IJEC
International Journal of Economics
https://ejournal.ipinternasional.com/index.php/ijec
e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

Perceptions of Students at Andalas University's Payakumbuh Campus Regarding the Security of Academic Information Systems

Yindrizal
Study Program of Management, Faculty of Economics and Business, Andalas University, Indonesia
Corresponding author's email; yindrizal@eb.unand.ac.id
Article history: received July 13, 2024; revised July 20, 2024; accepted July 23, 2024

Abstract

Higher Education is one of the public service providers that wants to provide the best service to internal and external parties who need information, namely by utilizing academic information systems. The use of academic information systems is prone to data and information crimes, which are problems experienced by many system users and this also occurs in Indonesia. The method in this study uses a qualitative description method in this study and data collection is obtained using triangulation techniques. The results of the study, that it is necessary to improve information security from various threats, thus ensuring the security of valuable information assets. Information security using The International Organization for Standardization (ISO)/IEC 27001. In addition, it is also necessary to perform two-factor authentication which adds a two-step verification process to access the account.

Keywords: Academic Information System, ISO, System Security, Authentication

INTRODUCTION

Higher education is one of the public service providers that wants to provide the best service to parties who need information such as students, employees or other parties. For this reason, the university formed a special unit to handle information management and communication services at the university. According to Darmawan and Fauzi (2013), with the development of information technology, information has become an important asset because apart from confidentiality, information experiences inaccessibility, data modification, data theft, human error, hardware and software damage and other risks such as risk of damage.

Data and information crime is an ongoing problem in Indonesia. Apart from that, Gemalto also reported that the data generated reached 6.9 million data per day. This is based on a total of $14.6 billion in data theft reports from 2013 to 2018, of which only 4% was encrypted by the owner. According to statistics, the most data loss due to crime comes from social media companies with 56.11%, followed by data from government agencies with 26.62%. Security systems are always prioritized for access to personal data in cyberspace. Computerized Forensic Indonesia (DFI) estimates there are around 7.5 billion. In the last 15 years, personal information of internet users around the world has been stolen by third parties. Sources of information crime in all these industries come from outside hackers (*vindictive pariah*) and insiders (*malignant insider), illegal* information from insecure systems (*unplanned misfortune*), hackers (*hacktivist*), lost small devices or cellphones, extortion devices (*ransomware*) and from many unknown sources. User data theft can occur if data protection on a website is weak. Therefore, personal information may change. In fact, Article 15 Paragraph 1 of the ITE Law stipulates data protection requirements that require electronic users to manage platform security.

According to the Symantec report (2015), 46% of crimes are mostly caused by attackers/ *hackers* . However, more than 22 percent of crimes were classified as "inadvertently made public,"

e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

21 percent were caused by stolen or lost computers or equipment, and 10 percent were caused by internal collaboration. Data encryption can prevent various data breaches and eliminate the consequences of data falling into the wrong hands.

Al-Sehri (2012) believes that one of the reasons data security and privacy violations occur is because users do not have sufficient knowledge about the safe use of information systems, and some do not do it well, despite having sufficient knowledge about the use of information systems. According to Whitman and Mattord (2011), information security is an effort to protect information and its contents, whether in the form of systems or equipment used to store and send information. McLeod and Schell (2008) say that information security aims to achieve information confidentiality.

Academic information systems must also be able to meet operational demands and reduce the risk of data corruption, data loss, service interruptions, and poor information system management systems. Therefore, there is also a need for an information audit, where an information system audit is the process of collecting and analyzing higher education information to determine whether it has protection for the integrity of data and information to achieve its goals effectively and efficiently. Alvin A. Arens and James K. Loebbecke (2005) say that information systems audit is the process of collecting and analyzing various available evidence to determine the relationship between all data and predetermined patterns.

Theoretical framework

Information security procedures include compliance with internationally accepted Information Security Guidelines. The Global Security Statement discusses how it can provide security information to *eCommerce partners* . The information security compliance process helps organizations benchmark their information security practices against international security management standards. The aim is to identify and verify organizational practices against the Standard. Measuring the level of compliance helps an organization determine that it is complying with the regulations set out in the standard. Compliance with internationally accepted standards is critical to measuring information security. For this reason, it is important for organizations to regularly evaluate their information security level in accordance with international standards (Al-Omari A, El-Gayar O, Deokar A. 2012)

According to Darmawan (2013), information is the result of data processing which can provide meaning and is useful for an individual. According to Laudon (2007), an information system is defined as a system that collects, processes, stores and distributes information to support decision making and management in an organization. An information audit is the process of collecting and analyzing evidence to determine whether the systems used protect assets, maintain the integrity of information, help the organization achieve its goals, and the resources used are used effectively and efficiently.

