International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Effective Policies to Protect Information Resources: Identity Management and Organizational Access Studies X

Rudolf Sinaga[1], Samsinar[2], Renny Afriany[3]
[1]Fakultas Ilmu Komputer, [2,3] Program Studi S1 Administrasi Rumah Sakit,
[1]Universitas Dinamika Bangsa, [2,3]STIKES Garuda Putih
Jambi, Indonesia
[1]rudolfverdinan@gmail.com,

Abstract— Information resources are an important asset for organizations, both government and private. Information resources can be data, systems, or applications used to support organizational activities. Therefore, it is important to protect information resources from various threats, such as cyberattacks, misuse, or loss. Identity and access management (IAM) is one of the efforts to protect information resources. IAM is the process of managing the identity of users and their access to information resources. Effective IAM can help organizations ensure that only authorized users can access information resources, detect and prevent unauthorized access to information resources, and facilitate user identity management. This study aims to examine effective IAM policies to protect the information resources of Organization X. The results show that an effective IAM policy must meet the following criteria: comprehensive; IAM policies should cover all aspects of identity and access management, from user identity creation to access review, risk-oriented; IAM policies should be designed to minimize risks to information resources, Flexible; IAM policies must be adaptable to the changing needs of the organization, Management support; IAM policies must be supported by the organization's management to be implemented effectively. Based on the results of this study, it is advisable to ensure that information security policies remain effective over time, so organizations should carry out regular evaluations to protect their information resources.

Keywords- ***identity and access management, information security, information resources***

I. INTRODUCTION

Information resources [1] are an important asset for organizations, both government and private. Information resources can be data, systems, or applications used to support organizational activities. Information sensitive [2] business data is a key component in day-to-day operations, therefore, it is important to protect information resources from various threats, such as cyberattacks, misuse, or loss.

One important aspect [3] in maintaining information security is Identity and Access Management (IAM).

Identity and access management (IAM)) [4] is one of the efforts to protect information resources. IAM is the process of managing the identity of users and their access to information resources. Effective IAM [5] can help organizations to:

a. Ensure that only authorized users can access information resources.
b. Detect and prevent unauthorized access to information resources.

An IAM policy is a document that governs how IAM is implemented in an organization. Effective IAM policy [6] must meet the following criteria:

a. Comprehensive: IAM policies should cover all aspects of identity and access management, from user identity creation to access review.
b. Risk-oriented: IAM policies should be designed to minimize risks to information resources.
c. Flexible: IAM policies must be adaptable to the changing needs of the organization.
d. Management support: IAM policies must be supported by the organization's management to be implemented effectively.

Effective information security policies [7–9] become the main basis for efforts to protect information resources from unauthorized access, data leakage, and cyberattacks. Identity and Access Management plays a crucial role in the management and management of access rights [10] for individuals to information resources needed in the context of the organization. Therefore, this research will focus on reviewing effective information security policies, with particular emphasis on the implementation and practice of Identity and Access Management in Organization X.

But there are still organizations that don't pay attention to identity and access management, this is due to a lack of understanding of potential security risks [2,11–13] which can arise from weak identity and access policies. In addition, some organizations do not yet fully believe that the business value provided by the implementation of identity and access management [14] will increase safety, efficiency, and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

productivity. Some organizations focus more on traditional security solutions [15–18] such as firewalls and antiviruses, and may underestimate the importance of identity and access management as an integral part of an overarching security strategy.

This research is important and urgent because identity and access management greatly impact the threat of information resources, in addition to many organizations experiencing attacks on assets, data leaks, information, and even loss. Therefore, the purpose of this study is to explore an effective IAM policy model to protect information resources. Several gaps must be considered on the topic of Effective Policies to Protect Information Resources, including:

1. Less comprehensive: [14,17,19] Information system security policies often do not cover all security aspects, such as data protection, hardware, and software. This can cause information resources to remain vulnerable to threats.
2. Unclear: [8] Information system security policies are often written in vague and difficult-to-understand language. This can lead to confusion and non-compliance with policies.
3. Not applied consistently: [8,20–22] Information systems security policies are often not applied consistently to organizations. This can lead to security holes that attackers can exploit.
4. Not observed by all parties: [22] All interested parties, such as employees, vendors, and customers, must comply with the information system security policy. It is important to ensure that everyone who has access to an information resource has the same understanding of how to protect it.

In addition to these gaps, several other factors need to be considered to ensure the effectiveness of information system security policies, including:

1. Organizational needs: [13,23] Information system security policies must be tailored to the needs of the organization. Policies that are too restrictive or too lax can be ineffective.
2. Technological change:[24,25] Information system security policies should be updated regularly to keep up with technological developments.
3. Security awareness: [21,26] All interested parties must have a high-security awareness. It is important to ensure that everyone understands the security risks and how to protect themselves.

