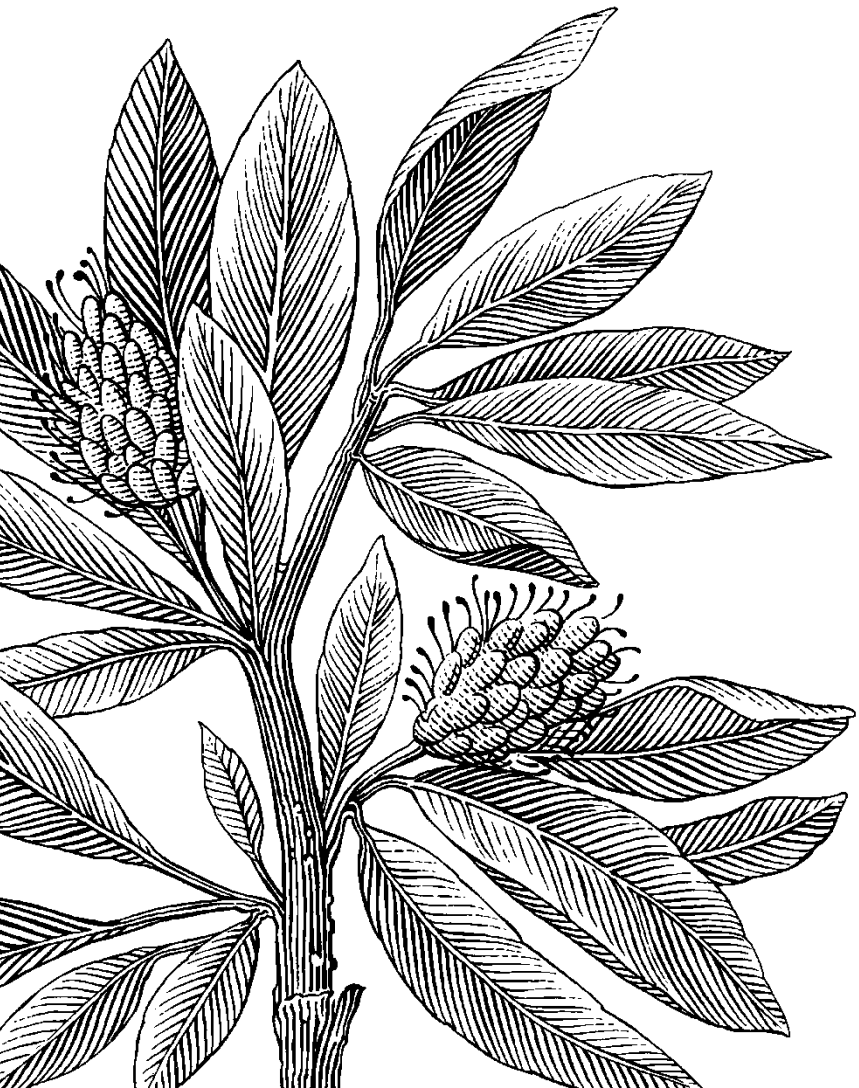
Linnéuniversitetet
Kalmar Växjö

# Information Security Policy ISO/IEC 27002:2013

*GVT Book Publishing Company*



***Authors:***

[redacted]

*Firas Moussa*

Table of Contents

# 1 Introduction

The following document presents the guidelines for applying the different security controls to meet the standards of ISO/IEC 27002:2013, as well as the GDPR. All security controls are covered generally, and some controls have been highlighted in more detail regarding the situation of the company. The information and implementation guidelines provided are in accordance with the information provided by the company CTO.

# 2 Scope

This policy documents applies mainly to all employees of GVT Book Publishing Company, as a guideline for secure operations. Parts of the policies covered in this document are applied to a specific group of employees, and third-party vendors. As a generalized document, it is upon all employees to take part and adhere to the rules and regulations.

# 3 Responsibility

The Chief Technology Officer (CTO) and IT manager are responsible for reviewing, maintaining, and enforcing the covered policies and procedures, with support from the department heads. Employees and third-party vendors of GVT Book Publishing Company are responsible for adhering to and following the stated policies.

# 4 Risk Assessment Overview

The following chapter provides a summary of the methods used for assessing the company risks, and an overview of the identified risks.

## 4.1 Methodology

The risk assessment was conducted using a qualitative approach, evaluating the potential impact and likelihood of security threats.

