Classification and Restriction of Information in Company X

Riku Karikoski

2020 Laurea

Laurea University of Applied Sciences

Classification and Restriction of Information in Company X

Riku Karikoski

Security Management

Thesis

May, 2020

Laurea University of Applied Sciences **Abstract**
Security Management
Bachelor's Degree

Riku Karikoski

Classification and Restriction of Information in Company X

Year 2020 Number of pages 30

Information security is an important part of individuals and businesses on an everyday basis. Information itself can be physical, electronic or even immaterial as an individual's knowledge. For companies it is crucial of making sure that the information and knowledge that is shared within the company stays within the company and that is where information classification and restriction plays a part. The background for the making of this thesis was the need for the case company (titled Company X) to have a unified, written document policy for information classification and availability restriction. Information classification refers to who gets to view and what information, whereas availability restriction refers to what information can be given out and under what circumstances. The main goal was to create general suggestions for creating such a policy, rather than to create the policy itself. For this purpose, two research questions were made: how the policy should be like and what is the current status of the policy within the company.

The research methods selected were an interview with the CSO/Vice President of the company and a questionnaire directed at the employees of the company. The results provided many key points to focus on with the development of the policy, such as defining the life cycle of information within the company, combining all existing policy guidelines under one document as well as to make the policy easy to comprehend and find when needed. During the questionnaire it also became apparent that the general knowledge of the policy within the company was rather poor.

Several conclusions were made and turned into suggestions to improve the policy. The policy follows the Katakri criteria and to create a new document for the policy it was suggested that all current information would be reviewed and possibly updated. Another theme was the need to create a system to track the copying of information within the company. The other themes that were suggested for development was to improve the knowledge of the company employees on the policy as well as include proper definitions and a quick referencing section to the document.

Keywords: information, security, classification, restriction

Contents

1 Introduction 6
1.1 Purpose and Goals 6
1.2 Case Company 7
1.3 Definition of a Policy 7
2 Thesis Framework 7
2.1 Information Security 9
2.2 Risks, Threats and Protection of Information Security 10
2.3 Information Security Policy 11
2.4 Information Classification 11
2.5 Restricting the Availability of Information 12
2.6 Katakri 12
3 Methodology 13
3.1 Introduction of Methodologies 14
3.2 Interview 14
3.3 Questionnaire 15
4 Results 15
4.1 Interview 15
4.2 Questionnaire 16
5 Conclusions 23
5.1 Interview 23
5.2 Questionnaire 24
5.3 Approach to the Development Process 24
5.4 Additional Suggestions to Policy Creation 25
Figures 28
Tables ..... **Error! Bookmark not defined.**
Appendices 29

1 Introduction

Information comes in many forms and different values. It can be in physical, electronic or knowledge of an individual person. The value of information is different between individuals and bigger companies. Personal data is a much-discussed topic and brings value to the individual, while companies put value on their own data, such as trade secrets. Companies should make sure that the information and knowledge that is shared stays within the company. This is what information classification and restriction aims of protect.

This thesis focuses on these two aspects. It will tell about the case company (referred to as Company X for anonymity) and the second chapter covers fundamentals of information security to give a basic understanding of the topic. A definition for the two main themes of the thesis is given.

In the third chapter methodology for the thesis is explained. Research is based on two methods: an interview and a questionnaire that will answer two research questions. The aim is to develop guidelines to create a policy for information classification and restriction of availability. The scope and scale of the development becomes apparent in this chapter. Chapter four will go over the results of the research, revealing main themes to focus on.

The final chapter focuses on conclusions of the study and introduces improvement options for developing the policy.

1.1 Purpose and Goals

The purpose of this thesis is to create suggestions for improvement to the policy regarding information classification and restriction within the case company. Reasoning for this is the need for a unified document to include all the information regarding data/information classification and restriction of availability. The final product of this thesis is not aimed to be a final version of the policy document. The purpose is to be a guideline to further develop the policy within the case company.

To reach the goal, methods selected for the research were a questionnaire aimed at the employees of the company as and an interview with the Chief Security Officer (CSO)/Vice President of the case company. With these methods the purpose is to find areas for development. This should help to create a basis for improvement on which the new policy could be build up on. Once a framework for improvement ideas and suggestions are created, they are then handed over to the case company for review and commenting.

1.2 Case Company

The case company for this thesis is a large government-owned corporation that operates in several locations throughout Finland, employing over 1000 people in operational and managerial fields. The company is managed by the general meeting, board of directors and CEO. The turnover of the company was 377 million euros in 2018. For confidentiality purposes, the case company will be referred to as "Company X" in this thesis.

A government-owned corporation (or state-owned enterprise) is created by a government to take part in commercial activity in different areas or fields for profit (Kenton, 2019). The company can be fully owned (for example Valtion Rautatiet yhtymä Oy in Finland) or partially owned (Finnair Oyj in Finland). In partially owned companies, the government takes part with decisions made in the company with a vote within the board of directors. The basic business principles are the same between a private and government-owned corporation. As the name implies, the government owns a part of the company in the latter and thus has a right to vote within the board of directors. The control of the vote is conducted by a separate ministry; however, the ministry primarily answers to the parliament which is the highest entity. State Shareholdings and Ownership Steering Act (1368/2007) is the legislation that defines these actions.

1.3 Definition of a Policy

A policy is a set of ideas or a plan within companies meant to give guidelines to different situations (Cambridge Dictionary). It can be a guideline for a big or small concept that has an impact towards the company culture. A policy on corporate social responsibility has a bigger impact that explains how a company deals for example with sustainable development (Schooley 2019). A company policy on no smoking at workplace is a minor policy that promotes a healthier work culture. The purposes of a policy are to assure that everyone within the company works with the same ruleset regardless of topic or field. The policy that this thesis aims to improve is the policy regarding Company X's information classification and restriction of availability.

2 Thesis Framework

"One problem with data and information assets is that they are not easily quantifiable when compared to traditional goods." (Borek, Parlikad, Webb and Woodall 2014, 8)

Information could be considered to have no implicit value: it depends on the use, purpose and context. In relation to information security and classification, companies set the value on the information they are classifying. The value would consist of how much monetary damage losing that information could cause to the company, for example trade secrets. "When data and information are important for the success of an organization, data and information become

assets for the organization" (Borek et al 2014, 6). Confidential information is generally valued higher than public information, as it holds data deemed vital to the success of the company or its reputation (trade secrets, client data etc.). Companies are trusted with protecting any possible data that has resulted from coalitions with other companies or client information data. This type of information has high value, even if not for direct financial losses, but for the reputation of companies. Losing sensitive data that regards other parties causes a dent in company reputation that can then result in losses financially.

Borek et al refer to a comparison of is data being the new oil, originally expressed by Clive Humbyat at the ANA Senior Marketer's Summit 2006 and Michael Palmer's blog post, brought up in an article for Forbes.com by Perry Rotella in 2012. Palmer wrote that "Data is just like crude. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc., to create a valuable entity that drives profitable activity; so must data be broken down, analyzed for it to have value" (Borek et al 2014, 5). Jer Thorp wrote a response in an article blog for Harvard Business Review, calling information "the ultimate renewable resource" and that data is created in vast quantities every day, instead of it being "lying in wait beneath the surface". He also wrote that "finding value from data is much more a process of cultivation than it is one of extraction or refinement" (Borek et al 2014, 5).