According to Whitman and Mattord (2011), security awareness is a control/policy designed to reduce information security violations caused by carelessness or planning. According to Kruger and Kerney (2006), social psychology theory is used to measure something into three parts: knowledge, emotions, and behavior. Information security is about how we prevent fraud or at least detect fraud in knowledge-based systems where information itself does not exist. The level or scale of information security is divided into three aspects to measure things such as knowledge, thinking and behavior. These elements are used to create three dimensions called a person's knowledge (*knowledge*), a person's attitude (*Attitude*), and a person's behavior (*Behaviour*).

In controlling and collaborating with information system security, we must consider three important aspects of information security, known by the acronym CIA (*Confidentiality, Integrity, Availability*)

e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

a. Confidentiality (*Confidentiality*). This is part of ensuring that information is only accessible to authorized personnel.
b. Justice (*Integrity*). This is part of ensuring that information is not changed without authorized persons' consent and that accurate and complete information is kept.
c. Availability *is* part of ensuring that information is available when and where it is needed.

Considering how important information is and the high risk of interference, universities need an information security management system. Information is one of the most important assets for organizations today. Therefore, it is natural that the system that supports this information is exposed to threats, whether intentionally or not. These threats pose risks to the privacy, integrity and availability of data and the systems that manage it. Organizational leaders should consider and implement steps to help prevent, detect, and respond to these threats. To complete information system protection activities, organizations need to take various steps. They need to improve integration and social metrics because this is the only way to ensure organizational health and control organizational justice (Dhillon and Backhouse 2000).

The document states that in order for organizations to achieve a specific level of security for information systems, it is most necessary and important to initiate and maintain the *International Space Station* (I SS) program. Given today's technology and business environment, organizations should stop worrying about hacking or *firewalls* and anti-virus applications and start focusing on building an *Internet Service Provider* (ISP) concept, where we cannot ensure that Internet use is safe just by installing *a firewall* . There are several other issues to consider, such as rules, procedures, standards and guidelines that will guide user behavior.

In the international journal " *Information Security Management System Standards: A Comparative Study of the Five Big Susanto et al* . (2011)", it is explained that ISO/IEC 27001 is the system most widely used by organizations, because the assessments carried out refer to ISO/IEC and maturity assessment criteria refers to *Capability Maturity Model* (CMM) for *System Security Engineering* (SSE) . *The Capability Maturity Model* (CMM) is a framework used to develop technical processes, both formal and informal.

Information security according to ISO/IEC 27002 (2005), is the protection of information from various threats, so as to ensure reduced business risks and business continuity, as well as providing profits on investment and business. In ISO/IEC 27001 (2013), information security manages the confidentiality, integrity and availability of information by implementing risk management procedures and providing assurance to parties who are satisfied that risks have been managed appropriately. Information security management is part of and integrated with the overall management and control process.

Apart from ISO/IEC 27001, to maintain information system security, it is also necessary to audit the information system. In general, audit (Gondodiyoto, 2007) is defined as "an independent investigation of a particular activity". Mulyadi (1998) said that analysis is a management process for obtaining and evaluating evidence of business statements and objective situations, reconciling requirements and decision models, and communicating the results to authorized users.

Sanyoto (2007) said that for information system security it is necessary to carry out an information system audit, where an information system audit is an examination carried out within the framework of information technology management. An information systems audit is the process of collecting and analyzing evidence to determine whether the system manages information fairly, contributes to achieving organizational goals, and uses resources effectively. The function of an information system audit is to examine the design and results of information system controls. Therefore, in an organization or company, data analysis is very important to ensure the security and privacy of information or assets within the organization.

e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

METHOD

The method in this research uses a qualitative description method in this research and data collection is obtained using triangulation techniques. Researchers chose a descriptive design because they wanted to describe events observed in the field specifically, transparently and in depth. Qualitative research tries to explain phenomena in depth by collecting as deep data as possible, emphasizing the importance of depth and detail in research data. Qualitative research has far fewer respondents or subjects than quantitative research, because it prioritizes depth of data rather than quantity of data.

Moleong (2013) said that qualitative research is about fully understanding the behavior, thoughts, motivations and actions experienced by the research object from texts and explanations. Qualitative research has far fewer respondents or subjects than quantitative research because it prioritizes depth of data rather than quantity of data. Sugiyono (2015), triangulation is defined as a data collection process using interview, observation and recording techniques simultaneously on the same data. This is based on regular analysis of academic information systems, which is explained in the form of analysis when conducting interviews and observations.