## 4.2 Summary of Findings

Key risks identified include vulnerabilities in many areas. The risks were summarized in a separate document, "***Risk Assessment - GVT Book Publishing Company.xlsx***". The document contains all identified risks and information about category, impact, recommended controls, etc. The IT management must periodically review and update the vulnerabilities and apply appropriate controls.

# 5 Policy Details

The following chapter covers the practical steps of complying with the International Standards regarding the company situation.

## 5.1 Organization of Information Security (A.6)

### 5.1.1 Scope

This policy section primarily targets the IT Department, Executive Management, and Department Heads at GVT Book Publishing Company. This policy covers the establishment of internal policies, procedures for interaction with external authorities, and the integration of information security practices in projects conducted at the company. The department responsibilities are as follows:

a) **IT Department** is responsible for technical aspects of information security management and the integration into IT systems and projects.
b) **Executive Management** is responsible for overseeing the company-wide information security policies to ensure their alignment with business objectives.
c) **Department Heads** are responsible for implementing the security practices within their respective teams by collaborating with IT and Executive Management.

### 5.1.2 Identified Security Risks

The company currently lacks a structured organizational approach to information security responsibilities, including critical procedures such as reporting breaches to law enforcement. To address this, we must implement a comprehensive structure detailing specific responsibilities and protocols for incident management, including a clear escalation pathway. Additionally, we must assess and fulfill the need for adequate IT staffing to ensure prompt and effective response to security incidents.

### 5.1.3 Internal Organization

To reinforce our commitment to information security, management must define, allocate, and enforce all security responsibilities across various departments. This includes:

a) Conducting mandatory security seminars for all employees to understand their roles and responsibilities in maintaining information security, both within and outside the company.
b) Assigning specific security responsibilities to each department, with regular reviews and updates.
c) Collaborating with department heads to develop and implement detailed procedures for complying with laws, regulations, and our information security policy.
d) Recruiting necessary personnel, such as additional IT administrators, to manage and enhance our security measures.

### 5.1.4 Contact with authorities

Management must establish and maintain up-to-date contact information for relevant authorities, including law enforcement. We must also develop a clear set of procedures outlining when and how to contact these authorities in various scenarios, ensuring legal compliance and efficient incident handling.

### 5.1.5 Information security in project management

Every project leader is responsible for integrating information security considerations into their projects. This includes setting specific objectives related to information security, identifying potential risks, and outlining procedures for incident reporting and secure information transfer. These measures must be clearly defined and agreed upon before the commencement of any project.

## 5.2 Human Resource Security (A.7)

### 5.2.1 Scope

This policy targets the Human Resource Department, IT Management, and all employees of GVT Book Publishing Company. This Policy aims to cover the recruitment of new employees, termination of employment, and everything in between that concerns employees within GVT Book Publishing Company. It describes the process and requirements when employing new staff, the continuous education about information security for employees and the process when employees end their employment. The parties must have the following responsibilities within the human resource security policy:

a) **Employees**: Required to participate in information security training and fulfil their information security responsibilities.
b) **IT Management**: Responsible for ensuring employees implement their training in accordance with current regulations. They must also perform regular information security training that is relevant for employee's information security roles.
c) **Human Resource Department**: Responsible to do ensure that new employees satisfy requirements for their new information security role.

### 5.2.2 Identified security risks

When doing the risk assessment, several vulnerabilities where found. The organization fails to include all staff in the NDA, potentially leading to unauthorized information disclosure. The company also fails to do adequate background checks when employing new staff potentially leading to a misuse of company resources.

### 5.2.3 Hiring new staff

When new people are employed, some steps must be taken to ensure that the employee is fit for his/her information security responsibilities. This must be done before the employees gain access to different systems containing sensitive information [1].

a) New employees must provide at least two references and the employer must conduct a follow-up on these.

b) New employees must also provide a CV, criminal record, and possible certificate to prove that they are fit for their information security role.
c) New employees must sign a non-disclosure agreement that deals with all sensitive information within the company.
d) New employees must also get education on how to follow policies for on handling information.