Data Type	Description
Master data	Master data is key business information about customers, suppliers, products, etc., and remains relatively static.
Transactional data	Transactional data describes events happening at a particular time and refers usually to one or more master or reference data elements. This data type is very volatile.
Historical data	Historical data is data about past transactions that often need to be retained for compliance purposes. Historical data may be saved in an obsolete format or in computer (legacy) systems, which can make them difficult to access and process in an organization. Historical data will also include master and transactional data.
Temporary data	When applications require additional memory in addition to the virtual memory available, temporary data is saved.
Reference data	Reference data is classification schemas and sets of values (e.g., country codes) provided by bodies external to the organization. It may also include internal classification schema and sets of values.
Business metadata	Business metadata is characterized by a lot of free text information describing business terms, key performance indicators (KPIs), etc. It can also contain business rules.
Technical metadata	This is structured data that describes objects such as tables, attributes, etc.; the database structure and technical rules are defined in this data type.
Operational metadata	Operational metadata describes operational characteristics happening in IT systems, such as the number of rows inserted by other software applications.

Figure 1 Data Types (Borek et al 2014, 7)

2.1 Information Security

Information security and cybersecurity are two concepts that are often mistaken to mean the same thing (Computer Science Degree Hub, Cisco.com). While similar, cybersecurity focuses on the digital world (computers, networks, internet) and information security is about both digital and analogue information, regardless of where it is saved. The terms data and information are different, with information being referred to as processed data. This means that data itself is raw facts which becomes information when it is processed (Borek et al 2014).

When it comes to security that is related to information, it should not be considered in a traditional way. Information as an asset can be considered limited on how it can be protected physically (such as physical security for servers). This creates different challenges compared to physical security of personnel or premises. Physical information and non-material information, such as human knowledge should be considered in the general definition of what information security focuses on. Information security aims to protect the following:

- Confidentiality – providing access to only those with validity and authorisation
- Integrity – to ensure that information is not tampered with or deleted
- Availability – ensuring that the information is available when needed

Confidentiality, integrity and availability are referred to as the CIA triad (Perrin 2008). The reason to keep information security infrastructure up to date is emphasized by how much companies rely their business on data and information they have. It can take one mistake for a company to end up in turmoil, for example with sensitive data exposure such as client data, trade secrets or in the worst-case scenario vital security and safety information (Layzell 2018). The primary focus of information security is to protect the CIA triad, but it also aims to maintain organisational productivity. The risk management process that information security is achieved via consists of identifying assets, their vulnerabilities, threats and how impactful they are. After evaluating these risks, decisions are made on if a threat should be avoided, mitigated, shared or accepted. Based on these decisions, security controls are implemented and then monitored for possible improvements. (Tunggal 2012)

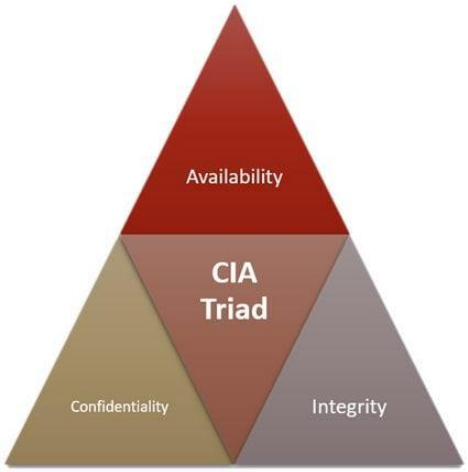

Figure 2 The CIA Triad (Infosecinstitute.com)

2.2 Risks, Threats and Protection of Information Security

Information Security faces several different threats and analysis of all these threats is important (Search Inform 2019). Different threats could be intentional, accidental, or caused by natural disasters. Intentional threats generally are malevolent in nature, such as sabotage or vandalism. Someone who wants to harm a company in any way for any reason could be considered the be a threat of malevolent intent. Malevolent threats could include viruses, phishing attempts, attempted disruptions or even copying sensitive information. Threats caused by human error are generally the opposite and are unintentional. Human error factors in threats such as mistakes or accidents due to for example lack of policy guidelines for handling sensitive information. There can also be failures in software or hardware. Natural disasters (earthquake, flood etc.) could also cause harm to a company by damaging servers for example (Whitman 2003). These are some of the main risks and threats that information security faces. Michael E. Whitman (2003) reported a study to identify and rank different threats. According to the study the top three threats were deliberate software attacks, technical software failures or errors and act of human error or failure.

Information protection happens in different ways and is aimed at preventing damage, copying, distortion or blocking access to information (Search Inform 2019). Layered defence is the best way to protect data and information, but it should also be remembered that risks are always present (Alexander 2008). The information and knowledge that company employees have are usually secured with classification policies with the aim to limit the possibilities of information leaks. This is enforced with policies, guidelines and non-disclosure agreements given to the employees to prevent them from giving the information to people without authorisation or to outside parties. As a part of information security, risk management identifies risks to their security processes, creating guidelines to mitigate or avoid the effectiveness of risks to the company's infrastructure. Encryption, authentication, information backup and

safeguarding physical targets (servers, computers) that withhold information are all tools of information security to enforce the CIA triad to prevent data and information loss. Some other vulnerabilities that information security could face are failures in software or hardware, lack of guidelines and protocols in information exchange and inadequate operational processes. (Andress 2014)

2.3 Information Security Policy

The basic need for any security policy is simple: it protects the organisation (Greene 2014). They aim to maintain a set of principles and instructions which enforce a better security culture. If followed correctly, policies prevent and mitigate security threats within the working environment. Regarding information security, a good policy is a plan that defines critical assets of the company, how they must be handled and how to operate within the organisation's secured systems. An aspect of this is how to respond to possible incidents or threats. An information security policy explains staff's responsibility within an organisation. (Danchev 2003)

Policies could be considered the law of an organisation and are mandatory (Wood 2005). While every policy is individual to each company, they are often created to comply with a specific standard. A standard is essentially a framework that can be used to create a policy. Standards cover things such as implementation, system and software specifications. International Organization for Standardization (ISO) is a standard series meant to help organisations with creating policies and its frameworks are used universally. The ISO27000 series of standards is the leading standard specific to handling information security policies (Kosutic 2014).

2.4 Information Classification

The simplest explanation for information classification would be the "need-to-know-basis". This means that information within a company is distributed by who needs specific information. For example, a security infrastructure maintenance employee would need to know specific information of the physical infrastructure to understand it and to be able to repair detected faults, while a software engineer does not need the same level of information. The highest knowledge should always be with the leadership and management of a company as the asset owner (in this case the company) is always responsible for the classification (Kosutic 2014). Information is classified with different levels. Levels of classification according to Katakri (based on internationally used classification levels):

- Secret
- Confidential
- Restricted

Depending on the size and field of the company, more levels of classification may be used or needed (Kosutic 2014). The idea with classifying information is to limit the possibilities of sensitive data ending up in the wrong hands. “Having established that companies should classify their data, it is important to understand what an effective information classification system should accomplish. That is to categorize information so as to communicate company-endorsed safeguards for information confidentiality, integrity and availability. An effective data classification system should also be easy to understand, use and maintain” (Fowler, 2003, p. 4).