RESULTS AND DISCUSSION

Results

Security is a part of information systems, where security is determined by the answer to this question "Does the message reach all users or only the targeted users? (*did the message reach all or only the intended systems users?*)" Data and information must be protected from access which is unauthorized, meaning that due to the nature and purpose of the information only those who have an account can access the information.

More security than discomfort, or more security less discomfort, are expressions that occur when there is security, sometimes creating a feeling of greater and less compared to the past. Information security can be understood as an effort to prevent, combat and reduce information-related crimes. The digital era is innovation or new technology that is often associated with the emergence of the internet and computers. We now live in a fast-paced and intelligent digital world where connectivity is inevitable. We cannot live without devices like tablets or smartphones in our daily lives.

In the digital world, information has become very valuable and the exchange of information and data has become very fast and easy. Technological developments bring convenience, but of course also bring threats to information security. Some unscrupulous and irresponsible parties obtain the information necessary to commit crimes. This makes individuals, organizations and countries vulnerable to data attacks such as hacking, cybercrime and eavesdropping. If information is misused and stolen, there will be loss, confusion, and If information is classified, the risks are very high.

The Indonesian government has established policies regarding information security in the Electronic Information and Processing Regulations. This law has been amended by Law no. 1. None. Federal Law No. 19 of 2016 Presidential Decree no. 71 of 2019 concerning Technology and Energy. Federal Energy Law No. 95 of 2018 and other regulations based on this law. States play an important role in ensuring information security by establishing communications and information infrastructure and regulations to protect information security from threats to the deaf. Implementation of government policies in the field of Communication and Informatics is carried out by the Department of Communication and Informatics. All written policies should focus on and promote security, including privacy to protect company data and information from unauthorized disclosure.

Data security is the responsibility of all of us, not just the government or an organization's IT department. That's why it's so important for everyone to know about data security. The data security

e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

aspect is too important to ignore. Implementing data security starts from ourselves with the tools we use regularly, such as computers and gadgets.

Keep your computer secure by using a password to log in, installing antivirus software, always using licensed software, using foreign media (*external hard drives*, *flash drives*), and don't forget to update files regularly. Important security features: always use a password consisting of at least 8 characters; uppercase letters, lowercase letters, special characters, and numbers.

Even if managers and users use adequate security measures, hackers and careless workers can cause security breaches, as well as physical damage to devices in the event of a disaster. Servers that store data and information depend heavily on energy. This measure shows how easy the information is to understand.

The following are several opinions from informants who expressed their experiences in using AIS. What is the informant's statement about SIA's actual level of security? The following are the opinions expressed by the informant:

Informant-2 expressed his opinion about the level of system security, where the informant:
"The confidentiality of the Academic Information System is not guaranteed, because our access rights can be used by other people by hacking the account. "In the future, we hope that this will become a concern for Academic Information System managers, so that they can improve the quality of system security, so that the confidentiality of informant data can be maintained." (interview, May 5, 2023);

Informant-2 was of the opinion that the system security level had not yet met their expectations, because accounts could still be hacked by hackers, so they felt uncomfortable with the existence of their data in the AIS. The same thing was also expressed by informant-4, where the informant stated his opinion as follows:
"Data security in the Academic Information System is not completely safe, because access rights can be exercised by students and SIA admins, so there is a possibility that the system can be hacked by hackers. For this reason, system security needs to be further improved." (interview, May 9, 2023);

The opinion of the informant above is also strengthened by the opinion of informant-5, where this informant said that:
"The security of the Academic Information System is not guaranteed, because the system does not have adequate protection, so there are parties who have no interest in trying to enter to access user data." (interview, May 6, 2023);

Informant-13 also expressed the same opinion, where the opinion expressed by the informant was:
"The security of the system is not guaranteed, because the login process only uses *Username* and *Password* . The system is not protected by a firewall system, so it is easy to hack." (interview, May 5, 2023);

The opinion of the informant above is confirmed by the opinion of informant-17 who said that:
"Confidentiality of user data in SIA is not guaranteed, because the system is quite easy for *hackers to hack*, even if you use *a user name* and *password to access it*." (interview, May 3, 2023);

The opinion of the informants above is that they are dissatisfied with the current level of SIA security. Apart from the opinions expressed by other informants, they felt quite satisfied with the current level of SIA security. An opinion that was satisfied with SIA's current level of security was expressed by the following informant, who said:

Informant-15 believes that they are quite satisfied with the level of security of SIA, but they also still have doubts about the level of system protection which is still not good. This is caused by the way to enter SIA using only *a user name* and *password* . The following is the opinion expressed by informas-15, saying that:

e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

"The security of the system is quite guaranteed, because access rights can only be exercised by users who have the rights. "Meanwhile, system protection is still not good, because access only uses *a username* and *password*, so it will be easy for hackers to enter the system." (interview, May 9, 20232);

