Linnéuniversitetet
Kalmar Växjö

Linnaeus University

1DV700 - Computer Security

Assignment 2

Software design document

Group Members: [redacted]

Table of Contents

1. Introduction

This document intends to give an understanding of the Information Security Management System (ISMS) of the Linnaeus Book Publishing Company. It is designed for employees and stakeholders to define the state of the security inside the company. The goal of this document is to explain the security measures that are implemented inside the company.

In the first part, we will explain the purpose of a Software Design document and its scope. In the second part, we will assess the existing company's system and explain the issues and vulnerabilities with principal risks linked to this system. In the third part, we will present the different solutions we would implement for Linnaeus Book Publishing Company and in the fourth part, we imagine different scenarios to emphasize the proposed implementations.

1.1 Purpose of the Software Design Document (SDD)

The purpose of the Software Design Document is to give an overview of all the solutions we intend to implement to assess the coherence of the project [1]. Through the elaboration of the document, both the consultants and The Linnaeus Book Publishing Company will be able to understand the implementations to bring to the organization to make it secure.

The goal of this document is to provide an understanding for anyone aiming to grasp what security measures are taken by the Linnaeus Book Publishing Company and how they cope with Swedish regulations.

1.2 Scope

With the help of this document, we will provide certain practices and guidelines to provide a secure environment for the system and business of Linnaeus Book Publishing Company to operate in. This document helps in increasing the reliability of this system while still maintaining the three pillars of security: confidentiality, availability, and integrity. The need for a security system will be fulfilled with help of much more competent and knowledgeable staff. This can be achieved by training and updating the knowledge of current employees along with hiring new employees. Current employees are the ones handling the system and its proper working, management, testing, and corrective measures, along with the communication channels and safely transmitting information with the help of encryption techniques and authenticating the access by authorized personnel together with keeping a log of the activity in the system. This policy will include all the IT hardware and software of the organization along with the usage of personal devices of the employees for business activity. This document also offers backup plans for day-to-day business activity and recovery plans. That can be useful in case of any emergency or security disaster incidents. It also includes unauthorized access and takes consideration of the incidents that occurred in the past such as viruses, denial of service or trojans, etc.

2. System Overview

The system goal is to provide the Linnaeus Book Publishing Company with a secure implementation of security systems inside their organization. Hence, several principles are followed to provide solutions to the company:

Restriction of access depending on user's profile: Due to the presence of different malware and a possible leak of information, the accesses need to be regulated with higher access to responsible people such as IT responsible.

Create an adaptive structure: The solution presented here should be adapted to the potential growth of the company.

Implement solutions for workers inside and outside of the office: The policies take into consideration workers and freelancers producing intellectual properties outside the office.

Data: The implementations and storing of data need to comply with the GDPR if one wishes to process and handle personal data and sensitive personal data [3]. Standardized and secure IT-security implementations for personal data with an emphasis on sensitive personal data.

"**In God, We Trust, All Other We Audit**": Develop an organization where trust and control work together, even with the neighbor law firm.

Files from the company should be readable only by the employees: A general encryption should be made by internal software so that only employees using the company's system can work with the company's material.

Establish a periodic review: Every year, the plan should be reassessed.

Implement a backup plan: To recover data from loss of information.

Update the security policies: The company should put in place the policies and update them through the months.

2.1 General Overview

The approach used for implementing the system in the company is the ISO 27001 standard [2]. It preconises to adopt an Information Security Management System which consists in:

1) Identify all the actors involved in the operations of the company and assess their expectations in terms of security
2) Identify existing risks in relationship with information flows
3) Define access control to set expectation and handle risks
4) Set objectives on the purpose of securing the organization
5) Complete others type of controls and assessment of risks
6) Estimate continuously the implementation of these controls
7) Provide continuous improvement

2.2 Assumptions

Here are all the assumptions we can make about the existing system:

The company loses business and value by not gathering data: By not gathering data from its customers and employees, the company deprives itself of important information that can help it grow or take better solutions. It is in their interest to invest in a system that gathers data for further business.

The company allows anyone to get access to their data: By not securing their system, the Linnaeus Book Publishing Company allows malware and other types of viruses to get access to their sensitive information. The same happens with not restricting their access to servers. They do not prevent people from coming and getting all their data from their employees or their. Even the neighbouring law firm can eventually steal their data. They need a system to prevent this.

Total access control allows threats from any device controlled by any employee: By not restricting the control, the company potentially permits access to their files through any device any employee has. We assume the company needs to protect itself and let its employees work outside of the office.
No encryption allows competitors to read the company's documents freely: By not encrypting the company's documents, competitors, if they can access the files, can consult them and copy them as they can. We assume the company will want to protect itself against robbers.
A small event could destroy most of the company's work: As the servers are not protected in case of natural catastrophes, the company's work can be destroyed pretty easily if anything happens to the servers. We assume the company does not want to lose all its activity.
The company has no solution to recover its data if it loses it: As they do not have any backup plan, it might lose all of its data at once. We assume the company does not want to lose its data.
The main focus is security: Even though the organization has not disclosed its budget it is assumed that the main focus is on improving security. As such the report will mainly concentrate on that fact and is expected to make amendments in the future if there is a need to cut costs

2.3 Constraints

According to Pfleeger, a constraint is: "an aspect of the security policy that constrains, circumscribes, or directs the implementation of the requirement." [3].

The implementation of security controls has several constraints. Here are some of them:
Need the right granularity: If the system is too secure, it can slow down the business processes and impede the work of employees.
Cope with the EU and Swedish laws: Comply with the GDPR when processing data and adjust the process and security accordingly[3].
Appoint a person responsible for security: One person needs to be taken accountable for the security of the company.
Empower employees: They need to be aware of how to handle security.
Change in the configuration of the office:
Not enough information about the system and its expectations: Information about the application itself was not available as such the report will be in a more general approach.