2.5 Restricting the Availability of Information

What information restriction in this context refers to is the process in which sensitive information is given to a third party under specific circumstances, for example a collaboration with a third party that would benefit the company in some way. When the information is given, some sort of actions is required to make sure the information stays with the authorised people and not end up any to anyone else than who it is meant for. In general, these situations are handled with non-disclosure agreements (Alexander 2008).

When information is given out, there should usually be someone responsible for the information on behalf of the company. Generally, the person who is involved in the process is the one responsible.

2.6 Katakri

Katakri is the information security auditing tool for authorities and it was first produced in 2009, with the latest updated version being from 2015. It was created as a collaboration between different authorities with the Ministry of Defence in the lead. It is used to assess an organisations ability to protect classified information, however it does not set mandatory requirements. Instead, based on national legislation (most importantly Government Degree on Information Security in Central Government (681/2020)) and international security obligations such as Council Decision on the Security Rules of protecting EU Classified Information (2013/488/EU) it provides basic principles and minimum requirements for protecting EU Classified Information (EUCI). Katakri combines the minimum requirements for information security. The requirements are divided into three subdivisions:

- Security Management: ensuring that security management abilities and skills are at a proper level
- Physical Security: for the description of physical environment of classified information
- Information Assurance: requirements of the IT environment.

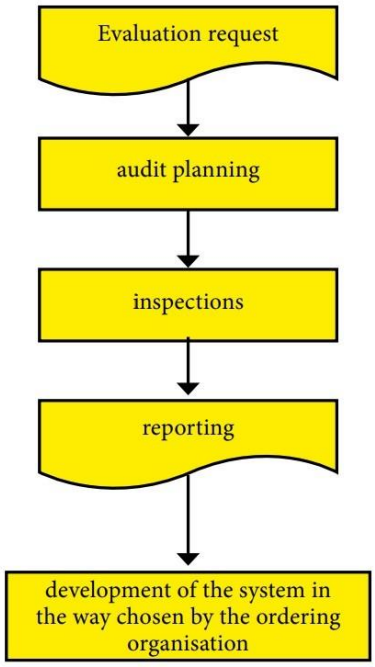

Figure 3 The Katakri evaluation process (Katakri 2015, 70)

Katakri as an audit tool can be used to assess for a Facility Security Clearance (FSC), the implementation of security arrangements and authorities' information assurance. Additionally, security measures can be supported and developed with the help of Katakri. The general ability to protect classified information is what Katakri is used to assess.

The requirements that Katakri describes, laid down by the Council's Security Rules, are based on the fundamentals collectively approved by the EU member states and thus provides a good basis for classified information protection for companies, authorities and organisations in Finland. (Katakri 2015)

3 Methodology

Aim of the research is to create suggestions for developing the case company's information classification policy. To reach this goal, two research questions were made to gather information:

- How should the policy on information classification be like within the case company?
- What is the current state of the policy within the case company?

The methods used to gather information for these questions were an interview and a questionnaire. The interview was done with the CSO/Vice President of the company, focusing on the first research question with figuring out what needs to be done to the policy, what is the

goal of the development and what is the policy based on. The questionnaire was aimed for the second question and done with responses from the employees of the company. This was to determine the general knowledge of the policy. The methods were selected for this thesis as they were considered helpful in recovering information needed to reach the goal of the thesis. The interview was easy to conduct as the CSO/Vice President was interested in the topic's development and the questionnaire would support the end goal with a point of view from the employee perspective.

3.1 Introduction of Methodologies

An interview as a research method is conducted with a small number of respondents at a time to figure out their ideas and opinions for a specific topic (Dudovskiy). The advantage of an interview is the possibility to collect more detailed information towards a topic and is usually considered a qualitative research method. Disadvantages of an interview are related to time requirements as well as arrangement difficulties with the different parties. Interview was selected as a method for this thesis in order to better understand different aspects (what it is based on, how is it handled currently) of the policy and its improvement (what needs to be done). With an interview this information can be attained in an efficient manner as the interviewee has the right information regarding the policy.

A questionnaire is a method where usually a form is sent out to recipients with several questions, to which they then reply (Dudovskiy). The answer options given can be multiple choice or open-ended. The advantage of a questionnaire is the speed of which information can be gathered from several recipients at once. Disadvantage however can be the recipient's misunderstanding of a question/questions or lack of interest to answer properly. A questionnaire can be considered both qualitative and quantitative, depending on the type of the questionnaire (open-ended vs. multiple choice, for example). The questionnaire was selected as a method for this thesis to easily gather a larger amount of data from the employees. This helps to create a better idea of what the employees think about the policy and to find solutions on how to develop the general knowledge of the policy within the company. The questionnaire was an easy way to gather enough information with a shorter schedule.

3.2 Interview

Initially questions were made to support getting answers to the first research question. As it was already agreed that the interview will be conducted with the CSO/Vice President of the company, the source of valid information was secured. The main themes for the interview were:

- What is the policy based on?
- How is it put into practice within the company?

- Levels of classification?
- Desire for development?
- What is the end goal?

Discussion based on these questions revealed some information that these questions did not necessarily intend to find, which further increased the usefulness of the information for the development process of the policy.

3.3 Questionnaire

To find out what the current situation of the policy within the company is, a questionnaire was conducted. The main point of the questionnaire was to figure out how well the employees know the policy, if they know where to find it, the main features as well as if they know the need and meaning of the policy in regard of information security. Questions about the company's employee's own ideas of improvement were also featured.

The questionnaire was created as a simple form in google docs with a total of 13 questions consisting of yes and no type of questions, few multiple-choice questions and a few open questions. After the basic questionnaire was finished it was sent into the corporate security unit of the case company for review and ideas for improvement. This took about a week after which some small changes were made to the questionnaire, mainly to clear up some terminology as well as add a few questions. After the "test" of the questionnaire, it was decided with the CSO/Vice President of the company that the questionnaire would be aimed towards team leaders and other personnel in a supervisory position to a total of 50 recipients out of which only 19 answered. The time to answer the questionnaire was only two weeks due to overall scheduling difficulties both before and after the conduct of the questionnaire. The questionnaire is considered qualitative in this thesis.

4 Results

In this chapter the results from the interview and questionnaire are presented. The findings of the research are then used as a base for conclusions, which are explained later in chapter 5 of the thesis.

4.1 Interview

The main point of the interview was to set a goal of what the policy should be like and when doing the interview, the CSO/Vice President of the case company gave direct and clear answers on the biggest points of improvement. One thing that was discussed was the lack of a unified policy document as currently the policy is split into separate smaller sections within other policies. To have all the information of the policy in one place would be an essential

part of spreading the knowledge of the contents as well as improving the policy in general. During the interview it became apparent that the policy is based on the KATAKRI standard. The main theme regarding development of the policy turned out to be the lack of a description for information's life cycle. This means that when a document is made within the company, it gets classified and archived and later there might be a need to give the said information out to a third party. In the policy there are clear instructions of how the information can be given out and what processes it includes (non-disclosure agreements, for example), but there is a lack of proper instructions, for example in retaining the material that has been given out. Another theme related to this was the lack of a tracking system for what information has been copied, by who, when and for what reason. It is apparent how important a system would be regarding the overall security culture of the company.