The informant above believes that the security level of SIA is quite good, but the level of system protection is considered not good. Another opinion expressed by informant-22 said that:
"The confidentiality of SIA data is quite guaranteed, because access is only owned by those who have the right to access, namely by using the student's *user name* and BP number. Security like this must be improved, because it will be easily hacked by hackers" (interview, 9 May 2023);

The opinion expressed by the informant above is that access can only be carried out by the account owner, but access using *a username* and *password* alone cannot guarantee complete system security. The following is the opinion expressed by the informant, who said that:
"The system is considered quite safe, because no one has experienced a data leak, but the system is still vulnerable to hackers. The system security level only relies on the username and password." (interview, May 3, 2023);

The statements made by the informant above can be described as indicating that the current level of security at SIA is still considered weak. This is caused by accessing SIA only using *a user name* and one *password* . Users want to be able to increase the level of system security, namely for system access other security measures can be added, such as the use of *a string* after using *a password*. Thus the level of data and information security is sufficiently secure, so that it can meet user expectations.

Discussion

Educational information systems are widely used by almost all universities in Indonesia to facilitate the provision of information to students, staff and administrators. The greater the interaction between the system and the user, the easier it is for the system to be accessed or compromised by unauthorized access. This will become a new security problem. Educational information based on student education management needs to ensure complete security, confidentiality and integrity of information. It was decided to make the best use of the information security system.

Security concerns lead to network access control procedures to protect the network from intruders (Hermadunti *et al* ., 2016). Developing software to support network communications is how to identify ways to facilitate data processing (Imam Riadi *et al* ., 2013). The system can continue to work according to needs and usage. This is important for performance evaluation through analysis. For data security analysis to be successful, standards must be established. There are no established standards by which an organization will select or use information security to use those standards correctly.

Data security is a must. This question is very important because if information can be accessed by unauthorized people, then the accuracy of the information can be questioned and the information could be wrong. Below are examples of some questions in research about whether the security used in educational information systems is in accordance with the application standards of security standards and higher education information directives (Elachgar *et al* ., 2012). In addition, security systems play an important role in protecting information storage from various existing threats.

Information can be said to be good if it is safe and reliable. System security can be seen from user data that is stored safely in the system. This user data must be kept confidential by the data stored by the system, so that other people cannot freely access the user data (Urbach and Muller, 2011). Secure storage of user information will reduce misuse of user information by others.

Security (*security*) in general, *databases*, *servers* , processes, channels, etc. in communications protection. This is a step to ensure confidentiality, integrity and capacity. The goal is to limit access to information only to users who have access rights. The security system also has

e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

the function of preventing data leaks and preventing data from being compromised and compromised. Information security is very important because the Information Exchange Environment *indicates* that hackers are a threat to information, so there is a need to increase information security for businesses, organizations and governments (Hassanzadeh et al., 2014). Research conducted by Sattarova FY, Tao-hoon Kim (2007) shows that computer security aims to protect information from thieves or hackers and the system can only be accessed by users who have access rights.

Data security means ensuring confidentiality, data integrity, availability, consistency, control and review to prevent fraud in data according to the process. According to Humphreys, Edward (2016), ISO/IEC 27001 is a standard for design, implementation, implementation, monitoring and analysis, known as Information Security *Management* or more generally Information Security *Management* . Manage, update and improve ISMS information on global business risks and opportunities.

For ISO/IEC 27001 published by *the International Organization for Standardization* (ISO), this organization has several working groups, one of which is SC27 WG1 which is responsible for ISO/IEC 27001. ISO/IEC 27001:2013 is a revision of ISO/IEC 27001 The previous :2005, ISO/IEC 27001:2005 used a higher level standard to replace the standard in the 2013 version, but still used PDCA (*Plan-Do-Check-Act*) (Humphreys, 2016).

According to *The International Organization for Standardization* (ISO)/IEC 27001 concerning information security management *system* , information security is preventing various threats to information security, thereby ensuring the security of valuable information assets. By improving data security, the risk of data leakage can be reduced. The more information that is managed and shared, the greater the risks, such as damage and loss of data, as well as unwanted disclosure of information to outside parties (Sarno and Iffano: 2009).