#### 5.2.4 Maintaining information security

During employment employees must be given adequate training in handling information and other resources they may encounter. Managers must also do follow ups on the employees to ensure that the skills and knowledge is correctly implemented [1].

e) Employees must on a regular basis be given education on any changes in the information security or information system.
f) Employees must also have access to guidelines for how to handle the information systems according to the policy and rules of the company.
g) When given access to additional information systems or duties, employees must be informed and educated on rules and regulations in handling the new information systems.
h) Employees must on a regular basis be given training and information on the need for information security and tools. The purpose is to refresh the knowledge and educate new employees.
i) Management needs on a regular basis to do spot-checks on employees to ensure proper implementation of information security and handling of information processing facilities.
j) When confirmed security breaches are discovered, employees responsible must be given disciplinary actions that match the magnitude of the breach.

#### 5.2.5 After employment

When an employee ends his/her employment or has changes to their information security role, their access rights and privileges must be changed. The purpose is to limit unnecessary access to possibly sensitive information to minimize loss of data or other data breaches [1].

k) When ending employment or getting a different information security role, employees access rights to unnecessary information systems must be terminated or changed.
l) Employees possessing equipment and other resources borrowed or owned by the company must return it and sign deallocation forms when ending their employment.

### 5.3 Asset Management (A.8)

#### 5.3.1 Scope

This policy section targets the IT Management / IT Administration, and all employees of GVT Book Publishing Company. This policy section aims to cover to the entire lifecycle of every company asset, including identification, documentation, ownership, usage, and disposal. The scope covers all types of assets such as mobile devices,

network equipment, desktops, laptops, and removable media. It also includes the establishment and maintenance of an asset inventory system, defining acceptable usage of assets, and the management of ownership and responsibilities related to these assets. The following responsibilities are given to the departments:

a) **Employees**: Required to report misuse of assets and performance issues with assets. Employees must also follow current rules on correct handling of assets.
b) **IT-Management/Administrator**: Responsible for managing ownership of assets. IT must also be responsible for management of removable media and ownership of assets.

### 5.3.2 Identified security risks

When doing the risk assessment, several vulnerabilities were found. There was no performance monitoring, no policy on actions allowed for different assets, and no sufficient tracking of company assets and equipment. Further, there was no adequate system for who is responsible for all different assets. All these vulnerabilities create a risk for loss of information and assets.

### 5.3.3 Inventory of assets

IT management must establish a process for collecting necessary information such as vendor, warranty information and lifecycle information about all the company assets such as mobile devices, network equipment, desktops, and laptops. The documentation needs to be accurate and up to date [1]. The document must be created by:

a) Identifying all relevant company assets.
b) Establish an asset inventory framework.
c) Document all the necessary information about all assets.
d) Add all information to a database and create a management system for the database.

### 5.3.4 Ownership of assets

All the assets maintained in the inventory must be assigned with an owner [1].
The procedure for updating the inventory must be clearly communicated to the appropriate entities such as the IT administrators or IT manager who must:

a) Ensure that all relevant assets are documented.
b) Ensure that the assets are protected.
c) Review access restrictions and classifications.
d) Ensure proper handling of the asset lifecycle.

### 5.3.5 Acceptable use of assets

The company must establish detailed rules and regulations for what the users can or cannot do with the assets. Proper responsibility must be put in place for each asset owner whenever they receive ownership of an asset, as well as a formal procedure on the return of the asset upon employment or contract termination [1].

a) Create digital contracts such as allocation and deallocation forms that contains information about the accepted and non-accepted use of the assets.
b) Upon receiving or returning the asset, the allocation form must be signed by the user and the person allocating the asset such as the IT administrator.
c) The forms must contain information such as asset name, user's name, IT administrators name, and date of receival.

#### 5.3.6 Management of removable media

Use of physical media for transferring company information must be limited to none. In case of business needs, procedures must be put in place and followed by all involved parties [1]. The procedures must follow the given guidelines:

a) If the media is no longer required, the contents must be destroyed and unrecoverable.
b) All media must be stored in a secure environment with control of who has access.
c) Copies of any valuable data must be made on a separate media to reduce the risk of data loss.
d) Media must not be accessed outside of the company office. In case of business needs, this must be approved and there must be a record containing the information about who used the media.