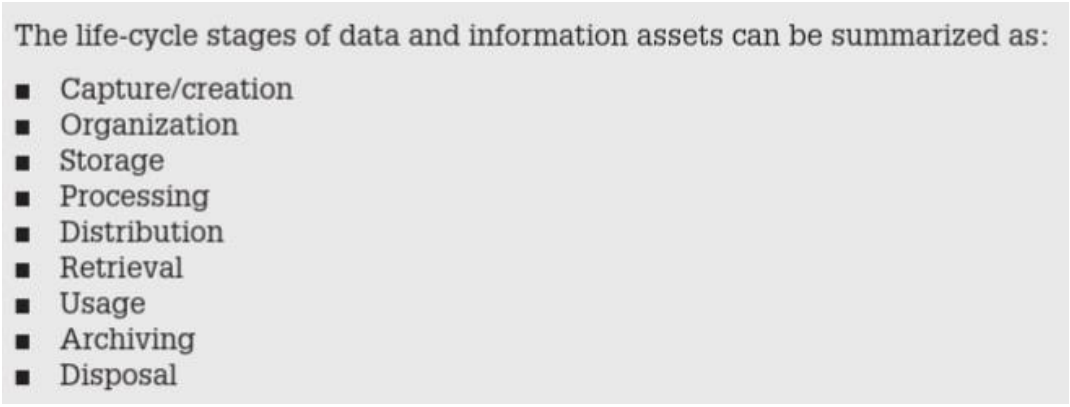

Figure 4 An example of an information life cycle (Borek, Parlikad, Webb and Woodall 2014)

4.2 Questionnaire

The questionnaire received 19 replies and to analyse them, an analytical framework was done in excel format. The framework consisted of six brackets:

- The questions in order
- Green, yellow and red colour-coded brackets out of which one was marked with an X to represent the need for attention for each question's topic
- General comments for analysing each question and the replies given to them
- Themes that were found in the replies for each individual question

Additionally, a separate bracket below the framework itself held the complete conclusion of the analysis. Some questions received replies that were evenly split to two answers, even if there were multiple choices, while some other questions received a bigger sparsity.

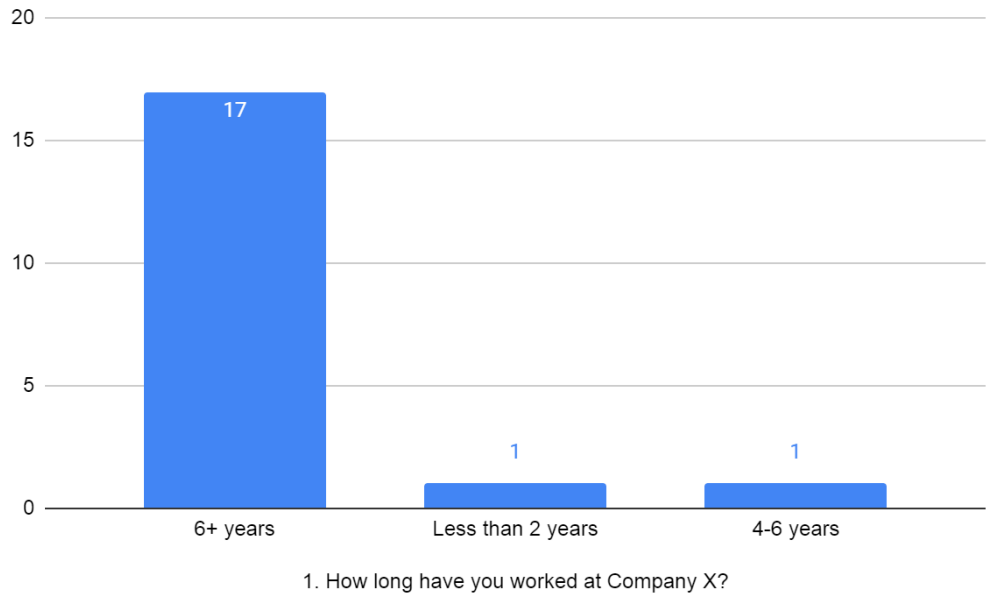

Figure 5 Replies to question 1 of the questionnaire

Most of the replies came from people who had worked in the company for six years or longer, only two had worked for less (one less than two years and the other between four to six years). This leads to the assumption that the overall experience for example the use of the company's internal systems (intranet, communications etc.) is in a good state. This means that overall people should know where to find the things they need for their everyday work routines.

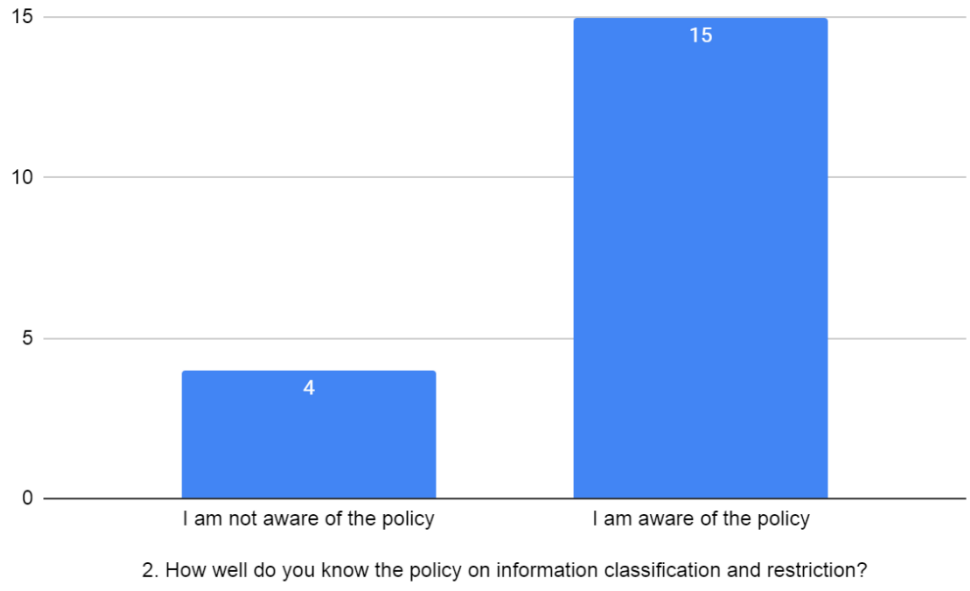

Figure 6 Replies to question 2 of the questionnaire

When asking the recipients about their current knowledge of the policy on information classification and restriction, the knowledge of the policy existing was present. Four recipients were not at all aware of the policy. None of the recipients were fully aware of the policy.