According to Sarno and Infani, information security (2009):

1. Physical security *is* a type of information security that aims to protect individuals or organizations, company assets from damage or natural disasters.
2. Personal security refers to the security of information related to personal security, which generally relates to the scope of personal security.
3. Operational security is a type of information security. This refers to how representatives have the right to ensure that operational work capabilities are not compromised.
4. Communications Security *is* a security document that explains how agent authorization will ensure that the agent's ability to operate is not compromised.
5. *Network Security* is information security that focuses on protecting information communications, communications technology and its content, and the ability to use information and communications technology to achieve organizational goals.

The main measure of educational information security is to improve the quality of information security according to the ISO 27001:2013 standard, apart from that, it is also to determine the level of security development used in academic article information. It is hoped that these results can be used as consideration in planning steps to improve information security management.

The International Organization for Standardization ISO has developed various standards for information security management (ISMS) or policies and procedures for information security management (ISMS). ISO 27001:2013 (*International Organization for Standardization*) is an international information security standard that recommends that the use of internationally recognized information security systems in organizations must meet the requirements, but in this article, security controls.

ISO divides all security systems into one single standard such as the ISO 27001 series and some of the standards in the ISO series are as follows:

e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

Table-1: ISO 27001: 2013

Clause	Target
Policy on Information Security	Ensure that information security is directed and managed in accordance with relevant information, policies and laws.
Information security organization	Establish a governance framework to control the use and operation of information security to secure remote work within the organization.
Information Security Human Resources	Make sure all employees understand their roles and responsibilities in the organization.
Asset Management	Identify agent resources and assign appropriate protection responsibilities to agents. Remember to keep records or control information.
Access Control	Ensure the use of appropriate encryption technology to protect the confidentiality, accuracy and integrity of data.
Cryptography	To ensure the use of correct and effective encryption methods to protect data confidentiality, authenticity and data integrity.
Physical and environmental security	Prevent physical control by third parties that could damage the person's data and data center
Safe operation	Ensure that document handling facilities function properly.
Communication security	Ensure data security on networks and data supporting sites.
Procurement/Acquisition, Development and Maintenance of Information Systems	Security is an important part of knowledge.
Relationship with Suppliers	Security is an important part of information.
Management of information security incidents	Ensure internal assets are protected from supplier access.
Aspects of Information Security and Business Continuity	Manage business disruptions and protect critical business processes from IS failure or damage with timely balancing.
Obedience	Prevent violations of any regulatory or contractual obligations and security laws.

Chazar's research (2015) shows that the use of ISO/IEC 27001 can protect all aspects of information security such as confidentiality, integrity and availability. Meanwhile, research by Mokodompit and Nurlaela (2016) shows that improving security requires special attention to security policy, security organization, security of security personnel, physical and environmental security, communication and control, management and compliance. Meanwhile, research results from Syaza Syauqina *et., al* ., (2019), said that the Information Security Culture of the Bandung City Health Center is management, exchange, selling information, problems - Freedom in the workplace and Attitude. Research results from Akraman, *et., al* ., (2018), stated that smartphone users in Indonesia have limited knowledge in managing information security and privacy.

Apart from that, the security system also prevents crimes such as data recovery by unauthorized parties, illegal data interception, and damage to the operating system. The security feature also prevents the system from creating new channels (*masquerades*) that look like illegal

e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

connections. Protection and security of operating systems and hardware requires security services in technical, administrative, legal and political terms. The security system is divided into 3 (three) items, namely:

1. *External* security , namely to protect the computer and all its facilities from intruders and from fire, flood and other damage.
2. User interface security , namely identifying users before they enter the system.
3. *Internal* security , namely security management of hardware and operating systems to ensure integrity and information (Harningsih: 2005).

Systems used to generate information must be free from interference *(noise*), including hackers, who could change or destroy correct data. The system can only be used in accordance with the access policy of each user who has an ID number (PIN). Based on research results, Dyna MK (2011) shows that security is an important issue because the Internet network is a public connection. It is easy for *sniffers* to monitor *passwords* so that user data can be captured. In this case, it is necessary to provide security by combining *the password* with *a string* for encryption.

The system security *of* academic information systems on average does not meet user expectations. This is because data security in the Andalas University Academic Information System (SIA) is still a barrier to access, so information security needs to be improved further so that it cannot be accessed by people who do not have an account. Research by Satoto, *et., al* (2008) states that the weakness of access is that the student identification number (NIM) is not secure. Andalas University's Academic Information System Manager has taken good security measures and must use a PIN to access Academic Information. However, this does not guarantee the security of user data, because by exchanging access with other business partners.

Information sent to the user indicates that data security is not as expected. Information in an information system is a very valuable asset for an organization and must be protected from various threats. Information security has several aspects, for example:

1. Confidentiality , only authorized people can access information.
2. Integrity , the *accuracy* and completeness of data is protected by effective procedures;
3. Availability *means* that authorized parties can access information on request (Sarno and Iffano, 2009).

