

**HANOI UNIVERSITY**

**FACULTY OF INFORMATION TECHNOLOGY**

**IIS MIDTERM REPORT**

**1801040089 – ĐỖ VĂN HÒA – IIS03**

**TABLE OF CONTENTS**

LISTS OF FIGURES……………………………………………………….....3

1. Introduction…………………………………………………………………4
2. The definition and importance of Security Policy………………………….4
   1. What is a Security Policy?............................................................... 4
   2. Why companies need a Security Policy .......................................... 5
3. Key elements of information Security Policy................................................ 6
   1. Purpose............................................................................................ 6
   2. Scope................................................................................................7
   3. Information security goals.............................................................. 7
   4. Authority and Access Control Policy……………………………. 7
   5. Data classification........................................................................... 8
   6. Data support and operations……………………………………… 8
   7. Security awareness and behavior………………………………… 9
   8. Responsibilities, rights, and duties of personnel…………………. 9
4. Steps to develop an effective Security Policy…………………………….. 10
   1. Get leadership involved…………………………………………. 10
   2. Identify the risks………………………………………………… 10
   3. Choose the security level matching the risk…………………….. 10
   4. Reach consensus……………………………………………….... 11
   5. Train Employees……………………………………………….... 11
5. Case study: Information Security Policy in the University
   1. Purpose……………………………………………….................. 11
   2. Organizational Scope…………………………………………… 12
   3. Key ISP definitions………………………………………………12
   4. Policy Statements……………………………………………… 13
      1. Information Security Responsibilities……………………13
      2. Security Policy Framework………………………………14
      3. Information Protection and Classification………………. 15
      4. Training and Awareness………………………………… 16
      5. Acceptable Use………………………………………….. 16
   5. Related Documentation………………………………………… 16
6. Conclusion………………………………………………………………..16

REFERENCE……………………………………………………………….. 17

**LISTS OF FIGURES**

**Figure 1:** CIA Triad…………………………………………………………… 5

**Figure 2:** User Access Controls and Authorization Policy…………………… 8

**Figure 3*:*** Information Security Awareness Training…………………............. 9

**Figure 4:**Information Security Framework…………………………….......... 14

**Figure 5:**Information Protection and Classification…………………………. 15

1. **Introduction**

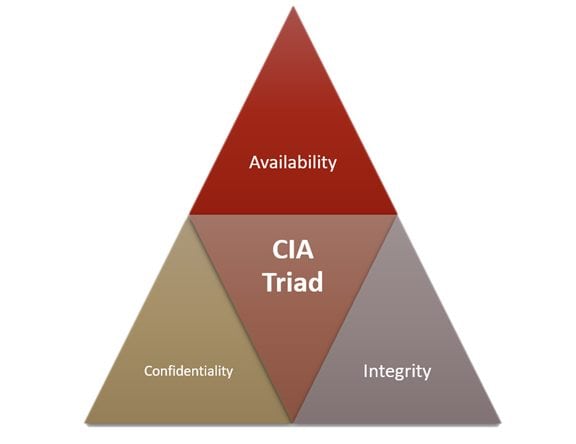
In recent years, institutions of all shapes and sizes have been utilizing information systems and technologies to thrive and succeed in a dynamic world. Organizations are progressively relying on the availability and accessibility of great quality information within their systems. The sensitive information has been highly paid attention by hackers, cyber criminals and rogue employees who try to ruin the company’s reputation by stealing or exploiting the data (Annureet Bajwa, 2018). Therefore, it is absolutely crucial that adequate security and control procedures are provided to ensure that all sensitive information is safe within their information systems to protect its integrity and confidentiality (Dhillon & Backhouse, 2001)**.** This has made companies recognize their responsibilities for safeguarding their physical and information assets because there are a great number of evidences mentioning that the frequency and severity of the attacks are considerably increasing every year. Hackers own a variety of types of cyber-attacks such as malware, phishing, denial-of-service attack and many other ones, which can cause huge damage to organizations, even top companies including Google, Facebook, Tesla, etc... Hence, an efficient Information Security demands to understand the implementation of security policies that will help enterprises protect their valuable properties.

1. **The definition and importance of Security Policy**
   1. *What is a Security Policy?*

A security policy is a written document for an organization that describes how to protect the company from threats, including computer security threats, and how to manage situations when they arise (techopedia, 2017). It provides employees with information of the reasonable use of their properties and defines what is permissible and what is not. Thus, this allows staff to understand and participate in protecting the information systems of their companies.