2.4 Risks

The risk analysis is describing the actual state of the security and the problem the company can face [3]. It follows this structure:

1. Identify assets
2. Determine vulnerabilities
3. Estimate the likelihood of exploitation
4. Compute expected annual loss
5. Survey applicable controls and their costs
6. Project annual savings of control

A risk analysis could be a longer document on its own. Here is a simplified risks analysis for the Linnaeus Book Publishing Company:

Asset: Servers - Risk: Physical destruction of their data: The risk is pretty rare but the chances of it occurring at least once through the years can be relatively high. The annuals loss are high as they would

impact the whole organization and eventually stop the activity. The expected savings represent more than 90% of the activity of the company.

Asset: Company's Data - Risk: Data can be physically accessed and stolen: Their servers do not have physical barriers and anyone, even the neighbor's firm can have access. The risk is relatively low as few people have enough knowledge on how to steal data from servers. However, the annual loss can be consequent depending on the type of leak of data.

Asset: Ideas - Risk: Ideas can be stolen: As malware and other viruses have access to their system, someone might have access to sensitive files that give the company its competitive advantage. The likelihood of exploitation is medium as competitors expose themselves to big legal risks doing so. However, the annual losses are huge. Some simple steps can be taken to avoid an easy leak of data. It is worth mentioning that ideas are hard to be considered stolen by copyright law. Hence, it is hard to prove that a competitor stole your idea. The best way is to protect yourself.

Asset: Company's organization : Risk: Nonadaptable plan: The company needs to adapt its security according to its size. The likelihood of exploitation is high as the company intends to grow. The annual loss is hard to count but there can be repercussions on the company's activity and its process and it can range from nothing to the destruction of the business. To prevent this, an evolutive plan should be planned.

Asset: Company's software, system, and data. Risk: Viruses and malware: The likelihood of exploitation is high. Expected annual loss can range from nothing to the destruction of the company's organization. Applicable control: Anti-malware software.

Asset: System access and system. Risk: Anyone can change anything in the system: There is no access control and everyone has full admin privileges. The latest intern can access the same file as the CEO. The likelihood of exploitation is high as someone can make a mistake without being aware of making one. Annual losses are hard to compute. Applicable controls: Give right access to the right persons, and multifactor authentication, closed systems through VPN.

Asset: Organization's system. Risk: Problem of compatibility between devices: The computers have different operating systems. This will make it difficult to use a centralized set of controls but not impossible.

Asset: Company's organization- Risk: Problem of accountability: No one is supposedly responsible for the security inside the company. The vulnerability is high as no one is accountable in case a problem would arise. The annual loss is hard to compute. Applicable controls: Designate a responsible for the security, and keep a logg of who accessed the data.

3. System Design

3.1 Software Design

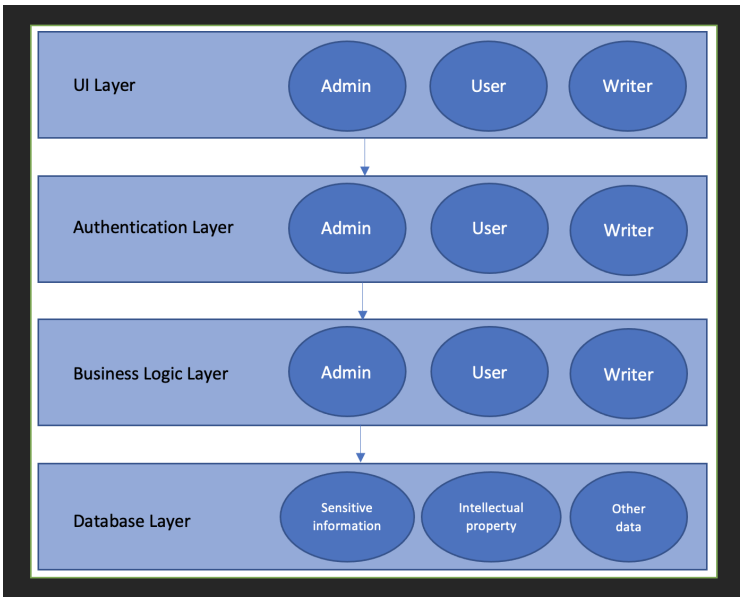
Software architecture

Software architectures are crucial aspects of software applications. They explain the different components of an application and their relationships. According to ISO 25010, indicators of a good architecture are: suitability, reliability, performance, compatibility, usability, security, maintainability, portability [4].

There are many different patterns of software architecture that are available out of which 'layered pattern' architecture has been selected for this project [5]. Please refer to the Appendix A for the full analysis on why this pattern was selected. It divides the application in different layers according to the expected activities of the company and the access that we aimed to give to the different profiles of the company.

Following is the suitable architecture for the Linnaeus Publish Book Company:

Figure 1: Proposed software architecture diagram



UI Layer

UI layer is the presentation layer where all users will communicate with the application. Here the application can be broken into different features and then based on the access level only the authorized features will be shown for the logged in individual.

Authentication layer

Authentication layer will handle the main authentication process. It is proposed to go for a two-factor authentication process to minimize the dependency on just a password. The two proposed methods are traditional username and password level and a SMS or email based code. Also, the number of incorrect attempts can be monitored and based on a limit the account can be locked and put through a forced password change. One possibility is to use a token-based approach through a third-party service. But here a little control over the security process is lost but the implementation is much easier that could help with the cost.

Business logic layer

Business logic is handled by the third layer which are the expected functions of the application. Here a layer of security can be added by checking if the relevant logged in user has the authority to execute the relevant task or view the specific data. If needed an extra layer can be added so that for some special tasks to require external authority by a higher-level user.