The need to monitor security regulations, corporate security, personnel security, physical and environmental security, communications and performance management operations, access control, and AIS security compliance. Educational knowledge is a way to meet the knowledge management needs of its users.

Entering the system using a PIN is one way to enter the system by entering the user account ID (Johnston, PA 2005). According to student informants, the login system does not make the system safe from hackers. There is a lack of security when using a Personal Identification Number (PIN), so it is necessary to combine the PIN with a special string as a better password for checking security or data integrity (Figure-1).

IJEC
International Journal of Economics
https://ejournal.ipinternasional.com/index.php/ijec
e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

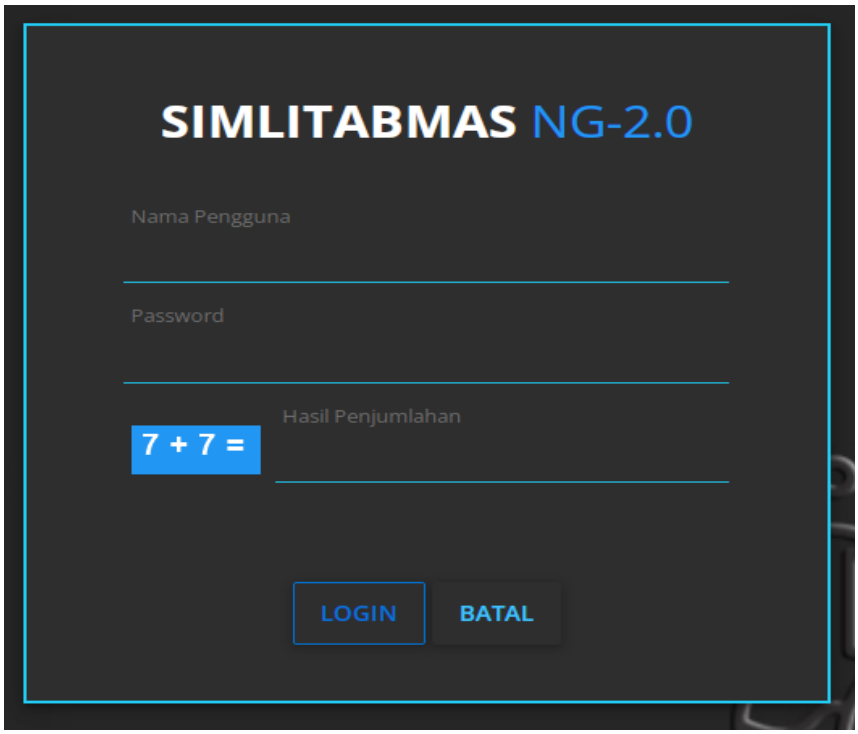

Figure-1: Login System with Combination (Two Factor Authentication) PIN

Factor authentication is an online account security system that adds a two-step verification process to access an account, regardless of the platform used. For this reason, apart from entering your username and password to access, you must first carry out special authentication according to the site you choose.

This verification process includes several methods, including:

1. Information known to the user. Examples include passwords, PINs (*Personal Identification Numbers*), pattern locks or other codes.
2. User-provided information. For example, a mobile phone number or smartphone application used to approve a personal identification request.
3. Biometrics. Thumb, face, eyes, voice, etc.
4. Geolocation. For example, other geolocation features such as IP addresses or smartphone GPS.
5. Personal time. For example, any entry that occurs outside the scheduled time will be rejected.

The above criteria are usually set by the platform or website offering the service, such as an online store or membership site. Users can easily open it to protect their accounts. At the same time, websites that use two-factor authentication *are* better protected from unauthorized access.

It is very useful to use Two Factor Authentication (*2FA*) for websites, here are some advantages of 2FA for websites:

1. **Prevent cyber crimes such as account theft** . Account breaches are on the rise for a variety of purposes, including identity theft, theft of personal information, and even stealing accounts from online businesses. Using 2FA is one way to prevent such account tampering. Because if you don't provide the second proof, you can't access the account. In fact, you will know that someone is trying to access your account from the verification you receive. This way, you can work quickly and safely by changing your username and password.
2. **Save time and operational costs** . Before 2FA, the risk of money leakage was huge. Eventually, many users lost access and had to reset their passwords through customer service. This step must

e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

be done manually because it requires verification of your KTP number and other personal information. Therefore, like it or not, this process requires special assistance for customers. Now, by using the 2-factor authentication method from the start, the chances of breaking into an account are much smaller. Meanwhile, the need to reset passwords is also reduced. As a result, operational costs can be further reduced and time spent reusing these services can be diverted to other, better services.