In technopedia.com, the author explains that a security policy should identify the core elements in an organization which must be secured. Computer’s network and its physical building are two typical examples of the previous idea. Moreover, potential threats to those elements such as cyber-attack, physical damage and so on must be carefully evaluated in the security policy. When the risks are defined, it is important to assess the probability that they will actually happen. These potential threats can be addressed by clearly establishing certain fields in the security policy including administrative and user responsibilities, intrusion detection, risk management, password policies, email policies, internet policies, and disaster recovery. This helps staff react and recover from most circumstances in minimum time. In addition, the data security process needs to be reviewed frequently and updated when new employees join the organization.

* 1. *Why companies need a Security Policy*

A security policy includes pre-approved administrative procedures that tell you exactly what to do to avoid security problems and next steps should you ever face data breach (Ng, 2020). Security issues can be shown by three key factors:

***Figure 1: CIA Triad***

* Confidentiality – People possess or share information improperly
* Integrity – Information is altered or inappropriately validated, whether accidental or intentional.
* Availability – Information is not accessible when it is requested or being available to more users than it should be

Hence, owning a security policy will guarantee that all staff in the organization are on the same page about security processes and procedures. In addition, there is a huge number of threats every single day for any associations containing highly sensitive assets, so it is becoming necessary to have a good security policy. Recently, many famous IT websites simultaneously have reported that Ransomware scumbags leak Boeing, Lockheed Martin, SpaceX documents after contractor refuses to pay (Corfield, 2020). Visser Precision is a US supplier and design contractor whose customers are supposed to include SpaceX, Tesla and Boeing has been attacked by a new type of cyberattack called DoppelPaymer ransomware. There are various types of documents that has been leaked in this hit such as billing and payment forms, supplier information, data analysis reports, legal paperwork and non-disclosure agreement between Visser Precision and both Tesla and SpaceX (Ikeda, 2020). These files are regard as sensitive business information which can cause potential threats to the top companies as the files are publicly accessible. According to Javvad Malik, Security Expert at KnowBe4.com says that “Ransomware including DoppelPaymer is becoming more preferred by criminals because it not only encrypts files like traditional ransomware but also steals the data before doing so”. He also explains “This approach does not only make attacks more powerful, but also broadens the possible targets that criminals can strike and feel forced to pay” (Ikeda, 2020). The reason for the attack was still a mystery because both Visser Precision and the three giant organizations such as SpaceX, Tesla and Boeing did not respond to the hit. However, there are a few noticeable comments on the topic in some security forums.

In slahdot.org, a username called guruevi shared his opinion: “This involves poor security protocols as much as criminal do bad stuff. It could have happened to any other state actor, and they would have a continuous node in the Lockheed and Boeing networks. The issue is that managers are denying to supply proper equipment for these people and then want the authority to investigate whenever something bad occurs. There is no longer any excuse for the appearance of ransomware, it is just poor security and corporate actors to let this happen” (guruevi, 2020). Another person with the nickname - GoldenJoe24 on reddit.com discuss the hot topic: Ransomware is a favor to companies. If a handful of people, or even one guy, can infiltrate your network this badly, you can be certain every major government around the world is, too. Your security policy has failed, and now you have a second chance.” (GoldenJoe24, 2020). From all the viewpoints above on the attack, it is quite certain that having an effective security policy is really essential.

1. **Key elements of information Security Policy**

A security policy can be as wide as the user would like it to be, but enforceable in its full extent, from anything related to IT protection to the protection of relevant physical properties (Cassetto, 2019). The following list provides some significant factors when establishing a strategy for security policy.

* 1. *Purpose*

Organizations construct Security Policy for a variety of reasons:

* To develop a general approach to information security
* To detect and avert information security vulnerabilities including misuse of data, networks, applications, and computer systems
* To safeguard the prestige of the organization in respect of its ethical and legal responsibilities
* To respect the rights of customers, including how to response to questions and complaints about non-compliance
  1. *Scope*

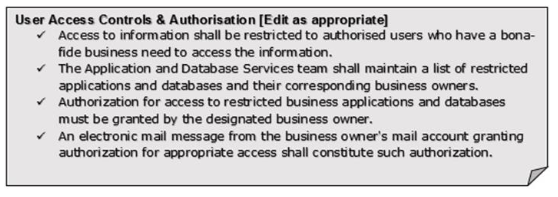
Organizations should define the targets to which the information security policy applies. It can handle all the issues of technology infrastructure, users, and third parties in a given organization, regardless of circumstances. This will help the companies identify adverse consequences with the aim of reducing risks and recovering as soon as possible if a cyber-attack or physical damage occurs in the near future.

