a consideration in conducting the preparation of interview protocol namely, clause ISO / IEC 27002:2013 and the results of exposure of the problems owned by the company. The first input is used to know the standards that must be available in securing information assets and controls that must be done to carry out those standards. The second input is exposure related to constraints owned by the company. The resulting output is an interview protocol document used to interview the source.

b. Exploring Existing Conditions

In this process, the input required is an interview protocol document created in the previous process. The excavation of information carried out in this process is the excavation of information security risks. The results of extracting existing conditions are used to identify risks. The output resulting from the process of extracting existing conditions is the result of interviews extracting existing conditions from the source.

2. Risk Assessment Stage

This stage is based on the information security risk assessment approach at ISO/IEC 27002:2013 which is divided into two main processes, namely risk identification and risk analysis. Here's an explanation of each process in the risk assessment phase.

a. Risk Identification

In this process, there are two inputs namely OCTAVE and also interview results from extracting existing conditions. Identifying risks will be related to the loss of confidentiality, integrity, and availability of information within the scope of information security on the aspect of access control. To get information, the interview was conducted with the company's IT division. Risk identification will be based on the OCTAVE method by identifying critical assets, critical asset security needs, and critical asset risk. The output obtained is a list of risks without level categories. The list of risks obtained will be a consideration as well as input for the risk analysis process.

b. Risk Analysis

In this process, there are three inputs namely FMEA, OCTAVE, and risk list without level

category. This process will be carried out process among others, the first is to assess the risk that will occur, the second is to assess the cause of the occurrence of the risk that has been identified and the last is to determine the level of risk that has been identified. Risk analysis is performed using the FMEA method. The analysis that will be carried out using the FMEA method includes asset threat categories, threats, causes, risks, effects of risk occurrence (severity), probability of occurrence of risk (occurrence), level of risk control (detection), and RPN (Risk Priority Number). The output of this process is a list of risks with category levels.

3. Control Determination Stage

This stage is a stage in mapping control over policy proposal documents and SOP. In this stage there are three main processes, namely policy determination and SOP against risk, making policy justification and SOP to risk, and determining control over policy and SOP. Here's an explanation of each process in the control determination stage.

a. Determination of Policies and SOP Against Risk

In this process, the determination of the document against the risk will be based on the list of risks that have been obtained from the results of the previous risk analysis. The input at this stage is a list of risks with level categories. Determination in making documents refers to clause 9. Access Control in the framework of ISO/IEC 27002:2013.

b. Making Policy Justification and SOP Against Risk

This process is a process in determining the mitigation actions that will be created into the policy documents and access control SOP related to information security. The output of this process is a list of policies and SOP needed.

c. Document Verification

In this process, the input needed is the required policy document and SOP. This verification process will be done by the company. After the verification process is completed and is appropriate by the company, the next process is to determine the control over the documents.

d. Determination of Control over Policies and SOP

This process will be based on a list of policy documents and SOP obtained from the previous justification. The determination of the control will refer to clause 9. Access Control in the ISO/IEC 27002:2013 framework.

## RESULTS AND DISCUSSION

This research focuses on important information assets contained in PT. Jui Shin Indonesia. It aims to identify and analyze information security-related risks related to access control over assets referred to in clause 9. Access Control is contained within the framework of ISO/IEC 27002:2013.

A. Identification of Critical Assets and Risks

Determination of critical assets and risk of critical assets is done through the collection of information based on the point of view of the company's IT division. Justification of determination of critical assets and risk of critical assets is done by direct observation and discussion with related parties. From direct observations made by researchers, there are several critical assets based on the category of asset threats and risk of critical assets contained in the company. Here is a list of critical assets based on the category of asset threats and risk of critical assets contained in the company.