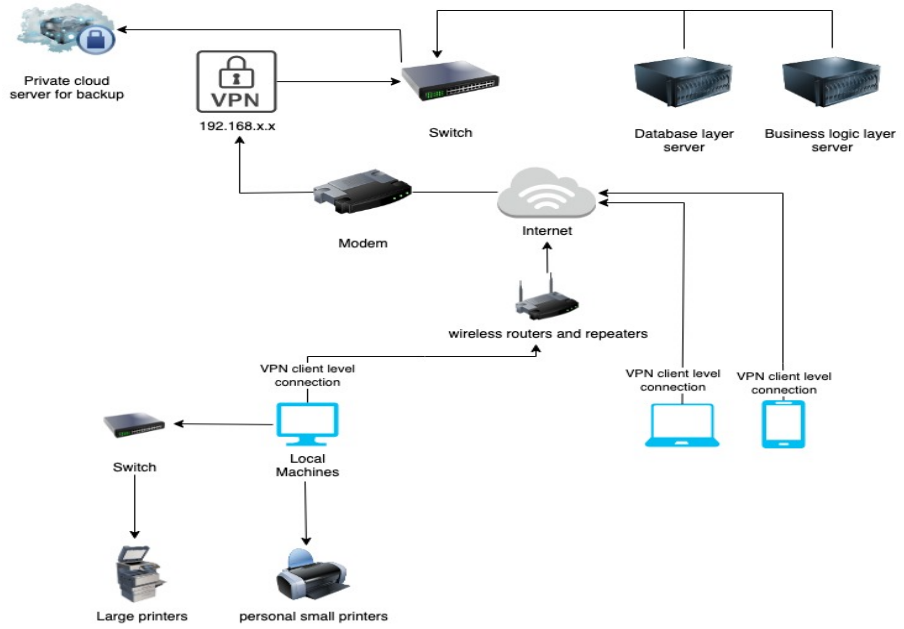
Database layer

database layer will handle the data storing, retrieving , manipulation and removal part of the application. The database layer is broken in three separate areas based on the requirement into Sensitive information (for legal requirements), Intellectual property (Security reasons) and Other (General purpose). This way the application can be clearly separated based on the client's requirement. By separating the data into different groups based on their level of sensitivity different methods can be applied to those sets of data. As an example, the most sensitive data can be kept in a separate table with encryption. This is further discussed in application security.

As noted, there are three different components in the first three layers named "Admin", "User", and "Writer". This way the application can increase or decrease the access to organisations resources based on the user.

System architecture

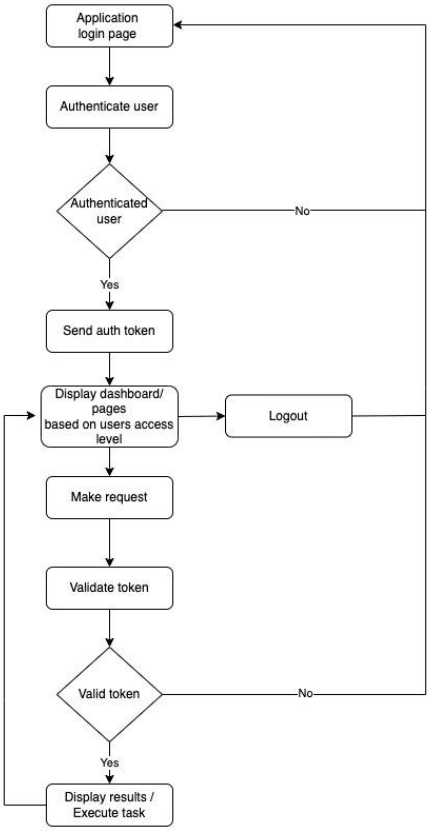
Figure 2: Proposed system architecture



The main motivation of this architecture was to create a closed system where no one has direct access to the server and its data. A separate modem and a VPN service is used to create a closed environment where the application is only accessible through that VPN's client level connection. Then it is connected to a private secure cloud service for regular backup of the data that was classified as most important to the business. Then the users can connect to the application through a client level VPN connection to the applications servers from the office or out of the office.

Data Flow diagram

Figure 3: Data flow diagram



When the application is accessed through a VPN connection the user will be brought to a login page where the authentication process will be carried out. If the request can pass both the authentication levels of the two-factor authentication process a dashboard with the relevant features accessible to the user based on the user's level of access will be shown. At the same time a security token will be saved as a proof of login for future requests with a refresh timeout. If the process fails, the user will be redirected to the login page. Then the user can carry out the different tasks that are available. When a task is executed, validity of the token will be assessed and checked whether the token has timed out. If it is invalid, then the user will be redirected to the login page otherwise if it is valid the request will be completed. When the user logout the token will be destroyed and the UI will redirect to the login page

3.2 Security Software Design

Authentication to validate user identity will be done with the help of an Identity Providers System. It is recommended to use the services of companies such as Okta that provide cloud-based identity authentication. In this type of offer, addition, maintenance, removal, and management of identity information and privileges for users, or systems are provided. It administers principal authentication for service applications within a federation or distributed network while still maintaining the security integrity of the system. Such services not only apply to employees but also to other stakeholders, like clients for example. First, the company will define who has the access to their resources and what is the extent of their rights. Then, employees will input their email and password as login information according to their roles. Then, they will be granted different access rights or privileges to the system. For monitoring this, some features help in restricting and determining access rights based on the user. It makes it easier for the IT department to control unmanaged devices and see that they do not have access to the company's resources. Thereby protecting the company's

sensitive data. Here, employees have to remember just a single authentication password and they will be able to easily log themselves in. Services use the benefits of multiple services Single Sign On(SSO). They allow for Multi-Factor Authentication (MFA). It solves the dual purpose of authentication as well as management of (audit) logs as to who used what service and at what time. Whenever there is an issue or incident it will be easy to identify [7][8][9].