* 1. *Information security goals*

An organization that seeks to develop an effective information security policy (ISP) must have well-defined security objectives and strategies on which management has reached an agreement (Kostadinov, 2018). Any existing disagreements in this context will make information security policy flawed. The most essential thing a security expert should note is that his understanding of security management standards will let him integrate them into the documents that he is assigned to draft, which is an assurance of completeness, consistency and workability. Information security emphasize three major objectives:

* Confidentiality: Data and information assets can only be accessed by those with authorization
* Integrity: Companies should keep data complete, accurate, and intact, and technology infrastructure must be properly functioning
* Availability: users allow access to information or system when asked
  1. *Authority and Access Control Policy*

In general, there is a hierarchical pattern in a security policy. It means that employees are not allowed to share some information if they do not have any valid authorization. In contrast, a senior executive may use his authority to determine which data can be circulated and with whom. Therefore, the reasonable demands that ISP should solve every fundamental role with criteria in the company that will justify their authoritative status (Kostadinov, 2018). In particular, each organization specifies the degree of authority about data and IT systems.

Besides the hierarchical pattern, network security policy is another factor that is worth considering. Users can only connect to association networks and servers through unique logins that requires authentication such as passwords, ID cards, biometrics and tokens. It is absolutely vital to check all systems and save login attempts (both successful ones or failures).

***Figure 2: User Access Controls and Authorization Policy***

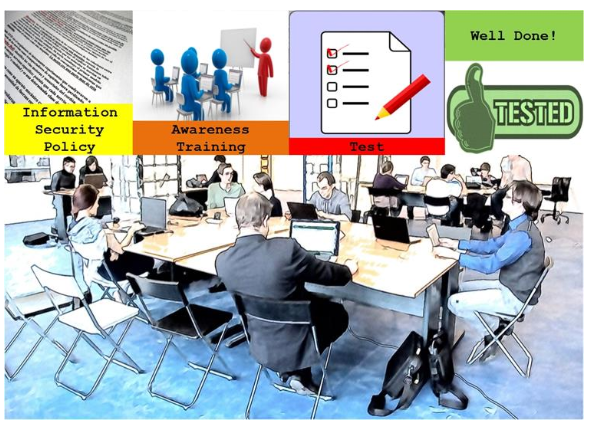
*3.5 Data classification*

Data should be categorized into three primary classes which include “High Risk Class”, “Confidential Class”, and “Public Class”. The main purpose of classifying data is to not only safeguard sensitive information but also evade unnecessary security methods for unimportant data. This helps companies protect highly critical information more effectively.

* 1. *Data support and operations*

There are three important factors in this part such as Data protection regulations. Data backup, and movement of data

* Data protection regulations – systems storing private or sensitive data must be secured in accordance with organizational standards, industry best practice and relevant regulations. In particular, the systems must operate an up-to-date anti-malware protection, a firewall and encryption.
* Data backup – data will be encrypted in line with industry best practices and hosted in an area of physical security to avoid losing data, especially sensitive data. Companies must safely store backup media including a computer center, data closet and so on or deliver backup to secure cloud storage.
* Moment of data – data should be transferred via secure protocols. Any information sent on a portable device outside the company or through a public network must be encrypted according to industry best practice and relevant regulations.
  1. *Security awareness and behavior*

Circulating IT security policies to staff is a crucial move. By regularly holding training sessions, employees can understand the definition and importance of the procedures and mechanisms in order to secure the data (data protection measures and data sensitivity issues for example). The training session should mention some vital topics on IT security such as social engineering, clean desk policy and appropriate Internet usage policy (Cassetto, 2019). At the end of the training, a small test will be given to check the understanding of IT security policies for each member in the organization.