Organization X, operating across multiple sectors, faces unique challenges in managing user identities and organizing access to their information resources. Technological developments, various information security regulations, and evolving cyber threats are factors that need to be taken into account. In this context, this study aims to identify and analyze the information security policies that have been implemented in Organization X, explore the effective and expanded aspects of regulations, and identify areas of potential improvement.

Through this research, it is expected to find solutions and best practices in Identity and Access Management that can help Organization X and similar organizations to optimize their information security policies. Information safety is a critical cornerstone in maintaining efficient organizational operations, customer trust, and maintaining data integrity. Therefore, the study has significant relevance in an increasingly complex and risky business environment.

II. RELATED WORK

Research [11], concluded that service-oriented architectures (SOAs) have a more secure protocol stack and focus on security by design. Future automotive architectures will require active security measures such as firewalls, intrusion detection, and access control.

Research [27], summing up the average maturity level of IAM in organizations, weaknesses are found in the process of user registration and logging as well as logging and tracking.

Research [28], Summing up the CSSPS proposal as a new set of system properties for the SSI system, the consistency of system properties is analyzed by one analyst.

Research [29], concludes with the proposed work improving cloud security through continuous auditing, while future work aims to improve protocols for IoT devices.

Researchers [30], Conduct a comprehensive analysis of facial identity threats and conclude proposed taxonomies for facial identity threats, and potential facial identity threats as well as a comparative analysis of coping techniques.

Researchers [2], resulting in the critical secure and dynamic access management, and concluding that decentralized identity is the future of IAM.

Researchers [12], concluded that blockchain integration increases trust in infrastructure as well as optimizations and improvements required for cryptographic elements and query times.

Researchers [31], That cyber security is a complex subject that requires interdisciplinary expertise, user education is essential to prevent cyber risks.

Researchers [32], Summing up a multi-authority attribute-based access control scheme that preserves the proposed privacy and ensures blockchain data confidentiality and fine-grained access control for data sharing

Researchers [33] infer that PHI confidentiality and authorized access is critical, and IAM systems enable fast and secure access to critical information.

Researchers [34], concluded the proposal of an integrated energy management platform and cross-system energy transactions and unified authentication.

Researchers [35], concluded IAM solutions improve infection control and patient safety and hospitals should consider IAM use cases for future surges.

Researchers [36], Summing up insider threats is a major concern in organizations and VIstaS authentication systems are effective and practical.

Researchers [37], Cloud CDM requires secure access control for researchers and proposed service models using DID and blockchain technology.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Researchers [38], concluded that the proposed SM9-ABE scheme performs well in security and functionality and SM9-ABE is desirable for fine-grained access control in DCC.
Researchers [39], concluded that the new methodology for managing cyber security, the digital service chain, and the proposed framework are promising tools for security strengthening.
Researchers [5], Conclude with the recommendations of a robust and secure cloud framework and proposed system ensuring secure data access, security, and data integrity

III. IAM

AIM (Access and Identity Management)

Access management [40,41] refers to the process of controlling and monitoring access to resources, systems, and information within an organization. It involves implementing policies, procedures, and technologies to ensure that only authorized individuals or entities are granted access to appropriate resources and data.

Access management [42] It typically includes the following activities:

1. Authentication: Verifies the identity of the user or device trying to access the system or resource. This can be done through various methods such as passwords, biometrics, or two-factor authentication.

2. Authorization: Specifies the level of access privileges a user or device should have based on their roles, responsibilities, and permissions. This includes determining what actions or data are allowed to be accessed, modified, or deleted.

3. Access control: Implement mechanisms to enforce authorized access rights and prevent unauthorized access. This can be achieved through technologies such as firewalls, intrusion detection systems, or role-based access control (RBAC) systems.

4. User provisioning: Manage the creation, modification, and deletion of user accounts and access privileges. This includes processes for onboarding new employees, granting temporary access, and deactivating accounts when no longer needed.

5. Audit and monitoring: Regularly review and monitor access logs and activity to detect suspicious or unauthorized access attempts. This helps in identifying potential security breaches or policy violations.

Effective access management is critical to maintaining the confidentiality, integrity, and availability of sensitive information and resources. It can help organizations prevent unauthorized access, data breaches, and insider threats while ensuring authorized users can perform their tasks efficiently.

AIM refers to access and identity management, a system or strategy used to control access to online resources. This involves managing user identities and ensuring that only authorized individuals can access certain online content.