Authorization to the user logging into the system will only be allowed according to the roles, responsibilities, and positions of the employees.
Functionalities will be offered on a role-based logic. For example, an employee working in the printing department will only have the access to the material that concerns them. That means systems are constructed as per the organizational structure. With the help of this logical approach, employees can only receive the information that is needed to discharge their day-to-day duties. Once a user has been authorized, they can log into the system and access the resources and functionality that have been made available to them [8].

Encryption Protocol is a set of transformations to encode and decode data. It is used through a network to make information unreadable so that anyone managing to get access to the data cannot decrypt it without a decryption key.
Decryption keys should be stored separately from data and regularly updated to the most recent. It is a measure that provides digital protection regarding the data stored on physical devices, servers, and online modes. Various encryption protocols include AES, RSA, and SSL/TLS for example. These protocols are needed to prevent information leakage in events of unauthorized access or crime like theft. As per current standards, AES-256-bit key encryption is recommended. It is secure and widely used in a variety of applications. Encryption can apply to multiple levels. That way, hacking becomes difficult for hackers even if they can access the original data. Encryption is easy to implement and resistant to attacks [10].

Communication Network is a group of interconnected devices or systems that exchange information, share resources, and communicate with each other and on the internet. The wifi router and repeaters should switch to WPA3 PSK to provide safer and stronger encryption. This type of wifi uses Advanced Encryption Standard with a Pre-shared Key for authentication. This utilizes a password that is shared with the devices and the access point. Hence, the password should be kept and regularly updated by an authorized person(s), as it is shared with devices. Even if this is secured, it cannot be immune to security threats. We recommend adding a modem to the fiber router that will not have wifi access and will be connected to a VPN, the router, and the repeaters. Along with that, there have to be two separate wifi connections: one for the internal company working and one for as guest wifi connection. That way, guests cannot access the local network at any cost [11].

Securing the network with Virtual Private Network (VPN). A VPN creates an encrypted and secure connection between a network and a device. Here, they will secure the link between the company's internal network and employees' devices. It will act as a security cover over the company’s internal network. It will make it difficult for hackers or third parties to access and intercept the company’s data.
VPN has no log policy, which makes it even more secure. It can access information that may be blocked in the country by getting around the geolocalization. We recommend a VPN that has a connection to multiple VPN servers. It will encrypt the data multiple times. That means employees' devices will get connected to the VPN server and that VPN server will build a connection to one or more VPN server(s) before transferring data to its ultimate destination. This way data will be encrypted more than once and be as secure as possible. The company's connection speed will be slowed with the use of a VPN. However, our primary concern is about the security of the network rather than speed. [12].
A VPN will also be needed, as employees are issued office devices to be carried for outstation work that is **remotely working possible.** That way, the employees will be able to secure connections at different locations and connect to the company's servers. It will reduce the risk of protection and unauthorized access by still maintaining the security of data [13].

Updating and upgrading Operating Systems (OS). It will be important for the company to keep the OS up to date to ensure the system is still secure and functioning properly. We recommend updating all the security patches to the latest version. It will help fix the bugs and improve security from new vulnerabilities. By updating, we mean that there should be only one OS version from a provider. That is upgrading all the devices with OS Windows to the latest version of OS that is Windows 11. Devices that cannot be upgraded or have been stopped from further support should be discarded as they will cause security problems. Along with updating Windows devices, all the MAC and Linux devices should also be upgraded to the latest version. To make sure everything is properly followed an authorized person should perform this task. The authorized person should follow proper procedures like:
1) Check for updates in OS and security patches
2) Install it on one system and test it, so that mass updation and upgradation do not bring down the company work and mess with or cause any conflict or issues in the existing infrastructure.
3) Test and monitor if everything works fine then in a controlled way perform upgradation and updation of the company-wide structure. There should be a backup of all the files and data and a disaster recovery plan if something does not work during this process. Sometimes, installation may cause problems if not done correctly. The authorized person can perform an adequate rollback while the company continues to work as it was before this process [14].

The use of Antivirus is also recommended as OS internal security features may leave few malware or risks like trojans, viruses, worms, etc. Those are not easy to detect and they may cause harm to the company's system. Our recommendation is to use antivirus software, such as Norton Antivirus, as it is one of the best and most highly reliable products in the market. It is also much more affordable than the others and provides an all-around protection suite. Its services include, but are not limited, to real-time protection, VPN protection, Webcam protection, Password manager, dark web monitoring, etc… Its scanning is also very effective and detects and quarantines or removes even a single virus that is in the system. It also blocks spam email links so that it maintains the integrity of employees' devices and causes no harm to employees or their devices. Along with that, it removes all traces of unauthorized files .

Backing up Data and resuming business activities helps in ensuring that this company can recover from either system failure, data loss, or downtime issues and resume business activities very quickly. Its recommendation is, to first classify and maintain data and information based on their criticality to business, that is rank them and then have a 3-2-1 backup strategy to be implemented. As per this strategy, there should be three copies of data that are two on-site and one is stored on a local server. The others are stored on external hard drive devices, and one off-site which means stored on a remote server usually via the use of the internet. It is recommended all the backups should be encrypted. Having an online backup will not make it vulnerable to physical damage or theft, but the cloud service provider should be very reliable and all past incidents should be found out before using their services. The speed of restoration will depend on the speed of the internet. Our recommendation is AWS suite services such as Backup and Database, as it provides Cloud-native backup, Hybrid and Centralised Data Protection of all applications and services and also ensures data protection compliance with real-time analytics and insights. How does it works? When creating a backup vault, you can use the AWS Key Management Service (AWS KMS) encryption key that encrypts the backups placed in this vault, and all copied backups are encrypted with the key of the target vault. Cloud Backup has become an important part of backup no matter the size of the company. Alternatively, the service of Acronis Cyber Protect Can be used. Along with this please refer to Appendix C for the recommended Procedure for Backup [15][16][17].