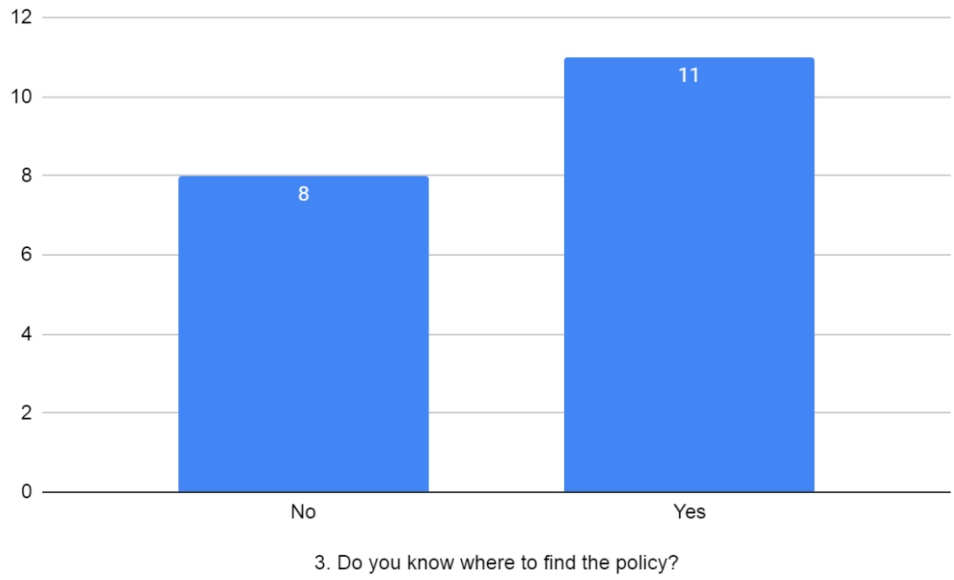

Figure 7 Replies to question 3 of the questionnaire

On the third question the answers were split, with about half of the recipients not knowing where to find the policy at all.

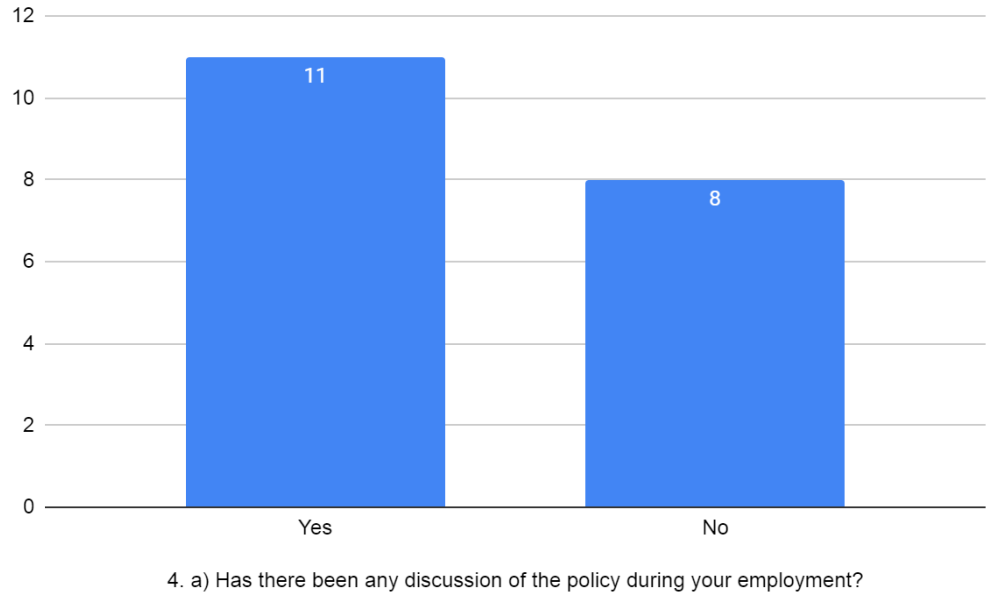

Figure 8 Replies to question 4 a) of the questionnaire

Fourth question was about discussing the policy within the company and like the previous question, the same amount of people had never even discussed the policy during their employment. When looking at the individual responses, the connection between the answers to this question and the previous one was apparent with the same people answering “no”.

Next question was a follow-up question to the previous one regarding when the policy should be discussed, and it was the first question with open-ended answers. With this question the first themes also surfaced:

- Discussion should happen at the beginning of employment
- Regular reminders to keep up to date with the policy

One response was that the policy should be discussed with proper time, while another one thought that it should be just a small part of a normal meeting and not something that takes too much time.

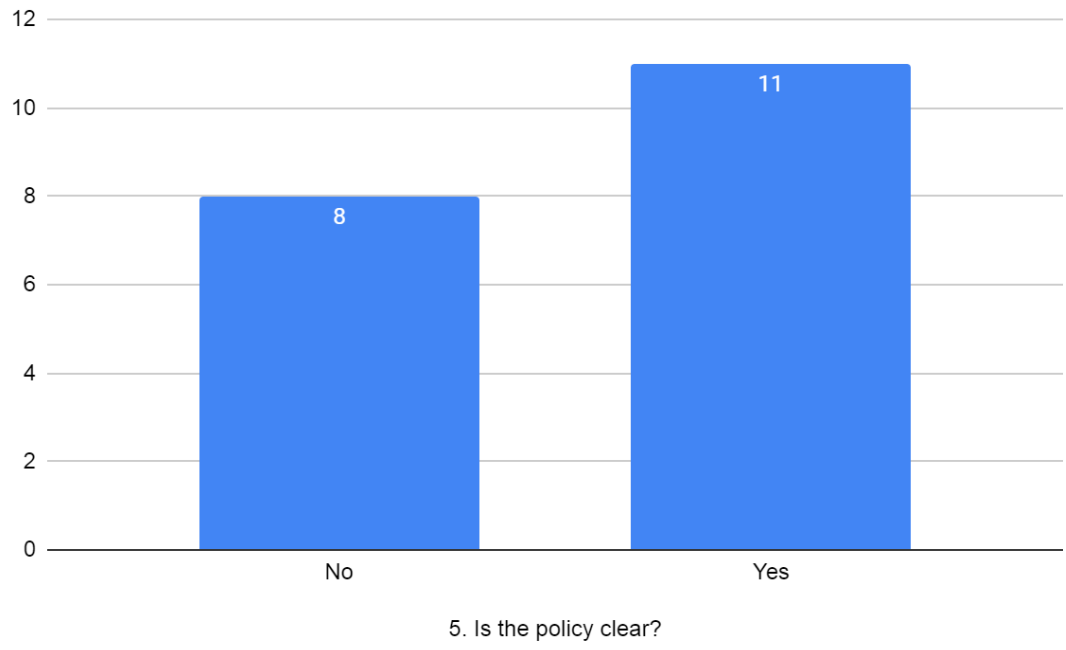

Figure 9 Replies to question 5 of the questionnaire

Clarity on the policy did not seem to be on a great level. Half of the recipients felt that the policy is not clear enough. Considering the amount of replies about the general knowledge of the policy it is not surprising that the recipients felt it to be unclear.