Table 1. List of Critical Assets and Their Risks

| Critical Assets | Asset Threat Category | Risk ID | Risk |
|---|---|---|---|
| Presence Information System | Network and Data | R1 | Illegal Access Data Manipulation (Employee Presence Data) |
| Sales Application System | Network and Data | R2 | Illegal Access Data Manipulation (Sales Data) |
| Company Website | Software, Network dan Data | R3 | Illegal Access Data Manipulation (Company Information Data) |
| Employee Computer Directory | Data | R4 | Illegal Access Data Manipulation (Computer Directory Data) |
| IP Based Telephone System | Network and Data | R5 | Illegal Access Data Manipulation (Phone Tapping Recording Data) |
| CCTV Camera-Based Monitoring System | Network and Data | R6 | Illegal Access Data Manipulation (CCTV Footage Data) |
| Server Control Room Authentication System | Network and Data | R7 | Illegal Access Data Manipulation (Authentication Factor Data) |

B. Identify Critical Asset Security Needs

Security needs are a form of protection against possible threats to ensure the continuity of

business processes, minimizing business risks. The needs of each asset have more than one need. The justification of determining the security needs of critical assets is done by direct observation and discussion with the relevant parties. From observations made by the researcher, there are several critical asset security needs contained in each critical asset of the company including confidentiality, integrity, and availability of information in the scope of information security in the aspect of access control.

C. Risk Assessment with FMEA Method

After identifying the risks contained in the company using OCTAVE, further assessment of each risk is carried out. This assessment is used to classify the risks that exist in the risk level, namely very low, low, medium, high, very high. The FMEA method is used in assessing the risks contained in the company. There are three criteria used, namely severity, occurrence, and detection. In assessing the risks, it is determined how much value is for each of these criteria. Then all criteria are calculated to determine the amount of RPN (Risk Priority Number) value of each risk by using the following formula:

$$RPN = \text{Severity} \times \text{Occurrence} \times \text{Detection} \quad (1)$$

The resulting RPN calculation result for each risk is contained in table 2, then categorized based on the scale of RPN value shown in table 3.

Table 2. RPN Value Determination Scale

| Risk Level | RPN Value Scale |
|---|---|
| Very High | >= 200 |
| High | >= 120 - < 200 |
| Medium | >= 80 - < 120 |
| Low | >= 20 - < 80 |
| Very Low | 0 - < 20 |

Source: (Fatimah, 2016)

The following are the results of the assessment of each risk using the FMEA method shown in table 4.

Table 3. Risk Assessment with FMEA Method

| Risk ID | FMEA Mapping | | | RPN | Level |
|---|---|---|---|---|---|
| | Severity | Occurrence | Detection | | |
| | Rank | Rank | Rank | | |
| **R1** | 6 | 2 | 4 | 48 | Low |
| **R2** | 9 | 2 | 6 | 108 | Medium |
| **R3** | 9 | 2 | 6 | 108 | Medium |
| **R4** | 9 | 2 | 9 | 162 | High |
| **R5** | 4 | 1 | 6 | 24 | Low |
| **R6** | 4 | 2 | 4 | 32 | Low |
| **R7** | 10 | 2 | 4 | 80 | Medium |

This FMEA calculation is obtained from the results of interviews conducted directly to the company related to the identified risks.

D. Policy Mapping Results Against Risk

Policy mapping of risks is performed on each critical asset identified in the beginning. This mapping is done to know what policies can be proposed to minimize any risks that will occur to critical assets of the company.