The AIM system in system can use various access control mechanisms, such as IP authentication, username/password authentication, and federated identity management. The system aims to provide secure and seamless access to online resources while protecting user privacy. Information systems need to adopt a comprehensive AIM strategy to effectively manage access to online content and ensure that users can access the resources they need.

IV. PROPOSED SYSTEM

To overcome these gaps, this study proposed an information system security policy system that is comprehensive, clear, applied consistently, and adhered to by all parties. This system consists of three main components, namely:

1. Information system security policy: The information system security policy should cover all security aspects, such as data protection, hardware, and software. Policies should be written in clear, easy-to-understand language, and can be implemented consistently throughout the organization.
2. Software management policies: Software management policies can help organizations implement and monitor the implementation of information system security policies. This software can help organizations to:
    a. Manage various information system security policies.
    b. Allocate roles and responsibilities to employees.
    c. Track policy compliance.
3. Security awareness programs: Security awareness programs can help increase employees' security awareness of security risks and how to protect themselves.

V. RESULT & DISCUSSION

Result

Effective policies in protecting information resources are the implementation of strict data security policies, such as the use of encryption and firewalls that can protect data from unauthorized access. In addition, policies on using strong passwords and changing passwords frequently also help protect information resources from cyberattacks. Data loss prevention policies such as regular data backups are also important to protect information resources from unexpected events such as damage. Here is an analysis of policies that are effective in protecting information resources:

1. **Identification and protection of information resources**
   This stage is an important step in maintaining data security. By identifying the most valuable information resources that are vulnerable to attack, organization X can take appropriate protective measures. In organization X, this stage is done by granting limited access permissions to sensitive data and encrypting data stored on the organization's computer devices. Thus,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

these organizations can prevent unauthorized access and protect data from theft or unauthorized use.

2. **Continuous management to ensure the sustainability of information sources**
   Organization X undertakes continuous management to ensure the sustainability of information sources. At this stage, the organization conducts regular monitoring and updates to the security system used. In addition, the organization establishes clear policies and procedures for managing information sources, including in terms of data use, storage, and deletion. With sustainable management, organizations can maintain the sustainability and reliability of their information sources.
3. **Community empowerment in managing information sources**
   Community empowerment in the management of information sources is also important to maintain the sustainability and reliability of information sources. Organization X engages the community (stakeholders of organization X) in the process of collecting and updating data and provides training on the correct and safe use of information. Thus, the community will become an active partner in maintaining the security and quality of information sources, so that they can play a role in maintaining the sustainability of the company or organization.

To find out information about the level of effectiveness of information resource protection policies in organization X, a policy assessment analysis was carried out to understand the effectiveness of policies and make necessary improvements to 83 employees consisting of the head of IT, IT staff, general, and employees. The results of the assessment carried out based on several aspects are as follows:

1. Information Security Policy

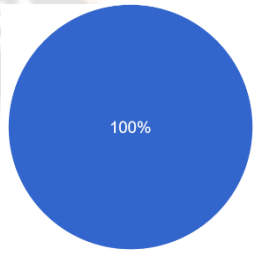

Figure 1. Availability of written policies

Figure 1 shows that 100% of respondents stated that an organization has an information security policy written.

Table 1. Policy Revision Interval

If Yes, how often is this policy revised and updated?				
Every 2 Years	Every Year	Never	Not sure	Grand Total
6	42	23	12	83

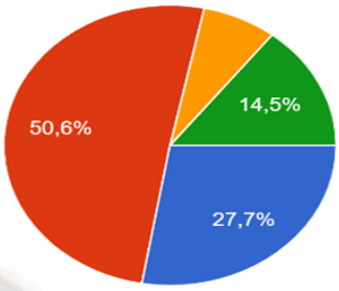

Figure 2. Policy revision interval

Table 1 and Figure 2 show that as many as 42 people or 50.6% of respondents stated that policy revisions or changes are made every year, 23 people, or 27.7% stated never, 12 people, or 14.5% stated unsure and 6 people, or 7.2% stated every 2 years. From this data, it can be concluded that the implementation of information security policies has not been implemented consistently in all units.

2. Identity and Access Management

Table 2. Identity Management Procedures

Does your organization have procedures for user identity management (e.g., registration, account deactivation)?	
Yes	Grand Total
100,00%	100,00%

Figure 3. Availability of IAM procedures

Table 2 and Figure 3 show that 100% of respondents stated that organizations already have user identity management procedures in place.

Table 3. Management of access rights to resources

How does your organization manage user access rights to information resources?