Physical Security of the Server Room is a very important factor. Right now the company has placed the servers in the basement without any proper facilities. The place is shared with another neighbor company that keeps files and old furniture near the servers. It is recommended to separate the company’s server location from the neighboring company by a strong wall and remove the files and old furniture from the area. This way the company will not be sharing the room. Alternatively, it is recommended to the company, if possible, to shift the server room altogether to a new location. Possibly to a higher floor than the basement. Access to the server has to be reduced only to a handful of people like the CTO, IT staff, and eventually the CEO. Should be authorized only employees who will be authorized by a competent authority.
Following a physical structure, a biometric lock or pin lock or smart card lock should be used for making an authorized entry or exit, to and from, the server room. Due to costs, it is suggested to atleast have a minimum

of a badge entry so that access will be recorded to keep a track of people accessing the server room.
To enhance security, the installation of CCTV surveillance cameras to check and record everyone accessing the room. The reason is, a pin, card, or badge can be stolen or lost or someone can make a duplicate copy. Then, unauthorized people can access, use or intervene in the server room.
All equipment in the server room should be placed in a fireproof and shockproof locked rack or cabinets. The room should have a fire and smoke alarm and also a leakage detection system.
The room should also be secured from any power outage or disruption and should also have a backup to prevent the servers from stopping, so an uninterrupted power supply is needed which can be achieved by the use of power generators and UPS.
Also, it is recommended to use an air conditioner to cool down the server room, and also this will help in slowing down the server fan speed which will thereby reduce noise as well [18][19].

Handling of Sensitive data and information can be done by the company by first identifying and classifying information and data they collect from their clients, employees, and other stakeholders. The company carries added responsibilities regarding security and safety for personally identifiable information and data. They have to go the extra mile to protect themselves from any risk. There are best practices or data privacy frameworks that can be used by the company like COSO, ISO 27000 standards, ITIL, ISACA, and EU General Data Protection Regulation (GDPR). All data and information that is personal and sensitive must be encrypted to protect its integrity and confidentiality. Also, the encrypted data and information should not be attributed or related to any client or employee, or stakeholder. In case of any breach of data, integrity, and security, its availability should be immediately restored.
When storing personal data, to ensure that its supported by one of the legal bases of the GDPR. As an expanding company its plausible to appoint a data protection officer, to monitor so that the company and its employees comply with the GDPR, keeping the data protection and security up to date. And to help keep track of personal data processing either keep records on processed data or implement a policy for data protection to help prove legality and that they comply with the GDPR [20].

Managing personal devices and equipment (BYOD Management) as the company has recommended adequate controls in place, to avoid any present security risks and compliance challenges for the company. As employees bring their devices such as mobile, smartphones, and tablets to work.
Using these personal devices may lead to data breaches or the risk of unauthorized access. But already, multiple controls have been recommended, like authenticating users, VPN, etc.
BYOD is not recommended as it might result in increasing the cost to put the necessary controls. If a BYOD plan is needed by the Company then please refer to Appendix B [21].

Application Security is going to be used for the collection of information. It will keep track of information quality, volume, type, and cost associated. From the information collected, some will be sensitive and will have to be regulated. The security risk involved here is cross-site scripting. Attackers introduce client-side code into the application and get direct access to information. Then, authorizing the user multi-level authentication (preferably two levels) is recommended for the company. A security issue here is the Denial of Service Attack (DOS). In this case, the attackers flood a designated server or the framework that upholds the different sorts of traffic. This traffic, in the end, keeps the real user from getting to the server, thereby attackers making it shut down. As an important quantity of data and information is involved, an application log records monitor is needed. It will record who accessed what portions of the application. After that, the authentication user is allowed to use the application, which means the identification of the user is validated to approve the access in the authorization step.
A security flaw called SQL Injection is used by hackers to exploit databases. Hackers uncover user personalities and passwords and create, modify and delete data without taking permission from the user. A lot of sensitive data and information are involved, and if a security break happens, the company's data and reputation will be at risk. To prevent that, proper encryption protocol is needed to keep the sensitive data safe while flowing from the end user to and from the application.
Another security flaw where a hacker executes a variety of attacks on an application and changes spaces of memory on the application and memory corruption can occur. It's called a buffer overflow. The software can behave normally or get shut down at the end. There should be testing of application security, to provide a guarantee that security controls are working properly. If any corrective action is needed then the same can be

taken.
Key Principles of Application Security are to maintain Confidentiality, Integrity, and Availability of data and information along with no repudiation of actions to be traced back to specific individuals. Third-Party developers must adhere to security in software development, and several of the best practices regarding security in the development process can be followed:-

– Security Bugs can be easily identified, in the design of applications, by the developers during peer review before merging changes to the main branch.
– Threat model existing design and create new threat model for when significant changes are introduced in the design of an application.
– Static and Dynamic Analysis tools are implemented to scan the code base during the development process and when the application is deployed.
– Testing of application against vulnerabilities and risk including OWASP top 10 vulnerabilities
– Pentest Report to be carried out before the application is deployed and every time new changes are pushed.

All the security protocols discussed separately will apply to the application security as well like authentication and authorization, encryption, communication network, VPN use, handling of significant data, etc. [22][23][24]

4. Use Case Scenarios

Use cases intend to explain how users interact with the system of the Linnaeus Book Publishing Company [25]. It is divided into 3 parts: System, Actors and Scenario. Here are the different use cases:

System: Retrieve password and two-devices authentication

Primary Actor: Any employee of the company

Scenario: Employee X has forgotten their password. While trying to log in, it can remember it. He clicks on the "forgot my password" and an email is sent to X. It needs to first enter a code, the same one that was written in his email, and then another email is sent to his mobile to confirm that it is intended to retrieve the password. X needs to confirm on their mobile too to be able to reset his password. Once confirmed, X can create a new password.