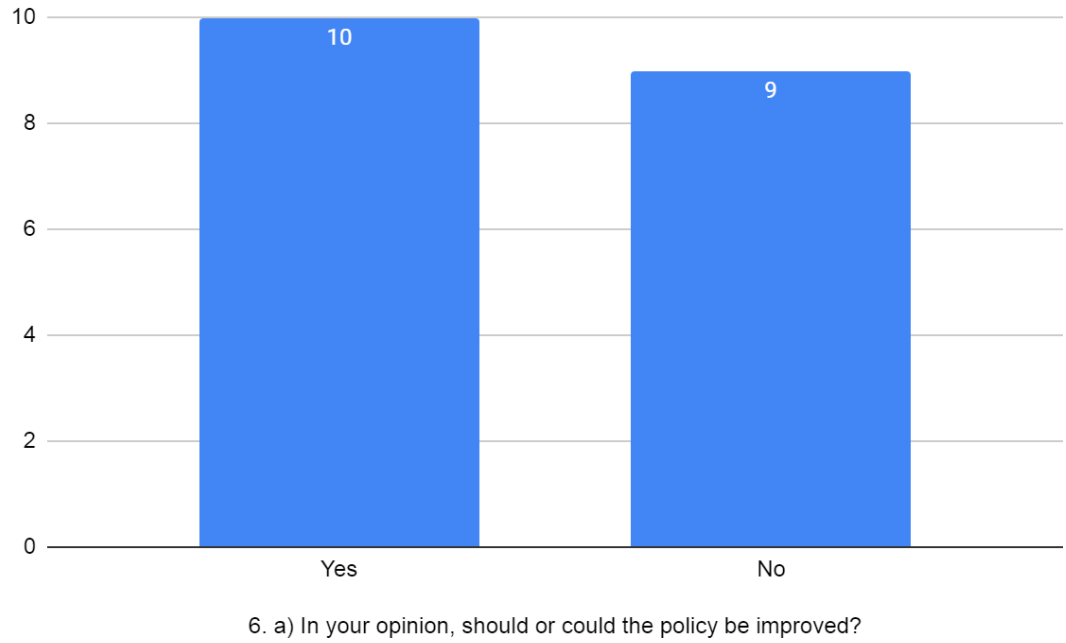

Figure 10 Replies to question 6 a) of the questionnaire

When asking if the policy could or should be improved, the same trend continued. The half that felt the policy could or should be improved had some similarities with answers to the previous questions. On the other hand, this meant that since the respondents who do not even necessarily know where to find the policy (or have no knowledge of it) will feel that an improvement is needed. People who did have knowledge of the policy felt that improvements are needed. The follow up question as to how the recipients would improve the policy revealed three themes:

- Easy to find and access
- Easy to comprehend
- Would include some sort of examples of how the policy works in practice

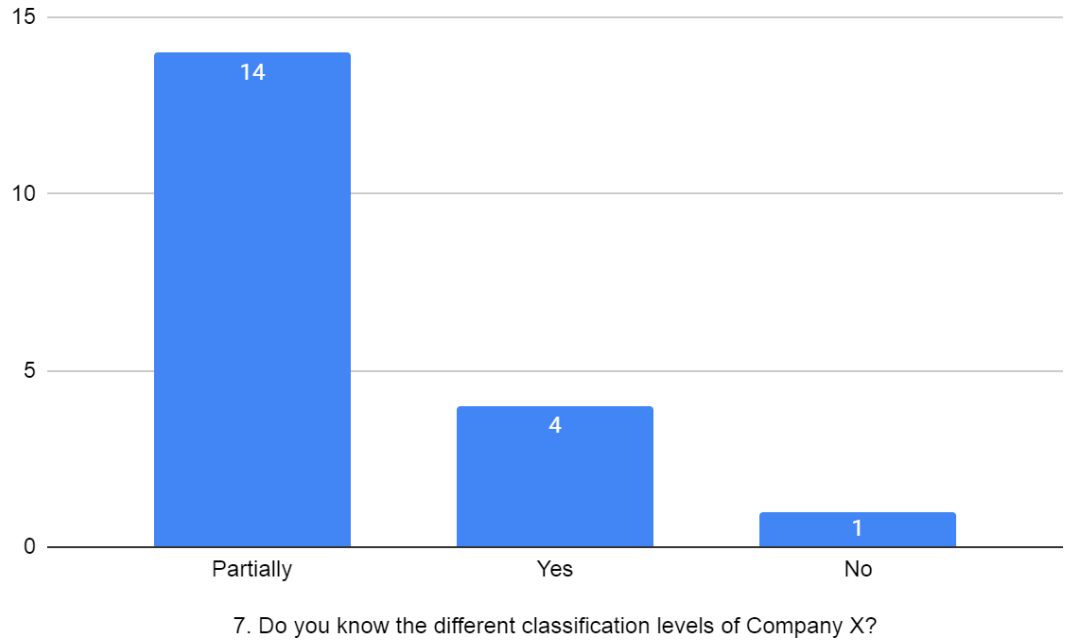

Figure 11 Replies to question 7 of the questionnaire

When asking about the general knowledge of the classification levels, most people only partly knew them. With this question the main theme is centred around if everyone needs to know the different levels especially if they do not need it regarding their own work. It could potentially be so that the focus could be more on making sure that everyone knows where to find this information rather than everyone needing to know the levels of classification.

Related to the previous question, the theme is again related to if everyone needs to know the different levels and would it be better to just focus on making sure everyone knows where to find the information.

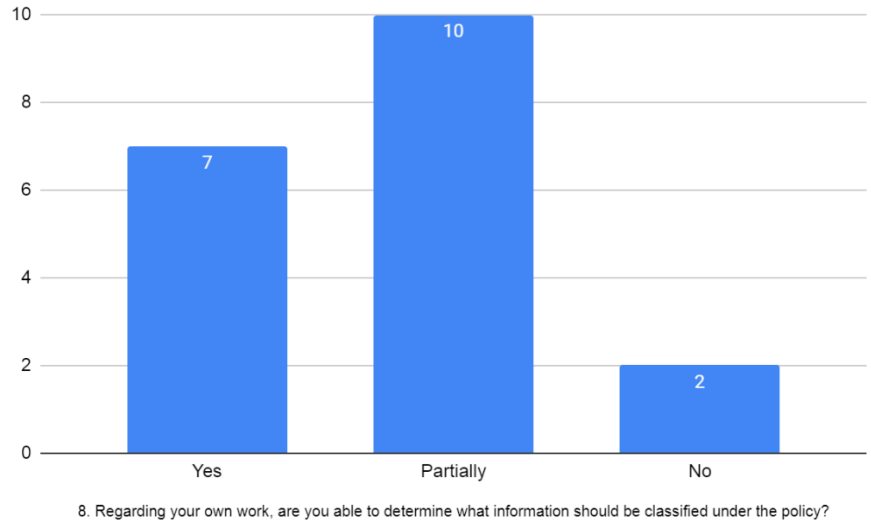

Figure 12 Replies to question 8 of the questionnaire

Question 8 relates to an individual's ability to determine what should fall into the classified information categories regarding their own work (creating or handling classified information mainly). With this question again it needs to be taken into consideration who requires this information. For example, someone who is often working on creating and updating documents should be much more aware of this compared to someone who would possibly just read the information or otherwise handle it.