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Based on the principle of user needs (updates and revisions)	No clear management	Grand Total
98,80%	1,20%	100,00%

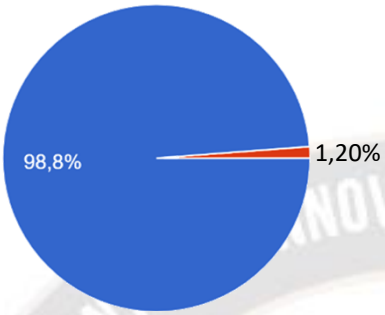

Figure 4. Management of access rights to resources

Table 3 and Figure 4 show that as many as 82 people or 98.8% of respondents stated that organizations manage user access rights to information resources based on the principle of needs, and 1 person, or 1.20% stated that there is no clear management. From this data, it can be concluded that organizations implement the management of access rights to information resources based on the principle of user needs, but still need thorough socialization so that no party feels ignorant.

3. Physical and Logical Safeguards

Table 4. Physical security procedures

Does your organization have physical security measures in place to protect information resources, such as limited access to data centers or servers?		
Don't know	Yes	Grand Total
1,20%	98,80%	100%

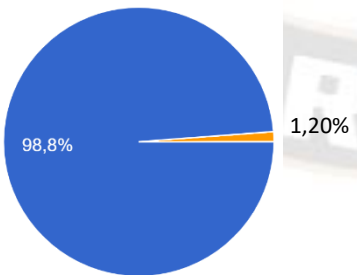

Figure 5. Physical security procedures

Table 4 and Figure 5 show that as many as 82 people or 98.8% of respondents stated that organizations have physical security measures in place to protect information resources, such as limited access to data centers or servers, 1 person, or 1.20% stated that they did not know. From this data, it can be concluded that the organization already has procedures or physical security measures for resources, but still needs thorough socialization so that no party does not know these procedures.

Table 5. Use of encryption

Does your organization use encryption to protect sensitive data in transit over the network?		
Don't know	Yes	Grand Total
2,41%	97,59%	100,00%

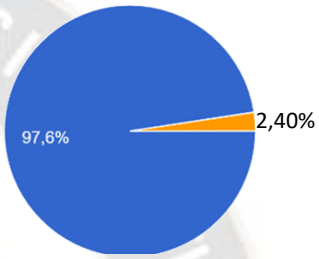

Figure 6. Use of encryption

Table 5 and Figure 6 show that as many as 81 people or 97.59% of respondents stated that the organization has used encryption methods to protect sensitive data on the network, and 2 people, or 2.40% stated that they did not know. From this data, it can be concluded that organizations have implemented encryption methods to protect sensitive data when transacting on the network, but still need thorough socialization so that all relevant parties understand the policy.

4. Monitoring and Audit

Table 6. Monitoring system

Does your organization have a security monitoring system in place to detect suspicious activity or cyber threats?		
No	Yes	Grand Total
3,60%	96,40%	100,00%

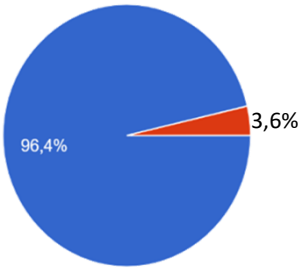

Figure 7. Monitoring system

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Table 6 and Figure 7 show that as many as 80 people or 96.40% of respondents stated that the organization has a security monitoring system in place to detect suspicious activity or cyber threats, and 3 people, or 3.60% stated that they do not or do not have one. From this data, it can be concluded that the organization already has a security monitoring system, but a thorough review is needed to ensure all relevant parties have understood the security management policies that apply to the organization.

Table 7. Security policy compliance audits

Does your organization conduct regular audits to check compliance with information security policies?		
No	Yes	Grand Total
7,20%	92,80%	100,00%

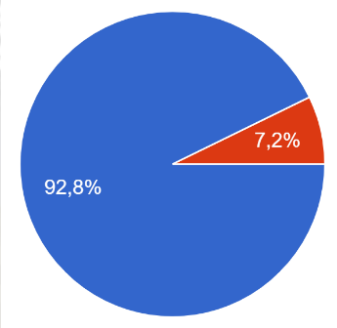

Figure 8. Security policy compliance audits

Table 7 and Figure 8 show that as many as 77 people or 92.80% of respondents stated that the organization had conducted an audit of information system security policy compliance, and 6 people, or 7.20% stated that they did not or had not done so. From this data, it can be concluded that the organization has conducted an information system security policy compliance audit, but a thorough review of all users is needed to ensure that all relevant parties have understood the security management policies that apply to the organization.