3. **Increase user trust** . Websites with better number protection will be preferred by visitors. Therefore, if a website uses 2FA for access, there is little chance of their information being misused. With this security guarantee, website users will have more confidence in continuing to use the website's services.
4. **Solutions for weak passwords** . Many people like to use the same password for multiple accounts. Of course, this creates the risk of easy compromise for all accounts. Using 2-factor authentication provides additional protection when you replace all your passwords with stronger ones. Even if someone knows your password, they can't access your account because your phone requires a second authentication.

AIS managers must conduct audits in addition to using ISO security standards and using two-factor authentication. Information analysis is the examination of activities in the information system environment. The purpose of information analysis is to provide ideas and recommendations to management to improve future information management (IT management) and achieve information quality management (IT management). Among other things, IS audits aim to (1) increase the security of company assets, (2) increase information integrity, (3) increase efficiency, and (4) improve performance (Ron Weber, 2000).

Information systems audit is an integral part of the audit function. This audit supports the auditor's assessment of the quality and integrity of information processed by computer systems (*information systems*). Perceptions of the internal audit function have changed dramatically over the years as it has shifted from the traditional perception of being seen as a corporate watchdog to a tool for monitoring compliance with corporate policies and procedures (Menk, 2007); becoming increasingly recognized for encouraging more preventative proactivity (Beecroft, 1997) with a strong focus on risk management and improving business performance; and today, technology is changing the complexity of the audit environment.

In an organization, it is important to carry out data analysis that can be used to see whether the system in the business is appropriate and the most important thing is that the system will contribute to achieving organizational goals. Information Systems Audit Objectives according to Sanyoto (2007), the objective of an IS audit is to measure:

1. **Asset Security** . The objective of an asset protection audit is not explicitly stated (not written) in the COBIT Standard. Company information assets such as hardware, software, human resources, data/documents and other resources must be managed through effective management to prevent misuse of company assets. For this reason, asset security is a very important thing for companies to do.
2. **System Effectiveness.** The effectiveness of corporate information systems plays an important role in decision making. Information systems can be used effectively if they are designed well (*do the right thing*) according to user needs. The information requested by the manager can be fulfilled.
3. **System Efficiency.** Efficiency becomes especially important when resources are limited. If computer application performance deteriorates, management must consider whether system performance is still adequate or resources need to be increased, because data media can be said to be effective if they can meet customer needs with minimal effort. information material. The way to work is the right way (doing good deeds). This also includes calculating the business, business

e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

profits and losses (*cost/benefit*) and more about *value for money* . Profitability is about using the fewest resources to achieve the best results when the economy is good.

4. **Availability.** This is based on the availability of information technology (IT) support/services. IT must be able to support the continuity of the company's operational business. The more frequently blackouts occur (*system outage*), the lower system availability will be.
5. **Confidentiality (*Confidentiality*).** The goal is to protect information and prevent unauthorized persons from accessing it.
6. **Reliability (Reliability).** Concerns the suitability and accuracy of management, reporting and accountability in organizational management.
7. **Maintain Integrity.** Data integrity *is* one of the most important aspects in information technology. Data has the following attributes: completeness, accuracy, and precision. If data integrity is not checked, the company will not have valid data/documentation and may suffer from poor management or poor decision making.

Conclusion

According to *The International Organization for Standardization* (ISO)/IEC 27001 concerning information security management *system* , information security is preventing various threats to information security, thereby ensuring the security of valuable information assets. *Network Security* is information security that focuses on protecting information communications, communications technology and its content, and the ability to use information and communications technology to achieve organizational goals.

The main measure of information security is to improve the quality of information security according to the ISO 27001:2013 standard, apart from that, it is also to determine the level of security development used in academic information. Apart from using ISO, it is also necessary to audit the academic information system and use two-factor authentication *to* access the account.

International Organization for Standardization (ISO) 27001:2013 is an international information security standard that recommends that the use of internationally recognized information security systems in organizations must meet security requirements and controls. ISO divides all security systems into a single standard such as the ISO 27001:2013 series whose goal is to ensure information security. Thus, information security has been managed in accordance with relevant policies.

REFERENCES

Akraman, R., Candiwan, C., & Priyadi, Y. (2018). Pengukuran kesadaran keamanan informasi dan privasi pada pengguna smartphone Android di Indonesia. *Jurnal Sistem Informasi Bisnis*, 8(2), 115.

Al-Sehri. (2012). Information security awareness and culture. *British Journal of Arts and Social Sciences*, 6(1), 61-69.