Table 4. Results of Mapping Policy Documents Against Risk

| Number | Policy |
|---|---|
| 1 | POLICY/CENTER/1/2021<br>Policy on restricting access rights to corporate data |
| 2 | POLICY/CENTER/2/2021<br>Company information technology asset procurement policy |
| 3 | POLICY/CENTER/3/2021<br>Policies related to employee sanctions against tangible and intangible IT assets |
| 4 | POLICY/PRESENSI/1/2021<br>Access control policies on presence information systems |
| 5 | POLICY/PRESENSI/2/2021<br>Policies related to development, maintenance, and changes to the information system |
| 6 | POLICY/SALES/1/2021<br>Access control policy on sales application system |
| 7 | POLICY/SALES/2/2021<br>Policies related to development, maintenance, and changes to the sales application system |
| 8 | POLICY/WEBSITE/1/2021<br>Access control policy on the company website |
| 9 | POLICY/WEBSITE/2/2021<br>Policies related to development, maintenance, and changes on the company's website |
| 10 | POLICY/COMPUTER DIRECTORY/1/2021<br>Access control policy on employee computer directory |
| 11 | POLICY /COMPUTER DIRECTORY/2/2021<br>Policies related to the development, maintenance, and changes to employee computer directories |
| 12 | POLICY/PHONE/1/2021<br>Access control policies on IP-based telephone systems |
| 13 | POLICY/PHONE/2/2021<br>Policies related to development, maintenance, and changes to IP-based telephone systems |
| 14 | POLICY/CCTV/1/2021<br>Access control policy on CCTV camera-based monitoring system |
| 15 | POLICY/CCTV/2/2021<br>Policies related to development, maintenance, and changes to CCTV camera-based monitoring systems |
| 16 | POLICY/SERVER CONTROL/1/2021<br>Access control policy on a server control room authentication system |

| Number | Policy |
|---|---|
| 17 | POLICY/SERVER CONTROL/2/2021<br>Policies related to development, maintenance, and changes to the server control room authentication system |

E. SOP Mapping Results Against Risk

SOP mapping of risks is performed on each critical asset that has been identified in the beginning. This mapping is done to know what SOP can be proposed to minimize any risks that will occur to the company's critical assets.

Table 5. SOP Document Mapping Results Against Risk

| Number | SOP *(Standard Operating Procedure)* |
|---|---|
| 1 | SOP/PRESENSI/1/2021<br>Procedures for making permissions for employees in the information system |
| 2 | SOP/PRESENSI/2/2021<br>Procedures for obtaining data and information on presence information systems |
| 3 | SOP/PRESENSI/3/2021<br>Procedures for the change (transfer or removal) of employee access rights in the presence information system |
| 4 | SOP/SALES/1/2021<br>Procedures for creating permissions for employees on the sales application system |
| 5 | SOP/SALES/2/2021<br>Procedures for obtaining data and information on the sales application system |
| 6 | SOP/SALES/3/2021<br>Procedures for changing (transferring or removing) employee permissions on the sales application system |
| 7 | SOP/WEBSITE/1/2021<br>Procedures for obtaining data and information management permissions on the company's website |
| 8 | SOP/WEBSITE/2/2021<br>Procedure in obtaining program code management permissions on the company's website |
| 9 | SOP/COMPUTER DIRECTORY/1/2021<br>Procedures for creating permissions for employees on employee computer directory data |
| 10 | SOP/COMPUTER DIRECTORY/2/2021<br>Procedures for obtaining data and information on a particular employee's computer directory |
| 11 | SOP/COMPUTER DIRECTORY/3/2021<br>Procedure in change (transfer or removal) of employee permissions on employee computer directory |
| 12 | SOP/PHONE/1/2021<br>Procedures for creating permissions for employees on IP-based telephone systems |
| 13 | SOP/PHONE/2/2021<br>Procedures for obtaining data and recording information on IP telephone systems |
| 14 | SOP/PHONE/3/2021<br>Procedures for changing (transferring or removing) employee permissions on IP-based telephone systems |
| 15 | SOP/CCTV/1/2021<br>Procedures for obtaining data access rights and recording information on cctv camera-based monitoring systems |
| 16 | SOP/SERVER CONTROL/1/2021<br>Procedure in creating/registering permissions for employees on the server control room authentication system |
| 17 | SOP/SERVER CONTROL/2/2021<br>Procedure for obtaining data and information permissions on a server control room authentication system |
| 18 | SOP/SERVER CONTROL/3/2021<br>Procedure in changing (transferring or erasure) employee permissions on the server control room authentication system |

F. Document Verification

After the policy document and SOP are determined, the next process is to verify the document to the IT part of the company concerned. This is done to obtain an assessment from the company regarding the documents per or not the documents that will be applied in the company.