System: Access to the servers and security linked

Primary actor: The CTO and all the employees accredited to access the server. Accredited in the system.

Scenario: X is an employee of the company. Due to the recent expansion of the company, she/he is IT accredited in the company, as well as the CTO. X has access to the servers through a smart card which is dedicated. It allows her/him to open the door of the room where the servers are. While working on the servers, X is recorded by a system of video cameras that is there to check who is accessing those servers. According to the recommendation of the European Data Protection Board, the footage of the recordings is stored for three days [2].

The room where X is has fire-resistant material all around, there is a fire extinguisher and also some smoke detectors. Servers are placed on cabinets that are shock resistant to reduce noise. Wiring is properly done and each of the servers has a special mark on the floor that indicates where they should be. The room has an air conditioner to dispense the heat generated even if the room is generally chill. In case of a power spike, there are electric surge protectors and UPS are installed with the server. The room has a waterproof ceiling to avoid any water leakage and a ventilator shaft window in case of emergency. The room is closed in a basement which is shared with the firm next door.

Y is an employee of the company. Y does not have the possibility to access the server/server room as Y has nothing to do with IT-related stuff. Y thinks that something Y is looking for is in the server room. Y comes downstairs to check if Y is right but it cannot access the room. Y needs to ask someone else from the company who has the right to access the server room to access it.

System: Encryption of data and data theft

Primary actor: Hacker outside of the company/competitor

Scenario: A hacker outside of the company is trying to steal the ongoing projects of the company. The goal is to sell this to the competition so that they can produce similar or even better stories.

The hacker managed to access the system and steal all the files. However, once those files have been downloaded, the hacker figures out that the files are encrypted. The hacker used to get only original files, which weren't complicated to decrypt but now, the hacker does not have the knowledge or the computational power to decrypt the files.

System: Access control and privileges

Primary actor: Any employee of the company

Scenario: X is a writer in the company. It is Friday afternoon and a window appears to ask X to update something on the system. The command actually asks X to restore the whole system. As X has limited knowledge and wants to leave for the weekend, X clicks on 'yes' without trying to understand what this is. X thinks it will help him to leave faster.

However, another screen appears saying that X does not have the access privilege to take such a decision. X then asks the CTO who understands that this command shouldn't have been there. They also understand the gravity of the situation and they tell X to leave for the weekend and that they will take over. With full admin privileges, X could have erased a lot of sensible data.

System: Authentication to the services of the company

Primary actor: Employee of the company

Scenario: X is an employee of the company. Every time X needs to access a special application, X needs to enter credentials and authenticate. X has access to those applications depending on his role in the company. The authentication is managed by an Identity Provider System (IPS) which regulates how and when to enter passwords. Sometimes, X needs to also use its phone as the IPS requires triggering a button on X's app.

System: Company's data, back up plan

Primary actor: Database administrator

Scenario: X is the administrator of the security of the company. Unfortunately, a fire started last night and it burned half of the servers. While insurance companies will repay for the equipment, the company needs to keep its operations running. Luckily, X has planned a weekly backup and only 3 days of work have been lost. Most of the writers can find projects they were working on or emails they wrote. They might have lost some paragraphs but everything is there due to the backup planning.

5. References

1. Angela Zhang (2018), *How to write a good software design doc*, [Online], Accessed: 12/06/2022, Url: https://www.freecodecamp.org/news/how-to-write-a-good-software-design-document-66fcf019569c/

2. Dejan Kosutic (2016), *What is an Information Security Management System (ISMS) according to ISO 27001?*, [Online]. Accessed: 12/09/2022. Url: https://advisera.com/27001academy/blog/2016/05/23/information-security-management-system-isms-according-iso-27001/

3. C. P. Pfleeger, *Security in computing* , fifth edition.. ed. Prentice Hall, 2015

4. M. Haoues, A. Sellami, H. Ben-Abdallah, and L. Cheikhi, "A guideline for software architecture selection based on ISO 25010 quality related characteristics," *International Journal of System Assurance Engineering and Management*, vol. 8, no. S2, pp. 886–909, 2016.

5. M. Richards, *Software Architecture Patterns*, 1st ed. Sebastopol, California : O'Reilly , 2015.

6. *What is a microservice architecture and it's advantages?* YouTube, 2018.

7. Helpshift, *What is User Identity Verification, and how do I set it up?* [Online], Accessed: 12/11/2022, Url: https://support.helpshift.com/kb/article/what-is-user-identity-verification-and-how-do-i-set-it-up/

8. Alexey AVerikhn , *What is Authentication-Authorization-Validation Framework?* [Online], Accessed: 12/11/2022, Url: https://netlicensing.io/blog/2020/09/24/authenticate-authorize-validate-framework/

9. Okta, *Byggd för alla i personalstyrkan,* [Online], Accessed: 12/11/2022, Url: https://www.okta.com/se/workforce-identity/

10. Riley Dickens, *What are Encryption Protocols and How Do They Work?* [Online], Accessed: 12/12/2022; Url: https://www.encryptionconsulting.com/what-are-encryption-protocols-and-how-do-they-work/

11. M. Jones, *10 Ways To Secure Your Business WiFi Network.* [Online], Accessed: 12/14/2022 url: .https://www.coxblue.com/10-steps-to-take-right-now-to-secure-your-business-wifi-network/.

12. eSecurity Planet, *VPN Security Risks: Best Practices for 2022*. [Online] Accessed: 12/10/2022, url: https://www.esecurityplanet.com/networks/vpn-security/

13. C. J. Team, *What is a VPN, and how can it help enterprises with remote workers?* [Online] Accessed: 12/14/2022, url: https://www.cybereason.com/blog/what-is-a-vpn-and-how-can-it-help-enterprises-with-remote-workers.