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security policy compliance: User acceptance perspective. In *System Science (HICSS), 45th Hawaii International Conference on* (pp. 3317-3326). IEEE.

Arens, A. A., & Loebecke, J. K. (2005). *Auditing: An integrated approach* (8th ed.). New Jersey: Prentice Hall Inc.

Beecroft, G. D. (1997). Implementation philosophy: ISO 9000 versus QS 9000. *Total Quality Management*, 8, 83-87.

Chazar, C. (2015). Standar manajemen keamanan sistem informasi berbasis ISO 27001:2005. *Jurnal Informasi*, 7(2), 48-57.

Darmawan, D., & Fauzi, K. N. (2013). *Sistem informasi manajemen*. Bandung: PT Remaja Rosdakarya.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM*, 43(7), 125-128.

e-ISSN: 2961-712X
Vol. 3 Issue 2, July-December 2024
DOI: 10.55299/ijec.v3i2.976

Dhillon, G., & Backhouse, J. (2002). Risks in the use of information technology within organizations. *International Journal of Information Management*, 16(1).

Hermaduanti, N., & Riadi, I. (2016). Automation framework for rogue access point mitigation in IEEE 802.1X-based WLAN. *Journal of Theoretical and Applied Information Technology*, 93(2), 287-296.

Humphreys, E. (2016). *Implementing the ISO/IEC 27001 ISMS standard* (2nd ed.). London: Artech House.

Imam Riadi. (2013). Optimalisasi keamanan jaringan menggunakan pemfilteran aplikasi berbasis Mikrotik. *Jurnal Sistem Informasi Indonesia*.

ISO/IEC. (2013). *International Standard ISO/IEC 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements*.

ISO/IEC. (2013). *International Standard ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls*.

Johnston, P. A. (2005). Login system. Retrieved from http://pajhome.org.uk

Krugger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computer & Security*, 24(4), 289-296.

Laudon, K. C., & Laudon, J. P. (2007). *Sistem informasi manajemen* (10th ed.). Jakarta: Salemba Empat.

McLeod, R., & Schell, G. P. (2008). *Sistem informasi manajemen* (10th ed.). Jakarta: Salemba Empat.

Menk, T. J. (2008). Internal auditing: Key to helping your operations and bottom line. Retrieved from http://www.alpern.com/resources/publications/internal%20audit.html

Mokodompit, M. P., & Nurlaela, N. (2017). Evaluasi keamanan sistem informasi akademik menggunakan ISO 17799: 2000 (Studi kasus pada Perguruan Tinggi X). *Jurnal Sistem Informasi Bisnis*, 6(2), 97-104.

Moleong, L. J. (2013). *Metode penelitian kualitatif* (Edisi Revisi). Bandung: PT Remaja Rosdakarya.

Mulyadi, & Kanaka Puradiredja. (1998). *Auditing* (Edisi Kelima). Jakarta: Salemba Empat.

Ron Weber. (2000). *Information system control and audit*. New Jersey: Prentice Hall Inc.

Sanyoto, G. (2007). *Audit sistem informasi + Pendekatan CobIT* (Edisi Revisi). Jakarta: Mitra Wacana Media.

Sarno, R., & Iffano. (2009). Sistem manajemen keamanan informasi. Surabaya: Percetakan ITS Press.

Satoto, K. I., et al. (2008). Analisis keamanan sistem informasi akademik berbasis web di Fakultas Teknik Universitas Diponegoro. Artikel Ilmiah Terpublikasi *Seminar Nasional Aplikasi Sains dan Teknologi*, 175-186.

Sattarova, F. Y., & Kim, T. H. (2007). IT security review: Privacy, protection, access control, assurance, and system security. *International Journal of Multimedia and Ubiquitous Engineering*, 2(2), 1-7.

Sugiyono. (2015). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Bandung: Alfabeta.

Symantec. (2015). *Information security threat reports*. Symantec Corporation.

Susanto, B. M. (2013). Mengukur keamanan informasi: Studi komparasi ISO 27002 dan NIST 800-55. *Seminar Nasional Teknologi Informasi dan Komunikasi*.

Susanto, H., et al. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical & Computer Sciences*, 11(5).

Thomas, M., & Dhillon, G. (2011). Interpreting deep structures of information systems security. *The Computer Journal*.

Urbach, N., & Mueller, B. (2011). The updated DeLone and McLean model of information systems success. *Springer Science and Business Media*, 28.

Witman, M. E., & Mattord, H. J. (2011). *Principles of information security* (4th ed.). Atlanta: Cengage Learning.

Wood, C. C. (1995). Writing InfoSec policies. *Computers & Security*, 14(8), 667-674.