G. Results of Mapping Control over Policies and SOP

After determining the policy document and SOP then mapping the resulting document based on the security of access control information in clause 9. Access Control on framework ISO/IEC 27002:2013. This mapping is done to know what control determinations can be used to create policy documents and proposed SOP.

Table 6. Results of Policy Mapping and SOP Produced Against ISO/IEC 27002:2013

| Access Control ISO/IEC 27002:2013 | Policy and SOP (Standard Operating Procedure) |
|---|---|
| 9.1.1 Access control policy | POLICY/CENTER/1/2021 |
| | POLICY/CENTER/2/2021 |
| | POLICY/CENTER/3/2021 |
| | POLICY/PRESENSI/2/2021 |
| | POLICY/SALES/2/2021 |
| | POLICY/WEBSITE/2/2021 |
| | POLICY/COMPUTER DIRECTORY/2/2021 |
| | POLICY/PHONE/2/2021 |
| | POLICY/CCTV/2/2021 |
| | POLICY/SERVER CONTROL/2/2021 |
| 9.1.2 Access to networks and network services | POLICY/CENTER/1/2021 |
| | POLICY/CENTER/3/2021 |
| 9.2.1 User registration and de-registration | SOP/PRESENSI/1/2021 |
| | SOP/PRESENSI/3/2021 |
| | SOP/SALES/1/2021 |
| | SOP/SALES/3/2021 |
| | SOP/COMPUTER DIRECTORY/1/2021 |
| | SOP/COMPUTER DIRECTORY/3/2021 |
| | SOP/PHONE/1/2021 |
| | SOP/PHONE/3/2021 |
| | SOP/SERVER CONTROL/1/2021 |
| | SOP/SERVER CONTROL/3/2021 |
| 9.2.2 User access provisioning | POLICY/CENTER/3/2021 |
| | SOP/PRESENSI/2/2021 |
| | SOP/PRESENSI/3/2021 |