***Figure 3: Information Security Awareness Training***

* 1. *Responsibilities, rights, and duties of personnel*

The company should assign employees to implement user access reviews, incident management and regular updates of the security policy (Cassetto, 2019). Responsibilities should be explicitly described as an important factors of the security policy.

The organization would like to employ an ISP due to prevention of stealing business know-how and confidential information. This helps the company protect its digital properties and intellectual rights.

1. **Steps to develop an effective Security Policy** 
   1. *Get leadership involved*

The role of senior executive should be noticed as one of the important parts in designing security policy because this person establishes a connection between an organizational business and its technical needs. Becky Friedman, a business writer at australianhelp.com, says: “It’s also important to keep your CEO and CIO up to date with what’s happening with your policy. Your leadership should be involved in evaluating your organization’s security needs and risks and the discussions about incident response plans,” (Bennet, 2019). This makes writing security policy more obvious to safeguard buy-in for the policy in the company and also ensure that security remains a ‘top-of-mind’ issue.

* 1. *Identify the risks*

After defining the role of leadership, the company needs to evaluate risks that can be encountered in the workplace. They may include failure to cover cybersecurity fundamentals, lack of a recovery plan and so on (Bianculli, 2017). Any one of these problems can lead to data breach, cyber-attacks or system downtime, which spends an amount of time and money to recover (Kimathi, 2020). Therefore, it must be well-understood that risk management plays an important role in the security policy (Gaw, 2003). The company should use sophisticated cybersecurity analytics and assessments in order to seek vulnerabilities that can influence an organization’s prosperity. However, this technique is not good enough to make sure that the company will avoid attacks in the future. In addition, organizations must educate and inform their staff not only about existing cyber-threats, but also about how to their own activities could violate confidential information if they do not follow established procedures.

* 1. *Choose the security level matching the risk*

The scope of security procedures should show the real threats that the company has to face. Abusing a sole cybersecurity plan can decrease the efficiencies in firm’s operations and impose unnecessary pressure on staff. Once writing an information security policy, its extent needs to meet the realistic requirements of the organization. For example, a small company startup should not own the same features of security protocols as top IT companies or a particular government agency, which may be unsuitable to the startup firm. However, it is really essential that the drafted information security policy should be explicit about procedures and implementations so as to help employees execute them correctly. Although with qualified and diligent personnel in place, companies still need a comprehensive instruction manual as the reference for behavior guidance.

* 1. *Reach consensus*

Creating an information security policy is a controversial and difficult process. To ensure the safety in the organization, some freedom and financial benefits need to be sacrificed. For instance, an internet marketing company would like to provide an internet usage policy including only access to private Wi-Fi company, prohibit the installation of software and so on to protect both the business and staff in the company. However, some personnel disagree with this policy and argue that it could lead to the unnecessary inconvenience for new employees and take much time to get familiar with these strict rules (GFI Software, 2020). Basically, the firm must create an explicit agreement between the leaders and the staff on what information security policy can achieve and whether its benefits will overweight over the drawbacks. Moreover, the purpose of consensus of all members in the organization is to guarantee organizational well-being, not for the sake of a certain group.

* 1. *Train Employees*

Even though educating staff is one of the most important factors contributing to an efficient security policy, many company ignore this measure (Bennet, 2019). It is generally speaking that humans are the weakest link in the information security chain (Huseyin, 2019). According to Code42 news, 78% of the security expert suppose the most potential threat to endpoint security is the carelessness among staff for security practices (Ltd, 2018). Without adequate training, employees may not even recognize how their behavior can jeopardize the organizational security. Particularly, employees can be easily profited by hackers or social engineers if they do not gain enough knowledge of information security policy. Training is also a good chance for staff to ask questions and pinpoint some difficulties that they feel ambiguous in the policy. This step even shows some shortcomings or inconsistencies in the ISP. After all, the educating process is a crucial stage to finalize an effective information security policy, which the organizations should not overlook this step.

1. **Case study: Information Security Policy in the University** 
   1. *Purpose*

The goal of University Information Security Policy is to guarantee that all data and information systems are totally secure. The effectiveness of the policy primarily relies on the personnel and students complying with security guidelines (University of Leicester, 2017). The University Security Policy provides criteria and recommendations on how:

* Confidential documentations must be safeguarded from unauthorized access.
* The integrity of data and information systems must be secured.
* Reasonable steps must be considered to minimize threats to the availability of information

Hanoi University has more than 15,000 students from 22 countries, and nearly 1,000 staff. There are total 20 academic departments, and the study environment is dynamic and international with high quality teaching and research. Open access to campuses at the university is an important component of academic life but is not risk-free. Therefore, designing an efficient security policy is necessary to ensure a safe environment for staff, students and visitors. The author also expects that this ISP will be suitable to the university or at least handle some fundamental issues.