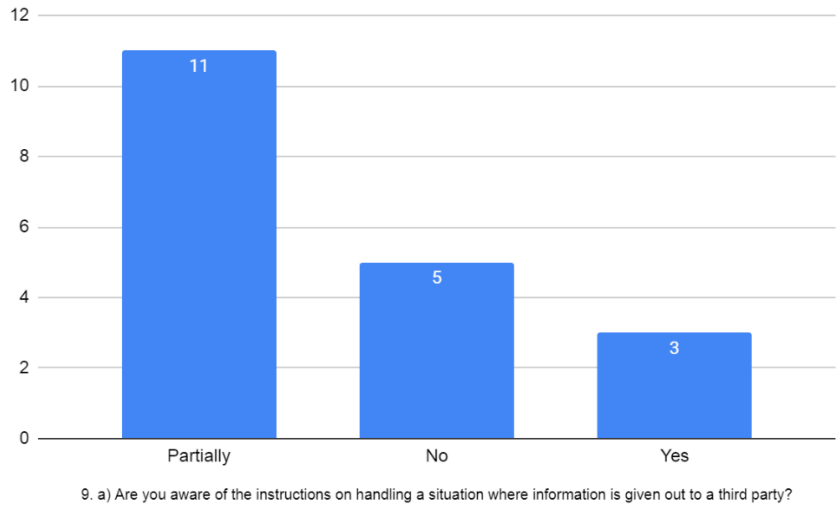

Figure 13 Replies to question 9 a) of the questionnaire

When it comes down to the general knowledge of the policy's instructions regarding handing out classified information, it seems to be on a good ground. However, with this question as well it needs to be considered who needs to know the instructions regarding their own work

and who does not. Once again, it would be more important to emphasize where to find the information.

Follow-up question was if the respondents did not feel the need for any improvement on policy, why would it be so. The question received similar responses as the question earlier on. A minor theme about opening the meanings behind the different classification levels would be appreciated. This means explaining what kind of authority is eligible for each classification, what would be the reasoning for each level of classification etc.

Last question was directly relating to the knowledge of information security within the company. The answers to this question were mostly well-based. The main points with the responses were possible security breaches that could potentially lead to financial losses as well as the loss of confidential information or important infrastructural security information.

5 Conclusions

These suggestions are based on the results of the interview, the questionnaire and the overall culture of Company X of having policies in general written out in document form. However, the structure should follow the Katakri criteria. Katakri as a tool is meant to be used as a whole, not only specific subdivisions.

First thing to keep in mind should be the scope of the policy. As the policy instructions already exist in some form (as parts of other documents/policies), the basis on where to start would be to gather all current information. Then it should be evaluated to determine the importance and accuracy of each section. If some information would be outdated for example, it should be updated before being added to the new document to make sure it still fits the Katakri requirements.

5.1 Interview

During the interview, it became apparent that the biggest target of improvement is as the original reason for this development project was, the lack of one unified document. While Katakri only sets requirements on practices, major policies such as this should have their own dedicated document as mentioned in subdivision T, section 04 it is mentioned that “the organisation documents the most important parts of monitoring and security measures” (Katakri 2015, 8). With all the information of the topic for ease of accessibility for the employees, it would promote a security culture where all information practices, procedures and overall guidelines are explained in a document. But as the lack of a unified policy document was quite apparent from the beginning, these conclusions will focus on what should the policy include and in what scope. As previously already mentioned, the other point of development based on the interview is a full instruction (or description) of the life cycle of information. The emphasis should be on the handling and retaining of information that is handed out in a

physical form. While not directly implying a procedure for retaining physical information given out, it is mentioned that “information of copies is marked on a diary or registers or is listed in some other respective manner” (Katakri 2015, 56). This backs up the fact that a system should be considered to keep track of where copies of information have been used. Compared to all the other development objects and what was understood during the interview, this is something that is mentioned in Katakri and should gain some attention to development. It needs to be mentioned that when it comes down to creating a system to track the copies of different information, there will be no suggestions on how it should be created. That falls out of the scope of this thesis and will only be mentioned as something that should be done. The technicalities of the system are up for Company X to create.

5.2 Questionnaire

Most of the answers to the questionnaire were quite evenly split, with about half of the people not having much information about the policy. When looking at the individual responses, the answers that had no or little knowledge to the questions about the different areas of the policy were consistently the same respondents. The main things to improve the policy should be a focus on the accessibility and making sure that everyone is at least aware of it. Many of the answers claimed never to have discussed the policy. Especially at the beginning of an employment, this topic could be discussed. When there is discussion of the policy, it would be recommended to go through the guidelines more in depth with people who will have to know the policy regarding their own work. People who do not necessarily need to know all the information within the policy should at least be informed of where to find the policy. Having the policy be easy to read and consistent with possible practical examples would be good to include. Taking into consideration that the company's classification has only four levels, this information could be known by every employee (even if a specific employee would not necessarily need to know them regarding their work) just to promote the security environment of the company. It also needs to be mentioned that 17 out of 19 respondents had worked within the company for more than 6 years. When most people with a good amount of experience are still not familiar with the policy it further increases the need on having employees know of the existence of the policy.

5.3 Approach to the Development Process

The approach to the development process could start with the main issues that the current policy has and what needs to be transferred into the new policy documentation. A good point to start would be a clear setup for the contents that the policy should include. After that, expand further ideas from there. Based on the responses from the questionnaire as well as the interview the main points to address would be:

- Creating a clear document that will include all the steps needed for possible third-party interaction, with instructions on how to deal with material that is given out before, during and after third-party interaction (as described in Katakri)

- Listing of the different classification levels and explaining the need and differences between them (as described in Katakri)

- Making sure the policy is easy to find and access and making sure knowledge of the policy is on a good level to support the security culture of the company

- Making sure that the policy is discussed in at least a few stages at the beginning of employment with frequent reminders later especially when updates on the policy are possibly made

5.4 Additional Suggestions to Policy Creation

When it comes to the overall contents of the document, besides having all the information written out and detailed, it could also have a few additional sections. Based on the replies to the questionnaire, a quick reference section as well as a practical example section could be included. However, these should only be minor parts in the overall document but could be of importance for security culture promotion within the company. Main information of the policy being available for a quick reference would make it easier for employees who do not continuously need to work on information documents to keep track of the overall policy.

Keeping people up to date with the policy could be enforced. The policy could be discussed at the start of employment and properly shown and explained to the new employee. After the initial discussion frequent reminders to check the policy (especially if updates have happened) could be done, for example in team meetings. Overall knowledge of the policy could be considered more important than everyone knowing it by heart.

The document could also include all four classification levels with descriptions on their differences and status. This was mentioned in the replies to the questionnaire and while not the most important feature, it would be a good addition to the overall knowledge base that the policy document includes.

Overall, the document should be clear and informative, with an easy-to-find location within the company's internal systems. To ensure this, the document could have one named person responsible for its integrity, availability and relevance. With these suggestions the document for the policy can be created into a solid, understandable and quickly referred form.

References

Printed

Alexander, P. 2008. Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers. ABC-CLIO, LLC.

Andress, J. 2014. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2nd Edition. Syngress.

Borek A., Parlikad, A.K., Webb, J., Woodall, P. 2014. Total Information Risk Management: Maximizing the Value of Data and Information Assets. Morgan Kaufmann.

Greene, S. 2014. Security Programs and Policies: Principles and Practices. 2nd Edition. Pearson IT Certification.

Wood, C.C. 2005. Information Security Policies Made Easy. 10th Edition. InformationShield.