14. GFI Software, *Windows Patch Management Best Practices*, [Online] Accessed: 12/15/2022, url: https://www.gfi.com/patch-management/windows-patch-management.

15. Yev Poussin, The 3-2-1 Backup Rule, [Online] Accessed: 12/07/2022, url: https://www.backblaze.com/blog/the-3-2-1-backup-strategy/

16. AWS, *AWS Backup Service* [Online] Accessed: 12/07/2022, url: https://aws.amazon.com/backup/features/

17. Gadjo Sevilla, *Acronis Cyber Protect Review, Deep cloud backup capabilities with huge array of security and device management features*, [Online], Accessed: 12/13/2022, url: https://www.pcmag.com/reviews/acronis-cyber-protect.

18. Segun, D. (2022) *Tips for keeping your server room safe and secure*, *SecureBlitz Cybersecurity*.[Online] Accessed: 12/13/2022, url:https://secureblitz.com/tips-for-keeping-your-server-room-safe-and-secure/

19 E. Yearwood, P. D. 2, and Edwin YearwoodEdwin Yearwood is an IT security expert with a passion for keeping data safe. With a diverse background in cyber security, "10 server room physical security best practices," *CLIMB*, 03-Dec-2022. [Online].: Accessed: 12/15/2022, url:https://climbtheladder.com/10-server-room-physical-security-best-practices/

20. Imperva, *What is General Data Protection Regulation (GDPR)*, [Online] Accessed: 12/12/2022, url:https://www.imperva.com/learn/data-security/general-data-protection-regulation-gdpr/.

21. Machine Engine, *BYOD Management, Simplified personal device management for your organization,* [Online] Accessed: 12/16/2022, url: https://www.manageengine.com/mobile-device-management/bring-your-own-device-byod-management.html .

22. GeeksforGeeks, *Application Security in DBMS,* [Online] Accessed: 12/14/2022, url: https://www.geeksforgeeks.org/application-security-in-dbms/

23. Snyk, *15 Application Security Best Practices*, [Online] Accessed: 12/14/2022, url: https://snyk.io/learn/application-security-best-practices/

24. Check Point, *7 Application Security Best Practices 2022*, [Online], Accessed: 12/15/2022, url: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-application-security-appsec/7-application-security-best-practices-2022/

25. Nicky Daly (2022), *What is a used case?,* [Online]. Accessed: 12/17/2022. Url: https://www.wrike.com/blog/what-is-a-use-case/

Appendix

Appendix A: Selecting a software architecture

Selecting the software architecture is one of the crucial aspects of developing a software application [4]. According to the definition of IEEE software architecture explains the different components and their relationships (among themselves and the environment), guidelines that the applications design and evolution is based upon [4].

Having a good software architecture can reduce the stress caused by problems related to functional, non-functional, and project-based requirements that may come up while the development is in progress [4]. When selecting an architecture there are several performance indicators that can be used to evaluate different patterns. According to the ISO 25010 they are suitability, reliability, performance, compatibility, usability, security, maintainability, portability [4].

When selecting these indicators, it is important to prioritize these based on the requirement because most aspects will have tradeoffs between each other. In this specific scenario the following indicators were selected as the primary indicators.

Indicator	Rationalization	Verdict
Suitability	The application should match the expected behavior, But the program is not very complex as such is not a primary concern	secondary
Reliability	The application should be very reliable as it is meant to work with intellectual property	Primary
Performance	The application will have a limited number of users and no need to have cutting edge level performance. But should have passable level of performance	Secondary
Compatibility	The Organization has different types of Operating systems in the machines. As such, compatibility will be an issue. However, this could complicate the development process and could increase the cost of development. Thus, it is a better option to select on OS for all the machines	Secondary
Usability	Most of the users will have a limited IT related knowledge. As such the program should be easy to use and understand	Primary
Security	The management want special attention to security	Primary
Maintainability	The application should be easy to maintain as the organization doesn't have the internal capability to maintain a complex program.	Primary
Portability	The organization has distance working in place as such the application should be portable	Primary

There are many different software architectural patterns available, out of which the following three patterns were considered for this project.

1. Layered pattern : The application is broken into different layers based on their expected job [5].
2. Microkernel pattern: There is a core application and then different components can be added or removed based on the requirement [5].
3. Microservice pattern: Application is broken into granular services and handled separately [5].

Out of which “Layered pattern” and the “Microservices pattern” were selected as the best options as “Microkernel pattern” is mostly used for commercial enterprise applications which could bring in unnecessary complexity [5]. Microservices pattern did show very good promise, but the issue was the publication company does not have the resource capabilities to maintain the application failing a primary evaluation criterion. As such, the “Layered pattern" was selected for this project. The following table evaluates pattern based on the performance indicators

Table 1: Pattern feasibility analysis

Indicator	Rationalisation	Verdict
Suitability	By breaking the program into separate layers it is easy to separate the logic but at the same time it will not make it too small to become a good match for this criterion [5].	Pass
Reliability	Having different layers means there are high levels of independence between layers, meaning if one layer fails it will have minimal impact on the rest [5]. Thus, increasing reliability	Pass
Performance	Even though layered patterns are known to be slow, by reducing the number of layers the speed can be improved which will go well in this project as it is not expected to be highly complex [5].	pass
Compatibility	As this is a monolithic approach to developing applications compatibility can be a bit on the low end. But it is not a key issue for this specific application [6].	fail
Usability	Since it is possible to have an aspirate UI layer it can be customised an improved based on the expectation of the organisation	pass
Security	Due to its layered nature each layer could be implemented with its own set of security controls improving the security level of the application [5]. But the tradeoff will be performance	pass

Maintainability	Due to it having few defined layers of the application compared to multiple service breakdown of microservice patterns it is much easier to maintain [5].	pass
Portability	To accommodate this it is proposed to develop a web based application, thus it is accessible to everyone.	pass

Appendix B: Complete BYOD plan

To develop BYOD IBM's 10 rules can be used (https://www.ibm.com/downloads/cas/YK52D6GD). The BYOD program is a bit expensive but depends on whether they want BYOD. If not BYOD should be completely stopped at the same time it is problematic not to have BYOD.