### 5.4 Access control (A.9)

#### 5.4.1 Scope

This policy section targets the IT Management, IT Staff, and all Users. This policy aims to cover the entire process of access control within GVT Book Publishing Company, applying to all users, systems, and data. It includes the management of user accounts, authentication mechanisms, and the assignment and revocation of access rights. The scope covers the establishment of an access control policy, the maintenance of access rights, and the responsibilities of users in maintaining secure access. This policy aims to address vulnerabilities related to user management, shared logins, and ensuring secure and appropriate access to company resources. The following parties have different responsibilities within the access control policy:

a) **Employees**: Adhere to policies on password management. Comply with the given level of access and report any anomalies.
b) **IT Management/staff**: Maintain and manage systems for access control for all parts of the company.

#### 5.4.2 Identified security risks

When doing the risk assessment, several vulnerabilities where found. There is no database for user management and authentication. There is also a problem with having shared login for the travel laptops which can compromise account security.

#### 5.4.3 Access control policy

IT management must establish clear procedures for user access control in all information systems. IT administrators must be responsible for allocating the correct access rights to users and there must be records containing information about the

access rights given, when they were given, and what they cover. The rules must be established on the premise “Everything is generally forbidden unless expressly permitted” [1]. The policy must contain the following:

a) Formal authorization of access requests.
b) Records of access administration and authorization.
c) Regulations for removal of access rights upon termination of employment, contract, or agreement.
d) Formal establishments of what access rights are required for each role in the company.

### 5.4.4 Access control maintenance

Access rights must be monitored and tracked during employment to ensure that no users have unnecessary access. All changes must be logged to ensure proper tracking in case of security breach. Access rights must be reviewed more frequently if they entail access to more sensitive information. All user accounts must also keep logs of access, login, logout timestamps to further secure tracking in case of data breach.

### 5.4.5 Password protection

Passwords used within the company needs to meet certain standards. Password policies must be enforced and implemented to ensure proper protection against brute force attacks. Sufficient passwords management must entail:

a) Strong passwords that they only use within the company.
b) Never disclose passwords to anyone.
c) Updating passwords in accordance with current regulations and on a regular basis.

## 5.5 Physical and environmental security (A.11)

### 5.5.1 Scope

This policy targets the Management, and all employees of GVT Book Publishing Company. It covers all aspects of physical and environmental security measures to protect company assets and personnel from environmental hazards, unauthorized access, and other physical threats. The following parties are responsible for the different parts of the physical and environmental security:

a) **Employees**: are required to report any irregularities in physical security and unauthorized personnel presence.
b) **Management**: is responsible for overseeing and maintaining physical security and access controls.

### 5.5.2 Identified Security Risks

Risk assessment identified several vulnerabilities in our server room, including the presence of flammable materials, lack of a cooling system, shared access with other companies, and a location susceptible to flooding.

### 5.5.3 Physical security

To ensure the protection of assets and staff, the company must:

a) Assign one person to be responsible for staff during emergencies where evacuation of building is necessary.
b) Relocate all premises to areas above the water level of nearby bodies to prevent flooding.
c) Implement comprehensive weatherproofing measures against rain, lightning, and wind.
d) Install fire security systems that minimize damage to electronics.
e) Equip server rooms with appropriate cooling and fire suppression systems.
f) Install fire doors where feasible.

#### 5.5.4 Physical access control

To prevent unauthorized access, the company must:

a) Implement multi-factor authentication for company spaces, combining methods like key cards and PINs, or biometrics and PINs.
b) Maintain an alarm system with access log monitoring.
c) Secure all portable assets in a safe outside office hours.
d) Use physical locks and CCTV surveillance in server rooms.
e) Ensure visitor identification and supervision.

## 5.6 Operations security (A.12)

#### 5.6.1 Scope

This policy section targets the IT Management, IT Staff, and Users within GVT Book Publishing Company. It aims to cover all operational aspects of GVT Book Publishing Company's information systems and processes. It encompasses the establishment and adherence to documented operating procedures, change management, and malware controls, ensuring secure and efficient operations. The following responsibilities are given to the target departments:

a) **IT Management**: Develop and update the operational procedures.
b) **IT Staff**: Keep the documentation up to date and share with users when necessary.
c) **Users**: Adhere to the procedures and guidelines.

#### 5.6.2 Identified security risks

The company currently lacks formal guidelines and procedures for the operation of information systems, posing significant security risks.

#### 5.6.3 Documented Operating Procedures

IT management must develop and maintain comprehensive operating procedures, accessible to IT support teams and users, including:

a) Protocols for computer start-up and shutdown.
b) Guidelines for installing and configuring laptops and desktops.
c) System restart and recovery procedures.
d) Performance monitoring protocols.