Electronic

Cambridge Dictionary. Definition for a policy. Referenced 27.3.2020. https://dictionary.cambridge.org/dictionary/english/policy

Cisco.com. What Is Information Security? Referenced 30.3.2020. https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

Computer Science Degree Hub. What is the difference between cyber security and information security? Referenced 12.2.2020. https://www.computersciencedegreehub.com/faq/what-is-the-difference-between-cyber-security-and-information-security/

Danchev, D. 2003. Building and Implementing a Succesful Information Security Policy. Referenced 12.5.2020. http://www.infosecwriters.com/text_resources/pdf/Security_Policy_JPak.pdf

Dudovskiy, J. Interviews. Referenced 30.3.2020. https://research-methodology.net/research-methods/qualitative-research/interviews/

Dudovskiy, J. Questionnaires. Referenced 30.3.2020. https://research-methodology.net/research-methods/survey-method/questionnaires-2/

Finlex. State Shareholdings and Ownership Steering Act (1368/2007) (unofficial translation). Referenced 19.3.2020. https://www.finlex.fi/en/laki/kaannokset/2007/en20071368.pdf

Finnish Ministry of Defence. 2015. Information Security Auditing Tool for Authorities – Katakri 2015. Referenced 24.2.2020. https://www.defmin.fi/files/3417/Katakri_2015_Information_security_audit_tool_for_authorities_Finland.pdf

Fowler, S. Information Classification – Who, Why and How. Referenced 8.5.2020. https://www.sans.org/reading-room/whitepapers/auditing/information-classification-who-846

Infosecinstitute.com. 2018. CIA Triad. Referenced 20.2.2020. https://resources.infosecinstitute.com/cia-triad/#gref

Irwin, L. 2017. What is information classification and how is it relevant to ISO 27001? Referenced 24.2.2020. https://www.itgovernance.co.uk/blog/what-is-information-classification-and-how-is-it-relevant-to-iso-27001

Kenton, W. 2019. State-Owned Enterprise (SOE). Referenced 25.3.2020. https://www.investopedia.com/terms/s/soe.asp

Kosutic, D. 2014. Information classification according to ISO27001. Referenced 12.5.2020. https://advisera.com/27001academy/blog/2014/05/12/information-classification-according-to-iso-27001/

Layzell, N. 2018. 12 Potential Consequences of Data Breaches. Referenced 17.4.2020. https://dataconomy.com/2018/03/12-scenarios-of-data-breaches/

Perrin, C. 2008. The CIA Triad by Chad Perrin. Referenced 5.2.2020. https://www.techrepublic.com/blog/it-security/the-cia-triad/

Schooley, S. 2019. What is Corporate Social Responsibility? Referenced 25.4.2020. https://www.businessnewsdaily.com/4679-corporate-social-responsibility.html

Search Inform. Information Security Threats. 2019. Referenced 19.3.2020. https://searchinform.com/infosec-blog/2019/08/17/fundamentals-of-is-data-protection/information-security-threats/

Tunggal, A.T. 2020. What is Information Security? Referenced 11.5.2020. https://www.upguard.com/blog/information-security

Whitman, M. 2003. Enemy at the Gate: Threats of Information Security. Referenced 28.4.2020. https://www.researchgate.net/publication/220422187_Enemy_at_the_gate_threats_to_information_security

Figures

Figure 1 Data Types (Borek et al 2014, 7)....8
Figure 2 The CIA Triad (Perrin 2008)....10
Figure 3 The Katakri evaluation process (Katakri 2015, 70)....13
Figure 4 An example of an information life cycle (Borek, Parlikad, Webb and Woodall 2014) 16
Figure 5 Replies to question 1 of the questionnaire....17
Figure 6 Replies to question 2 of the questionnaire....17
Figure 7 Replies to question 3 of the questionnaire....18
Figure 8 Replies to question 4 a) of the questionnaire....18
Figure 9 Replies to question 5 of the questionnaire....19
Figure 10 Replies to question 6 a) of the questionnaire....20
Figure 11 Replies to question 7 of the questionnaire....21
Figure 12 Replies to question 8 of the questionnaire....22
Figure 13 Replies to question 9 a) of the questionnaire....22

Appendices

Appendix 1: Excel form for questionnaire analysis 30

Appendix 1: Excel form for questionnaire analysis

	1 - Requires significant improveme	2 - Requires some improvemen	3 - Does not require improvemer	Comments	Themes
1. How long have you worked at Company X?	-	-	-	The first question is just to get information on the duration of employment of the people who replied to the questionnaire, hence no 1-2-3 rating is given.	17 responders out of 19 have worked inthe company for over 6 years, one had worked less than 2 years and one between four to six years. Thi
2. How well do you know the policy on information classification and restriction?		X		Overall the knowledge of the policy seems quite fine, possibly due to a bigger need to know the policy somewhat. However, it would be better if everyone in the company would at least have an	None of the responders knew the policy very well, but only knew of its existence. 4 out of 19 were not aware of the policy.
3. Do you know where to find the policy?	X			Almost half of the responders did not know where to find the policy. This needs to be fixed so that	8 out of 19 responders did not know where to find the policy.
4. a) Has there been any discussion of the policy during	X			As with the previous question, the same amount of	8 out of 19 responders had never discussed the policy.
4. b) When and how should the policy be discussed?	X			In relation to question 4. a) some sort of systematic discussion should be had with every employee.	happen at the beginning of the employment with regular reminders of keeping up to date with the policy. Interestingly one response was that the policy should be discussed with proper time, while another one thought that it should be just a small part of
5. Is the policy clear?	X			8 out of 19 responders did not deem the policy clear	
6. a) In your opinion, should or could the policy be improved?	X			9 out of 19 felt that the policy should or could be improved	
6. b) If you answered yes to the previous question, how?	X			As said above, nearly half felt that the policy needs improvement.	possible practical examples of situations.
7. Do you know the different classification levels of Company X?		X		Most people are aware of the classifications, however actually knowing the different classifications can be deemed important only for those who need to know	
8. Regarding your own work, are you able to determine what information should be classified under the policy?		X		7 people were able to determine, 10 people only part- ly and 2 people were not able to determine. This once again falls down to the question of who actually needs	
9. a) Are you aware of the instructions on handling a situation where information is given out to a third party?		X		General knowledge of the instructions seems to be fair. 3 people knew the instructions, 11 knew them partly and 5 people did not know them. Everyone sho uld at least know the basics and where to find the	
9. b) How would you improve the policy? If the policy doesn't require improvement in your opinion, explain why		X		Same as above.	Biggest themes were simplifying (as in easy to comprehend) and in general so that people would receive information of the policy. The policy should also be acknowledged straight from the
10. What kind of risks does a lacking policy on informa- tion classification and restriction cause?			X	People generally seem aware of the importance of information security, mainly listing the same risks.	Security breaches, financial losses and the loss of confidential information. Also with one reply it was mentioned that it is sometimes difficult to get access to information within the com-

Most of the answers to the questions were quite evenly split, with about half of the people not having much information about the policy. When looking at the individual responses, the answers were consistently the same people in regard to not knowing of the policy. The main things to improve the policy should be a focus on the accessibility of it and making sure that everyone is at least aware of it. Many of the answers claimed never to have been discussing the policy and this is one place where to start: especially at the beginning of an employment, this should be brought up and be the starting point of the development. Also when there is discussion of the policy, it would be recommended to go through the guidelines more in depth with people who will have to know the policy regarding their own work, whereas people who do not necessarily need to know all the information within the policy should at least be informed of where to find the policy. Having the policy be easy to read and consistent with possible practical examples would be good to include. Taking into consideration that the company's classification has only four levels, this information could be known by every simple employee (even if a specific employee would not necessarily need to know them regarding their work) just to promote the security environment of the company.