5. Education and Security Awareness

Table 8. Information security education

Does your organization provide information security training for employees?		
No	Yes	Grand Total
1,20%	98,80%	100,00%

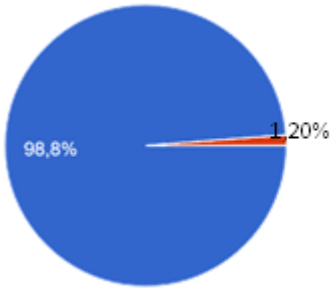

Figure 9. Information security education

Table 8 and Figure 9 show that as many as 82 people or 98.20% of respondents stated that the organization has conducted information security education, and 1 person, or 1.20% stated that it has not or has not done so. From this data, it can be concluded that the organization has carried out educational activities about security, but a thorough review is needed so that all relevant parties understand the security management policies that apply to the organization.

Table 9. Promotion of security awareness

Bagaimana organisasi Anda mempromosikan kesadaran keamanan di antara karyawan?			
Through internal communication	Through regular training	No special efforts	Grand Total
72,29%	25,30%	2,41%	100,00%

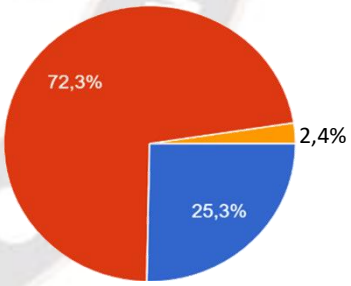

Figure 10. Promotion of security awareness

Table 9 and Figure 10 show that as many as 60 people or 72.30% of respondents stated that organizations promote security awareness among employees through internal communication, and 21 people or 25.30% through regular training while 2 people, or 2.40% stated that there is no specific effort to promote security awareness among employees. From this data, it can be concluded that the organization promotes security awareness to most employees through internal communication, while some other employees promote it with regular training, besides that there are still employees who state no effort is made by the organization. Therefore, a thorough

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

review is needed so that all relevant parties have understood the security management policies that apply to the organization.

6. Continuity and Surveillance

Table 10. Security policy effectiveness

How does your organization ensure information security policies remain effective over time?		
Through regular evaluations	There is no specific mechanism	Grand Total
96,40%	3,60%	100,00%

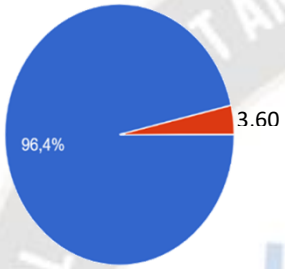

Figure 11. Security policy effectiveness

Table 10 and Figure 11 shows that as many as 80 people or 96.40% of respondents stated that to ensure information security policies remain effective over time, the organization conducts regular evaluations, and 3 people, or 3.60% stated that the organization does not have a certain mechanism. From this data, it can be concluded that organizations conduct regular evaluations to ensure the effectiveness of security policies, but a thorough review of all users is needed to ensure that there are no more users who do not understand the security management policies that apply to the organization.

Table 11. Security policy stakeholder engagement

How does your organization involve stakeholders in decision-making regarding information security policies?		
Through active collaboration	Limited to information security teams	Grand Total
89,20%	10,80%	100,00%

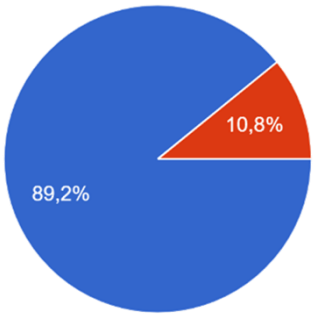

Figure 12. Security policy stakeholder engagement

Table 11 and Figure 12 shows that as many as 74 people or 89.20% of respondents stated that organizations actively collaborate in involving related parties in decision-making on security policies, and 9 people, or 10.80% stated that they are only limited to the organization's information security team. From this data, it can be concluded that most users in the organization understand party involvement is done with active collaboration, but there are still other users who understand the involvement of decision-making only at the team level. Therefore, a thorough review and socialization of all users is needed so that all parties can understand the security management policies that apply to the organization.

Discussion

Information system security policy is one of the important components of information system security. Effective policies can help protect information resources from a variety of threats, such as data theft, misuse, and cyberattacks. An effective information system security policy should cover all security aspects, such as data protection, hardware, and software. The policy should include the following:

1. Purpose and scope of the policy
2. Definition of terms and acronyms
3. Security principles
4. Specific policies and procedures
5. Accountability and accountability
6. Monitoring and evaluation

An effective information system security policy must be written in clear and easy-to-understand language. It is important to ensure that all employees understand the applicable security policies and procedures.