*5.2 Organizational Scope*

This policy applies to all individuals processing information as part of their jobs or positions on behalf of the University (students, scholars, employees, honorary members and third parties performing a function in the University). In particular, the policy and the framework applies to:

* Anyone inside Hanoi University who gets access to University information properties or technology, which includes instructors, students and alumni.
* Processing, transferring or storing university information handled by internal and/or external devices.
* The usage of university information for the 3rd party.

*5.3 Key ISP definitions*

* Incident: an occurrence of an unexpected action or situation that can threat to individuals and property.
* Emergency: an urgent need for assistance or relief
* Security Services: include the following elements:

1. Allowed access to basic information infrastructure and facilities
2. Surveilling the physical environment
3. Providing security for a situation where there is an incident or identified risk
4. Providing a central point of communication with outside agencies for security problems

* Security Equipment: include the following elements:

1. Keys and locks
2. Closed-circuit television
3. Identification hardware and software
4. Devices for detecting thefts or intruders

*5.4 Policy Statements*

*5.4.1 Information Security Responsibilities*

A*.* The head of College or Support Group

This group includes Head of Campus Services, Heads of Faculties / Departments, Assistant Supervisors and so on. Its role is responsible for ensuring that appropriate and efficient controls on information security are in place within their position of accountability. The group of people often bear responsibility for enforcement within their management of any subsidiary entity, for example, affiliated institutes, research groups, and multidisciplinary organizations.

B. Senior Management and associated Governance committees

Senior Management within the University has administrative responsibility for information security. Its mission is to actively promote the implementation of policy, requirements and structure for Information Security as well as ensure conformity within the area of accountability. In addition, setting security strategy and monitoring risk management are important tasks that Governance committees undertake.

C. Data steward

The Data Steward is accountable for protecting the security of dataset; defining data access criteria; saving the data that makes accessible to other services; and developing processes to ensure data quality. Furthermore, the position is also responsible for guaranteeing that restricted and sensitive data is handled safely and properly, which makes data only available to those individuals that need to access. This access must ensure that those people follow the University’s internal policies.

D. Staff

Each employee must ensure that they understand, follow University Security Policy procedures and pay careful attention to the issues related to their activities. They must also comply with instructions from Security Team, especially in emergency, evacuation instances and security procedures. Staff are expected to hold their university cards at all times.

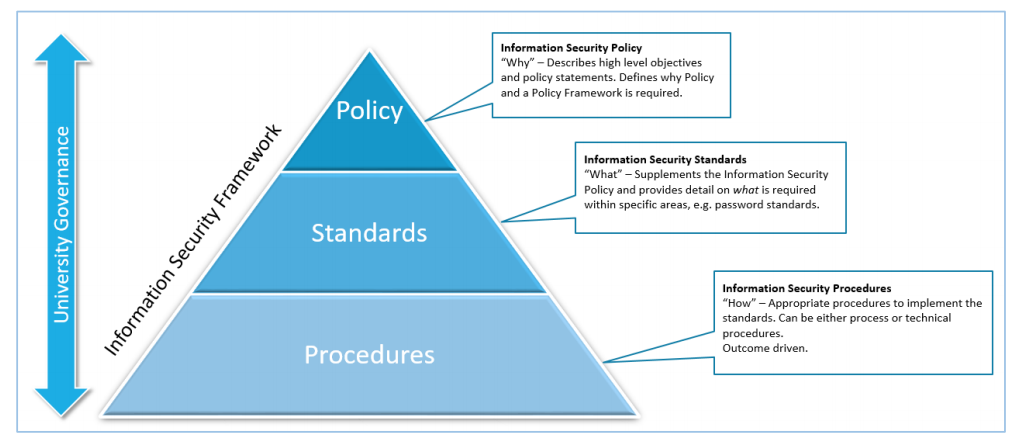
E. Students

The general duty of students is to properly notice the University's facilities and take due account of security concerns. They must obey security procedures designed in order to safeguard the university assets, especially the rules on access computer rooms or places equipped with other services. Students must also comply with instructions from Security Team, especially in emergency, evacuation instances and security procedures.