Proactive policy creation plan

Criteria	Policy
Devices	Phones, Tablets, Warbles should be allowed in the premises. Personal storage devices are strictly forbidden. Personal laptops are forbidden in the workplace. All forbidden items should be left in a secure location until the individual is to leave the premises
Compliance	Analyze the rules and regulations that need to be followed when implementing the plan. European Union's General Data Protection Regulation (GDPR) and the copyright and intellectual property related laws
Security	All devices are to be installed with malware protection software and are required to update their software frequently. A compliance monitoring software should also be installed to the device
Apps	On devices where sensitive information is allowed, the device is only allowed to have a whitelisted set of applications.
Agreements	Develop an acceptable usage agreement on companies' intellectual property
Access	The employee will only be allowed the least level of access to company information without supervision. A support system with tickets is to be introduced in case extra access is required. Two separate WIFI connections are to be installed, one for public usage and the other for the organizational tasks. A VPN service coupled with two factor authentication is to be implemented to access company data when the individual is using an external connection.

User Privacy	The bare minimal amount of user details will be collected from the personal devices of the employees. An effective period is to be discussed with the management on when such data is deemed no longer valuable at which point the data is to be destroyed.
Data Plans	It is to be discussed whether a data plan or a stipend is provided to the employees or not

Identifying devices that are accessing organizational resources

The next step is to identify what devices are in contact with the organizational resources. Here device management tool is proposed where the organization can analyze the devices and their compliance to the security policies in place. Then a log can be kept on what devices accessed which resources and if they are in non-compliance state the service can be denied. The idea here is to closely monitor the devices that have access to the companies' data.

Making adoption easy

When selecting a tool, it is suggested to use a tool which is easy to use and a one where the employees are comfortable. As an example, Microsoft's service is very easy to enroll in and the familiarity of the programs may make it easier for the employees. Also, if the computers are also all converted into Microsoft based systems the whole security monitoring can be done at on avenue. Some other options are Google's zero touch program or Apple's device enrollment program.

Implement OTA (Over the air)

This is related to configuring the devices remotely to do tasks such as installing updates and security patches, configuring VPNs , embedding security policies, or encrypting organizational data. This can be especially helpful since writers are working from a distance.

Promote self-help

Place systems to make using the system easier when needed. As an example, a self-password reset, device locator services could help users to avoid going to the support team for every issue. Also, an emergency device lock and reset options can also be added based on requirement.

User privacy protection

Personally Identifiable data is not to be collected from the users at any given case. Device reporting on personal applications and other sensitive data is to be turned off through the monitoring application. Any violation is to be strictly enquired and transparency is to be maintained with the employees

Separation of organizational data

The data related to the organization is to be stored separately from the personal data of the use and is to be encrypted. In case the employee resigns the data is to be destroyed.

Data plan

Based on the data usage for the device management, it is suggested to the business to allocate a reasonable stipend for the employees. If not, the organization is to communicate with employees to come to an agreement.

Continues monitoring

The devices should be continuously monitored, and new policies and controllers are to be implemented through continuous learning and adjustment. Recurring security audits are to take place every two months for the first quarter and every quarter for the first year. Then onwards it is recommended to have an audit at least every six months.

Benefit analysis

It is suggested to monitor and calculate the benefits of using the BYOD program and its security system to evaluate its worth. If the results are unsatisfactory the business will be able to cancel the BYOD program.

Training

It is suggested to create a training video on how to enrol for the BYOD programs and the DO's and DON'Ts which can be used to educate the employees on the program and its benefits.

Appendix C: Procedure of Backup

Information to be saved	- All critical or sensitive along with normal information, assets and systems logs and audit trails saved
Frequency of Backup	- All security related logs will be kept online for a minimum of 1 week. - Daily incremental tape backups will be retained for at least 1 month. - Weekly full tape backups of logs will be retained for at least 1 month. - Monthly full backups will be retained for a minimum of 2 years
Procedure for making a backup	- A full backup is taken once a month, then every day incremental backup is taken which updates the files that have been worked upon and adds on new files. Also, then every bi-weekly a differential backup over the full backup to be taken.

	- Alongwith that an Alternate processing site to keep the backup should also be discussed.
Repositories	- Should only contain physical books and magazines but cannot contain the financial, employee and sensitive data, that has to be scanned and kept a copy on secure server and backup drive but not with normal documents
Location for keeping Backups	- Offline backups to be kept for the books and magazines alongwith the copies of the plans, emergency contacts, legal and insurances (securely) - Online backup to be kept in the google drive encrypted - Along with that backup on the hard drive will also suffice with proper encryption. - The server should also be connected to cloud storage and along with that it should be fed with the backups as planned, this will help the organisation in case backup is needed. To achieve this a connection time and be set for 12 hours (or can be even lower) for automatic transfer of files with adequate encryption.
Person/team responsible for gathering backup	- IT head or a person authorised by CTO, also all the roles, responsibilities and duties are properly conveyed to the authorized person

Other General Point	- Prioritizing which operation or recovery based on critical nature is of utmost importance
	  - Approximate Time frame for recovering each system should be properly laid down, after proper discussion and consultations with management
	  - All paper like emergency contacts, insurance, list of employees, emergency exits, blueprint of plans in case an emergency arises.