### 5.6.4 Change management

Changes in the organization, business processes, information processing facilities and systems that affect information security must be controlled, planned, tested, communicated to all relevant entities and fall-back procedures must be in place for aborting unsuccessful changes [1].

### 5.6.5 Controls against malware

IT management must implement robust anti-malware measures and conduct user training to enhance awareness and skills in protecting assets from malware and responding to infections.

## 5.7 Communication security (A.13)

### 5.7.1 Scope

This policy section applies to the IT Manager, Network Administrator, Security Officer, and All Employees of GVT Book Publishing Company. It aims to cover the security measurements needed to be implied within the network infrastructure of the company. It covers the following responsibilities:

a) **IT Manager**: Accountable for updating network hardware and overseeing the regular patching of network devices. Also responsible for ensuring the implementation of network segmentation and overseeing the overall network security posture.
b) **Network Administrator**: Charged with installing and configuring firewalls, monitoring network traffic, and ensuring compliance with network security protocols. They must also handle the implementation of NAC measures and report any suspicious activities.
c) **All Employees**: Required to adhere to network security protocols and report any anomalies or suspicious activities. They must also be aware of their role in maintaining the security of their network connections and devices.
d) **Security Officer (if applicable)**: Oversees the enforcement of firewall policies and conducts regular reviews to ensure the effectiveness of network security measures.

### 5.7.2 Identified Security Risks

The company's network infrastructure faces several risks due to outdated routers and switches, lack of firewalls and network monitoring, and potential misuse of physical network connections. These vulnerabilities pose risks of network breaches, data interception, and unauthorized access.

### 5.7.3 Network Controls and Security

To ensure a secure company network and prevent attacks:

a) Update network hardware to current security standards and ensure regular security patching.
b) Install business-grade firewalls and integrate network monitoring tools.
c) Secure physical network ports and implement Network Access Control (NAC) measures.
d) Implement network segmentation strategies and use firewalls to protect servers exposed to the external internet.

### 5.7.4 Security of Network Services

To protect the company network from any intrusion:

a) Adopt measures to shield internal networks from external attacks.
b) Establish protocols for monitoring and responding to network threats.

## 5.8 Supplier relationships (A.15)

### 5.8.1 Scope

This policy section applies to the Management and All Employees, as well as all third parties of GVT Book Publishing Company. It covers the following responsibilities:

a) **The company management** must closely monitor the security protocols of all third parties and enforce formal agreements and contracts. They must assign an entity to regularly review and monitor the third parties fulfilment of the contract.
b) **All employees** must follow the procedures outlined for establishing communication with third parties, handling data in accordance with the security protocols, and reporting compliance issues.

### 5.8.2 Identified Security Risks

The company does not have any formal contracts and agreements with third-party vendors. Nor does the company review the security policies of the third-party vendors. This is a high risk for the business due to the potential information leakage through third-party channels and needs to be mitigated completely.

### 5.8.3 Agreements with third parties

The management of the company must establish formal contracts with third parties. The contracts must contain security clauses with agreements on how data must be transferred, handled, and destroyed by the third parties. The management must enforce formal protocols for all employees on how to establish communication and share data with third parties, as well as reporting any compliance issues.

### 5.8.4 Reviewal of third-party policies

The management must conduct formal and regular review of the security policy of the third party, such as their protocols for handling data, their security regulations of how employees are working with the provided sensitive data.

## 5.9 Information security incident management (A.16)

### 5.9.1 Scope

The following section applies to the IT Manager, Incident Response Team, and All Employees within GVT Book Publishing Company, working together to maintain a formal incident management procedure. It covers the following responsibilities:

a) **The company management** must provide regular trainings to the IRT increasing their knowledge in how to handle incidents. They must conduct trainings to the

users educating them on how to report incidents following the formal procedures.

b) **The IT manager** must monitor the SLA's and incidents.
c) **The incident response team (IRT)** must follow the given procedures on how to correctly handle incident calls, as well as uphold the given SLA's. They must educate users, when possible, to decrease the likelihood of reoccurring incidents, in the form of sharing instructions for handling small impact incidents and keeping the instructions up to date.
d) **All company employees** must follow the procedures on how to correctly report incidents, as well as adhering to the SLA's.