F. Visitors (including delegates from the conference and external event attendants)

Visitors is accountable for keeping track of the University services when on campus and taking considerations of security problems. Particularly, they must wear their visitors badge once entering the conference. They must also obey guidelines from the Security Team or from the host department, especially in emergency instances.

*5.4.2 Security Policy Framework*

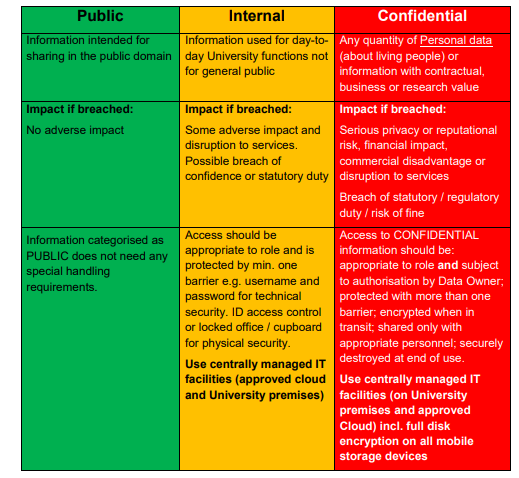
The University’s information security is shown on the following structure which comprises: (a) Policy, (b) Standard, (c) Procedures, besides University Governance. This framework is highly flexible and efficient platform for the requirements of University’s information security. The structure is described below:

***Figure 4: Information Security Framework***

All staff and students must follow associated security standards strictly. The framework is, however, versatile by providing various strategies to fulfill this policy. It not only enables local self-determination in how the purposes and results of the policy, but also permit those who ask for thorough recommendations from the Information Security Division will understand the policy through detailed instructions in the Security Procedures.

*5.4.3 Information Protection and Classification*

Protecting and classifying information means paying huge effort and resources to safeguard the most confidential and important information. The following table outlines three data classifications which lay fundamental foundations for Information Security Policy. The higher the threat of information exposure, the more shielding layers are essential to protect it.



***Figure 5: Information Protection and Classification***

Data Owner may a person who takes the role as a Principal Investigator or Head of Department / Institute. In the confidential area, Data Owner can be intensely vulnerable due to exploiting data from hackers or intruders. Accordingly, its responsibility must comply with relevant regulations and contractual criteria mentioned in the Security Policy.

*5.4.4 Training and Awareness*

The university is committed to raising awareness of the information security obligations of its staff in order to ensure that university members recognize the risks and provide the information they manage as part of their position with sufficient security. This can be implemented by means of a framework of policies, guidance, team meetings and staff mandatory e-learning. User training should be suitable for positions and business needs defined i.e. personnel and postgraduate researchers with privileged access or business areas that handle high-risk information on a regular basis that require additional and relevant training material or recorded operating procedures.

*5.4.5 Acceptable Use*

The University will hire or make reference to those who are the best security experts around the world with a view to gradually completing Information Security Policy / Acceptable Use Policy that specify the expected activities and behaviors that all University members must follow. It comprises regulations for permissible and banned use of University equipment. Anyone that does not comply with the policy and lead to the severe consequence can be strictly disciplinary.

*5.5 Related Documentation*

The design and content of University Security Policy has been referenced of five ISPs’ leading universities around the world. The section list is shown below:

* [Security Policy – University of Wellington](https://www.wgtn.ac.nz/__data/assets/pdf_file/0010/1674271/security-policy.pdf)
* [Information Security Policy – University of Leicester](https://www2.le.ac.uk/offices/ias/resources/policies/ispolicy)
* [Security Policy – The University of Sheffield](https://www.sheffield.ac.uk/polopoly_fs/1.762507!/file/SecurityPolicy2018.pdf)
* [Information Security Policy – University of Liverpool](https://www.liverpool.ac.uk/media/livacuk/computingservices/regulations/informationsecuritypolicy.pdf)
* [Information Security Policy – The University of Edinburgh](https://www.ed.ac.uk/files/atoms/files/uoe_informationsecuritypolicy_v1.0.pdf)

1. **Conclusion**

To summarize, the author would like to restate some important points in the report. In the first page, the writer gives a brief introduction of security policy. Then, the definition and importance of the policy is specifically mentioned. Next, he explains what the factors of security policy comprise. After that, some essential steps to design an effective security policy are thoroughly illustrated. Finally, the case study the author wants to specify is University Security Policy. It is undeniable that there are some shortages in the report due to short research time. The writer, however, hopes that readers can understand many interesting facts about security policy.