An effective information systems security policy must be applied consistently throughout the organization. This is important to ensure that these security policies and procedures are implemented effectively.

An effective information system security policy must be adhered to by all parties. It is important to ensure that everyone who has access to an information resource has the same understanding of how to protect it.

Effective policy implementation of information system protection in terms of access and identity management provides significant positive benefits and impacts. With this policy in place, organization X can ensure that only authorized individuals have access to sensitive and important information. This will reduce the risk of data leakage and misuse of information by irresponsible parties. In addition, this policy can also increase the efficiency and productivity of the company, because each individual will have appropriate access.

1. Maintain and improve the quality of informationsources

Several things are done to guarantee maintain and improve the quality of information sources:

a. Encourage collaboration and exchange of information between departments

In this case, organization X implements a database management system that allows regular updating and validation of information. By maintaining the quality of information sources, organizations can avoid data errors and inaccuracies that can lead to wrong decisions. Organizations also create online forums or communication platforms that allow departments to share information in real time.

Thus, teams can work together to collect and analyze data more efficiently, improving the accuracy and speed of decision-making and minimizing errors and information loss are other benefits of this policy. With online forums or communication platforms, departments can give each other feedback and find solutions together to problems that arise. This can reduce the risk of errors in decision-making and also avoid losing important information.

b. Strengthen data security and customer privacy
When there is a problem in the data security system or customer privacy, the IT department and the legal department collaborate through communication platforms to find effective solutions and ensure that customer data remains safe and their privacy is maintained.

2. Prevent loss and damage to information resources
Organization X should use a data backup and recovery system to prevent loss and damage to information resources. By keeping regular backup copies of data and using reliable recovery technology, organizations ensure that critical information remains secure and available in emergencies such as natural disasters or cyberattacks.

3. *Encourage the development of sustainable security systems*

In software development, organizations implement continuous security practices in the software development cycle. This includes regular security checks, identifying and fixing security vulnerabilities, and involving security experts or companies in the development process. In this way, security systems can be continuously improved and protect data and users from threats that may arise.

Thus, it is important to continue to encourage the development of sustainable security systems to ensure the security of data and users from evolving threats. Continuous security systems can be continuously improved and updated as new technologies and attack methods evolve. In addition, collaboration between software developers and security experts can help identify and address possible security gaps. With a continuous security system in place, organizations and individuals can have a sense of security and trust that their data and information are well protected.

VI. CONCLUSION

This article has explained in detail that the IAM policy that is effective for organization X is that it must meet the criteria: comprehensive, risk-oriented, and volatile. IAM should be designed to minimize risk to information resources, fluctuate, be adapted to the changing needs of the organization, support management, and be supported by organizational management to be implemented effectively. An effective information security policy is the main basis for protecting information resources from unauthorized access, data leakage, and cyberattacks.

To improve effective information security policies, special emphasis is placed on the implementation and practice of Identity and Access Management in Organization X. However, organizations still find some obstacles that do not even pay attention to identity and access management, this is due to a lack of understanding of effective information security. Here are some recommendations to improve the effectiveness of information system security policies:

1. Commitment from management: Top management must give full commitment to the security of information systems. This commitment will be reflected in the security policies and procedures implemented in the organization.
2. Socialization and training: Information system security policies should be socialized and trained for all employees. It is important to ensure that all employees understand the applicable security policies and procedures.
3. Monitoring and evaluation: The implementation of information system security policies should be monitored and evaluated periodically. This is important to ensure that these security policies and procedures are implemented effectively.

VII. ACKNOWLEDGEMENT

Thank you to the editorial team of the International Journal on Recent and Innovation Trends in Computing and Communication for providing the opportunity to submit our article and of course with the hope that it will get a review and hopefully it can be published.

REFERENCES

[1] Luskatov I V., Pilkevich S V. Model for Identifying Cyber Threats to Internet Information Resources. Automatic Control and Computer Sciences 2019;53:987–94. https://doi.org/10.3103/S0146411619080170.

[2] Badirova A, Dabbaghi S, Moghaddam FF, Wieder P, Yahyapour R. A Survey on Identity and Access Management for Cross-Domain Dynamic Users: Issues, Solutions, and Challenges. IEEE Access 2023;11:61660–79. https://doi.org/10.1109/ACCESS.2023.3279492.

[3] Astorga J, Barcelo M, Urbieta A, Jacob E. How to Survive Identity Management in the Industry 4.0 Era. IEEE Access 2021;9:93137–51. https://doi.org/10.1109/ACCESS.2021.3092203.