| Access Control ISO/IEC 27002:2013 | Policy and SOP (Standard Operating Procedure) |
|---|---|
| | SOP/SALES/2/2021 |
| | SOP/SALES/3/2021 |
| | SOP/WEBSITE/1/2021 |
| | SOP/WEBSITE/2/2021 |
| | SOP/COMPUTER DIRECTORY/2/2021 |
| | SOP/COMPUTER DIRECTORY/3/2021 |
| | SOP/PHONE/2/2021 |
| | SOP/PHONE/3/2021 |
| | SOP/CCTV/1/2021 |
| | SOP/SERVER CONTROL/2/2021 |
| | SOP/SERVER CONTROL/3/2021 |
| 9.2.3 Management of privileged access rights | POLICY/CENTER/1/2021 |
| | POLICY/CENTER/3/2021 |
| | SOP/PRESENSI/2/2021 |
| | SOP/SALES/2/2021 |
| | SOP/WEBSITE/1/2021 |
| | SOP/WEBSITE/2/2021 |
| | SOP/COMPUTER DIRECTORY/2/2021 |
| | SOP/PHONE/2/2021 |
| | SOP/CCTV/1/2021 |
| | SOP/SERVER CONTROL/2/2021 |
| 9.2.4 Management of secret authentication information of users | POLICY/CENTER/3/2021 |
| | POLICY/PRESENSI/1/2021 |
| | POLICY/SALES/1/2021 |
| | POLICY/WEBSITE/1/2021 |
| | POLICY/COMPUTER DIRECTORY/1/2021 |
| | POLICY/PHONE/1/2021 |
| | POLICY/CCTV/1/2021 |
| | POLICY/SERVER CONTROL/1/2021 |
| 9.2.5 Review of user access rights | POLICY/CENTER/3/2021 |
| | POLICY/PRESENSI/1/2021 |
| | POLICY/SALES/1/2021 |
| | POLICY/WEBSITE/1/2021 |
| | POLICY/COMPUTER DIRECTORY/1/2021 |
| | POLICY/PHONE/1/2021 |
| | POLICY/CCTV/1/2021 |
| | POLICY/SERVER CONTROL/1/2021 |
| 9.2.6 Removal or adjustment of access rights | POLICY/CENTER/3/2021 |
| | SOP/PRESENSI/3/2021 |
| | SOP/SALES/3/2021 |
| | SOP/COMPUTER DIRECTORY/3/2021 |
| | SOP/PHONE/3/2021 |
| | SOP/SERVER CONTROL/3/2021 |
| 9.3.1 Use of secret authentication information | POLICY/CENTER/1/2021 |
| | POLICY/CENTER/3/2021 |
| | SOP/PRESENSI/1/2021 |
| | SOP/SALES/1/2021 |
| | SOP/COMPUTER DIRECTORY/1/2021 |
| | SOP/PHONE/1/2021 |
| | SOP/SERVER CONTROL/1/2021 |
| 9.4.1 Information access restriction | POLICY/CENTER/1/2021 |
| | POLICY/CENTER/3/2021 |
| 9.4.2 Secure log-on procedures | POLICY/CENTER/3/2021 |
| | POLICY/PRESENSI/1/2021 |
| | POLICY/SALES/1/2021 |
| | POLICY/WEBSITE/1/2021 |
| | POLICY/COMPUTER DIRECTORY/1/2021 |
| | POLICY/PHONE/1/2021 |
| | POLICY/CCTV/1/2021 |
| | POLICY/SERVER CONTROL/1/2021 |
| 9.4.3 Password management system | POLICY/PRESENSI/1/2021 |
| | POLICY/SALES/1/2021 |
| | POLICY/WEBSITE/1/2021 |
| | POLICY/COMPUTER DIRECTORY/1/2021 |
| | POLICY/PHONE/1/2021 |
| | POLICY/CCTV/1/2021 |
| | POLICY/SERVER CONTROL/1/2021 |
| | SOP/PRESENSI/1/2021 |
| | SOP/SALES/1/2021 |
| | SOP/COMPUTER DIRECTORY/1/2021 |
| | SOP/PHONE/1/2021 |
| | SOP/SERVER CONTROL/1/2021 |
| 9.4.4 Use of privileged utility programs | POLICY/CENTER/1/2021 |
| | POLICY/CENTER/3/2021 |
| 9.4.5 Access control to program source code | POLICY/CENTER/1/2021 |
| | POLICY/CENTER/3/2021 |
| | SOP/PRESENSI/2/2021 |
| | SOP/SALES/2/2021 |
| | SOP/WEBSITE/2/2021 |
| | SOP/COMPUTER DIRECTORY/2/2021 |
| | SOP/SERVER CONTROL/2/2021 |

## CONCLUSION

The conclusion obtained in this study is that this study produces policy documents and access control SOPs related to information security, which later this document can be applied by PT. Jui Shin Indonesia. The entire document refers to clause 9. Access Control in the ISO/IEC 27002:2013 framework. Based on the results of the study, there are 17 for policy document creation and 18 for making SOP documents. The creation of this document is expected to minimize and even reduce the risk that will occur in critical assets that can interfere with the running of the company's business processes.

## REFERENCE

Anarkhi, P. G., Ali, A. H. N., & Kurnia, I. (2013). Penyusunan Perangkat Audit Keamanan Informasi Aplikasi Berbasis Web Menggunakan ISO/IEC Klausul Kendali Akses. *Jurnal Teknik POMITS*, *1*(1), 1–5.