# **REFERENCES**

Annureet Bajwa, C. H. (2018). *Security Policy: What it is, Why and Challenges.* Cardiff: Cardiff School of Management, Cardiff Metropolitan University, CF5 2YA.

Bennet, C. (2019, March 18). *Blog: 5 Steps to creating an Effective Information Security Policy*. Retrieved from vXchnge: <https://www.vxchnge.com/blog/effective-information-security-policy>

Bianculli, L. (2017). *Cybersecurity: 10 Common IT Security Risks in the Workplace*. Retrieved from CCSInet: <https://www.ccsinet.com/blog/common-security-risks-workplace/>

Cassetto, O. (2019, May 30). *Information Security Blog: The 8 Elements of an Information Security Policy*. Retrieved from exabeam: <https://www.exabeam.com/information-security/information-security-policy/>

Corfield, S. N. (2020, April 10). *Security: Ransomware scumbags leak Boeing, Lockheed Martin, SpaceX documents after contractor refuses to pay*. Retrieved from The Register: <https://www.theregister.co.uk/2020/04/10/lockheed_martin_spacex_ransomware_leak/>

Gaw, L. (2003). *Global Information Assurance Certification Paper.* SANS Institute.

GFI Software. (2020). *Sample internet usage policy*. Retrieved from GFI Software: <https://www.gfi.com/pages/sample-internet-usage-policy>

GoldenJoe24. (2020, April 14). *Technology: Ransomware scumbags leak Boeing, Lockheed Martin, SpaceX documents after contractor refuses to pay*. Retrieved from Reddit: <https://www.reddit.com/r/technology/comments/g0tloi/ransomware_scumbags_leak_boeing_lockheed_martin/>

guruevi. (2020, April 13). *Story: Ransomware Scumbags Leak Boeing, Lockheed Martin, SpaceX Documents After Contractor Refuses To Pay*. Retrieved from Slashdot: <https://it.slashdot.org/story/20/04/13/207205/ransomware-scumbags-leak-boeing-lockheed-martin-spacex-documents-after-contractor-refuses-to-pay>

Huseyin, M. (2019, July 17). *Why humans are the weakest link in cybersecurity*. Retrieved from treasurers.org: <https://www.treasurers.org/hub/treasurer-magazine/why-humans-are-the%E2%80%93weakest-link-in-cybersecurity>

Ikeda, S. (2020, March 17). *Cyber Security - News: DoppelPaymer Ransomware Hits Major US Parts Supplier*. Retrieved from CPO Magazine : <https://www.cpomagazine.com/cyber-security/doppelpaymer-ransomware-hits-major-us-parts-supplier/>

Kimathi, S. (2020, April 13). *2020 Review: Top five outages, data breaches & cyber-attacks this quarter.* Retrieved from FINTECH FUTURES: <https://www.fintechfutures.com/2020/04/2020-review-top-five-outages-data-breaches-cyber-attacks-this-quarter/>

Kostadinov, D. (2018, February 6). *Key Elements of an Information Security Policy*. Retrieved from INFOSEC: [https://resources.infosecinstitute.com/key-elements-information-security-policy/#gref](https://resources.infosecinstitute.com/key-elements-information-security-policy/%23gref)

Ltd, K. T. (2018, February 11). *Humans are the weakest link in the information security chain*. Retrieved from Medium.com: <https://medium.com/@kratikal/humans-are-the-weakest-links-in-cyber-security-of-any-organisation-ac04c6e6e71>

Ng, C. (2020, March 29). *How to Create a Good Security Policy*. Retrieved from Varonis: <https://www.varonis.com/blog/how-to-create-a-good-security-policy/>

techopedia. (2017, January 12). *Security Policy*. Retrieved from techopedia: <https://www.techopedia.com/definition/4099/security-policy>

University of Leicester. (2017, December 19). *Information Security Policy*. Retrieved from University of Leicester: <https://www2.le.ac.uk/offices/ias/resources/policies/ispolicy>