[4] Partida A, Criado R, Romance M. Identity and access management resilience against intentional risk for blockchain-based IOT platforms. Electronics (Switzerland) 2021;10:1–26. https://doi.org/10.3390/electronics10040378.

[5] Sonya A, Kavitha G. A data integrity and security approach for health care data in a cloud environment. Journal of Internet Services and Information Security 2022;12:246–56. https://doi.org/10.58346/JISIS.2022.I4.018.

[6] Zhao Y, Tian B, Niu Y, Zhang H, Yi Z, Zeng R. A security management and control solution of smart park based on sensor networks. Sensors 2021;21. https://doi.org/10.3390/s21206815.

[7] Choi M. Leadership of information security Manager on the effectiveness of information systems security for secure sustainable computing. Sustainability (Switzerland) 2016;8. https://doi.org/10.3390/su8070638.

[8] Bansal G, Muzatko S, Shin S Il. Information system security policy noncompliance: the role of situation-specific ethical orientation. Information Technology and People 2021;34:250–96. https://doi.org/10.1108/ITP-03-2019-0109.

[9] Petrov P, Kuyumdzhiev I, Malkawi R, Dimitrov G, Jordanov J. Digitalization of Educational Services about Policy for Information Security. TEM Journal 2022;11:1093–102. https://doi.org/10.18421/TEM113-14.

[10] Saidi H, Labraoui N, Ari AAA, Maglaras LA, Emati JHM. DSMAC: Privacy-Aware Decentralized Self-Management of Data Access Control Based on Blockchain for Health Data. IEEE Access 2022;10:101011–28. https://doi.org/10.1109/ACCESS.2022.3207803.

[11] Rumez M, Grimm D, Kriesten R, Sax E. An Overview of Automotive Service-Oriented Architectures and Implications for Security Countermeasures. IEEE Access 2020;8. https://doi.org/10.1109/ACCESS.2020.3043070.

[12] Abu-Alhaija M. Cyber security: Between challenges and prospects. ICIC Express Letters, Part B: Applications 2020;11:1019–28. https://doi.org/10.24507/icicelb.11.11.1019.

[13] Pöhn D, Seeber S, Hommel W. Combining SABSA and Vis4Sec to the Process Framework IdMSecMan to Continuously Improve Identity Management Security in Heterogeneous ICT Infrastructures. Applied Sciences (Switzerland) 2023;13. https://doi.org/10.3390/app13042349.

[14] Jeon S, Son I, Han J. Exploring the role of intrinsic motivation in ISSP compliance: enterprise digital rights management system case. Information Technology and People 2021;34:599–616. https://doi.org/10.1108/ITP-05-2018-0256.

[15] Patrick Keenan K. Creating spaces of public insecurity in times of terror: The implications of code/space for urban vulnerability analyses. Environment and Planning C: Politics and Space 2019;37:81–101. https://doi.org/10.1177/2399654418776660.

[16] Kuo KM, Talley PC, Lin DYM. Hospital Staff's Adherence to Information Security Policy: A Quest for the Antecedents of Deterrence Variables. Inquiry (United States) 2021;58. https://doi.org/10.1177/00469580211029599.

[17] Meng Y, Huang Z, Shen G, Ke C. A security policy model transformation and verification approach for software-defined networking. Comput Secur 2021;100. https://doi.org/10.1016/j.cose.2020.102089.

[18] Chang V, Golightly L, Modesti P, Xu QA, Doan LMT, Hall K, et al. A Survey on Intrusion Detection Systems for Fog and Cloud Computing. Future Internet 2022;14. https://doi.org/10.3390/fi14030089.

[19] Alraja MN, Butt UJ, Abbod M. Information security policies compliance in a global setting: An employee's perspective. Comput Secur 2023;129. https://doi.org/10.1016/j.cose.2023.103208.

[20] Somchart Fugkeaw. Q1-Achieving Decentralized and Dynamic SSO-Identity Access Management System for Multi-Application Outsourced in Cloud. IEEE 2017;XX.

[21] Amo D, Gómez P, Hernández-Ibáñez L, Fonseca D. Educational warehouse: Modular, private and secure cloudable architecture system for educational data storage, analysis and access. Applied Sciences (Switzerland) 2021;11:1–19. https://doi.org/10.3390/app11020806.

[22] Indu I, Anand PMR, Bhaskar V. Identity and access management in cloud environment: Mechanisms and challenges. Engineering Science and Technology, an International Journal 2018;21:574–88. https://doi.org/10.1016/j.jestch.2018.05.010.

[23] Grüner A, Mühle A, Meinel C. ATIB: Design and Evaluation of an Architecture for Brokered Self-Sovereign Identity Integration and Trust-Enhancing Attribute Aggregation for Service Provider. IEEE Access 2021;9:138553–70. https://doi.org/10.1109/ACCESS.2021.3116095.