Andriana, M., Sembiring, I., & Hartomo, K. D. (2020). SOP of Information System Security on Koperasi Simpan Pinjam Using ISO/IEC 27002:2013. *Jurnal Transformatika*, *18*(1), 25–35. https://doi.org/10.26623/TRANSFORMATIKA.V18I1.2020

Arsin, F., Yamin, M., & Surimi, L. (2017). Implementasi Security System

Menggunakan Metode Idps (Intrusion Detection And Prevention System) Dengan Layanan Realtime Notification. *SemanTIK*, *3*(2), 39–48. Retrieved from http://ojs.uho.ac.id/index.php/semantik/article/view/3199

Department for Digital Culture Media & Sport. (2020). Cyber Security Breaches Survey 2020. Retrieved June 30, 2021, from GOV.UK website: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

Fahrurozi, M., Tarigan, S. A., Tanjung, M. A., & Mutijarsa, K. (2020). The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence). *ICITEE 2020 - Proceedings of the 12th International Conference on Information Technology and Electrical Engineering*, 86–91. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICITEE49829.2020.9271748

Fatimah, A. N. (2016). *Pembuatan Dokumen Sop (Standard Operating Procedure) Keamanan Data Yang Mengacu Pada Kontrol Kerangka Kerja Cobit 5 Dan Iso27002:2013 (Studi Kasus : Stie Perbanas)*. Institut Teknologi Sepuluh November, Surabaya.

Hom, J., Anong, B., Rii, K. B., Choi, L. K., & Zelina, K. (2020). The Octave Allegro Method in Risk Management Assessment of Educational Institutions. *Aptisi Transactions on Technopreneurship (ATT)*, *2*(2), 167–179. https://doi.org/10.34306/ATT.V2I2.103

International Organization for Standardization. (2013). ISO/IEC 27002:2013(en), Information technology — Security techniques — Code of practice for information security controls. Retrieved August 26, 2021, from Online Browsing Platform (OBP) website: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

Jufri, M. T., Hendayun, M., & Suharto, T. (2017). Risk-assessment-based academic information System security policy using octave Allegro and ISO 27002. *Proceedings of the 2nd International Conference on Informatics and Computing, ICIC 2017*, 1–6. Jayapura: Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/IAC.2017.8280541

Liu, H. C., Wang, L. E., Li, Z., & Hu, Y. P. (2019). Improving risk evaluation in FMEA with cloud model and hierarchical TOPSIS method. *IEEE Transactions on Fuzzy Systems*, *27*(1), 84–95. https://doi.org/10.1109/TFUZZ.2018.2861719

Pratiwi, W. A. (2019). *Perencanaan Sistem Manajemen Keamanan Informasi Berdasarkan Standar ISO 27001:2013 pada Kominfo Provinsi Jawa Timur* (Universitas Dinamika.). Universitas Dinamika., Surabaya. Retrieved from https://repository.dinamika.ac.id/id/eprint/3310/

Rachmawan, D. I., Pribadi, A., & Wahyu, T. D. E. (2017). Pembuatan Dokumen Sop Keamanan Aset Informasi yang Mengacu pada Kontrol Kerangka Kerja Iso 27002:2013 (Studi Kasus : CV Cempaka Tulungagung) - Neliti. *Jurnal Teknik ITS*, *6*(1), A-198-A-201.

Sadzah, A. H. (2018). *Analisis dan Desain Tempat Kerja Menggunakan Macroergonomics Analysis And Design Pada PT. Jui Shin Indonesia* (Universitas Sumatera Utara). Universitas Sumatera Utara, Medan. Retrieved from http://repositori.usu.ac.id/handle/123456789/9137

Saputra, A. Y. (2016). *Pembuatan Standar Operating ProcedureKeamanan Aset Informasi Berdasarkan KendaliAkses Dengan Menggunakan Iso/Iec:27002:2013Pada Studi Kasus STIE Perbanas Surabaya* (Institut Teknologi Sepuluh Nopember). Institut Teknologi Sepuluh Nopember, Surabaya. Retrieved from https://repository.its.ac.id/72788/

Sudirman, A. (2019). *Kerangka Kerja Digital Forensic Readiness pada Sebuah Organisasi (Studi Kasus : PT Waditra Reka Cipta Bandung)* (Universitas Islam Indonesia). Universitas Islam Indonesia, Yogyakarta. Retrieved from https://dspace.uii.ac.id/handle/123456789/17263