[24] Alshammari K, Beach T, Rezgui Y, Alelwani R. Built Environment Cybersecurity: Development and Validation of a Semantically Defined Access Management Framework on a University Case Study. Applied Sciences (Switzerland) 2023;13. https://doi.org/10.3390/app13137518.

[25] Ra G, Kim T, Lee I. VAIM: Verifiable Anonymous Identity Management for Human-Centric Security and Privacy in the Internet of Things. IEEE Access 2021;9:75945–60. https://doi.org/10.1109/ACCESS.2021.3080329.

[26] Li H, Yoo S, Kettinger WJ. The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches. Journal of Management Information Systems 2021;38:222–45. https://doi.org/10.1080/07421222.2021.1870390.

[27] Schrimpf A, Drechsler A, Dagianis K. Assessing Identity and Access Management Process Maturity: First Insights from the German Financial Sector.

Information Systems Management 2021;38:94–115. https://doi.org/10.1080/10580530.2020.1738601.

[28] Pattiyanon C, Aoki T. Compliance SSI System Property Set to Laws, Regulations, and Technical Standards. IEEE Access 2022;10:99370–93. https://doi.org/10.1109/ACCESS.2022.3204112.

[29] Rupa CH, Patan R, Al-Turjman F, Mostarda L. Enhancing the access privacy of IDAAS system using SAML protocol in fog computing. IEEE Access 2020;8:168793–801. https://doi.org/10.1109/ACCESS.2020.3022957.

[30] Rusia MK, Singh DK. A comprehensive survey on techniques to handle face identity threats: challenges and opportunities. Multimed Tools Appl 2023;82:1669–748. https://doi.org/10.1007/s11042-022-13248-6.

[31] Moreno RT, Garcia-Rodriguez J, Bernabe JB, Skarmeta A. A Trusted Approach for Decentralised and Privacy-Preserving Identity Management. IEEE Access 2021;9:105788–804. https://doi.org/10.1109/ACCESS.2021.3099837.

[32] Liu C, Xiang F, Sun Z. Multiauthority Attribute-Based Access Control for Supply Chain Information Sharing in Blockchain. Security and Communication Networks 2022;2022. https://doi.org/10.1155/2022/8497628.

[33] Gellert GA. Leveraging identity and access management technology to accelerate emergency COVID-19 vaccine delivery. Ther Adv Vaccines Immunother 2023;11. https://doi.org/10.1177/25151355231173830.

[34] Zhang Q, Bai F, Yu Z, Liu Y, Shen T, Xie A, et al. Editable and Verifiable Anonymous Authentication Incorporating Blockchain in the Internet of Energy. Electronics (Switzerland) 2022;11. https://doi.org/10.3390/electronics11131992.

[35] Gellert GA, Kelly SP, Hsiao AL, Herrick B, Weis D, Lutz J, et al. COVID-19 surge readiness: use cases demonstrating how hospitals leveraged digital identity access management for infection control and pandemic response. BMJ Health Care Inform 2022;29. https://doi.org/10.1136/bmjhci-2022-100680.

[36] Ali A, Ahmed M, Khan A, Anjum A, Ilyas M, Helfert M. VisTAS: Blockchain-based Visible and Trusted Remote Authentication System. PeerJ Comput Sci 2021;7:1–26. https://doi.org/10.7717/PEERJ-CS.516.

[37] Kang Y, Cho J, Park YB. An empirical study of a trustworthy cloud common data model using decentralized identifiers. Applied Sciences (Switzerland) 2021;11. https://doi.org/10.3390/app11198984.

[38] Ji H, Zhang H, Shao L, He D, Luo M. An efficient attribute-based encryption scheme based on SM9 encryption algorithm for dispatching and control cloud. Conn Sci 2021;33:1094–115. https://doi.org/10.1080/09540091.2020.1858757.

[39] Repetto M, Striccoli D, Piro G, Carrega A, Boggia G, Bolla R. An Autonomous Cybersecurity Framework for Next-generation Digital Service Chains. Journal of Network and Systems Management 2021;29. https://doi.org/10.1007/s10922-021-09607-7.

[40] Spacey R, Cooke L, Muir A, Creaser C, Loughborough University. Library & Information Statistics Unit, Arts & Humanities Research Council (Great Britain). Managing access to the internet in public libraries (MAIPLE). n.d.

[41] Rachna Dhamija. Identity Management 24. 2008.

[42] Macy jason. Product vs toolkit- API and IAM security. Network Security n.d.