### 5.9.2 Identified Security risks

It has been identified that the company does not have any formal procedure for managing and reporting incidents. This poses a great risk for the company when coming across new incidents and disasters. To eliminate these risks, we must take immediate action to create a well-functioning incident response team.

### 5.9.3 Incident Response Team (IRT)

The company must conduct a professional IRT, consisting of an IT manager, IT administrators and IT support-technicians to fulfil the incident response requirements of the company. The IRT must be conducted upon the following requirements:

a) Well defined procedures for how to handle incoming incident calls such as documentation process, escalation procedures, and Service Level Agreements (SLA) for different types of incidents.
b) Well defined procedures for collaborating within different entities of the company and projects conducted, providing clear responsibilities for the respective entities.

## 5.10 Information Security Aspects of Business Continuity Management (A.17)

### 5.10.1 Scope

This policy section applies to the Management, IT Administrators, and All Employees within GVT Book Publishing Company, encompassing the creation, execution, and maintenance of a Business Continuity and Disaster Recovery Plan. The different responsibilities are:

a) **The company management** must work together and look at the security from all aspects and perspectives to develop a well-defined plan, as well as host trainings and drills simulating a disaster and using the plan.
b) **The IT administrators** must work according to all procedures to help mitigate the risks of a disaster.
c) **All employees** must participate in trainings and drills, as well as following the security procedures set by the management.

### 5.10.2 Identified Security Risks

It has been identified that the company currently lacks a comprehensive disaster recovery plan. This gap poses significant risks, including increased business downtime

and potential data loss in the event of an attack or disaster. To eliminate these risks, immediate action is required to develop and implement a robust disaster recovery strategy.

### 5.10.3 Developing a business continuity and disaster recovery plan

Management must actively engage in identifying all potential risks and develop a comprehensive Business Continuity and Disaster Recovery Plan. This plan must address major potential impacts and include strategies for rapid recovery and data preservation. It must be subjected to regular reviews and updates, especially in response to any significant organizational changes or emerging threats.

# 6 General Policies

While the policy primarily focuses on risks identified in the risk assessment, it is also important to address other key security controls from ISO/IEC 27002:2013 [1] that are not covered in chapter 5 of this document. These controls are essential for maintaining a robust security posture and include:

- **Cryptography (A.10):** Implementing and managing cryptographic controls for the protection of information in both storage and transmission of data [1].

    a. Sensitive information managed by the company must be encrypted using regulated cryptographic controls.

- **System Acquisition, Development, and Maintenance (A.14):** Ensuring that information security is an integral part of information systems across their lifecycle [1].

    a. New projects must evaluate risks and implement suitable actions to protect assets.
    b. Rules for safe update and development of software must be established and meet.
    c. Transactions to applications must be protected with adequate methods to maintain the integrity and confidentiality of data.
    d. Development of outsourced software must be monitored.
    e. Testing of software must be in a secure environment and the test data must be adequately protected and controlled.

- **Compliance (A.18)**: Ensuring adherence to information security policies, standards, laws, and regulations. All employees must be educated on the motivation for information security and what consequences data breach or data misuse can lead to [1].
    a. The company's legal responsibilities must be documented and when updated to adhere to any changes.
    b. Methods of storing information must meet legal requirements.
    c. The company information security policy and compliance of-information systems must be reviewed and updated accordingly to meet any changes in laws and regulations.

# 7 GDPR

When the company collects data covered by GDPR [2], certain requirements must be met. Legal basis is always needed for collection of personal data, and when subjects give consent for collection or processing of data, the contract must clearly state what and how the data must be processed. Subjects must always be able to withdraw the consent for any reason and must also have access to information about the data being stored about them.

## 7.1 Handling Employee Data

The company must incorporate the following measurements for handling employee data in regulation with GDPR [2]. The procedures must apply to the security controls for Human Resource Security (A.7), Asset Management (A.8), and Access Control (A.9).

a) GVT Book Publishing Company must ask for consent from any candidate or new employee of the company upon collecting personal data.
b) GVT Book Publishing Company must only collect necessary data, limiting the amount of data collected.
c) GVT Book Publishing Company must protect the data in its lifetime.
d) GVT Book Publishing Company must delete any unnecessary data about an employee in case of any change of employment or contract regarding the employee's role in the company.
e) GVT Book Publishing Company must delete all data about an employee upon termination of employment.

## 7.2 Handling Supplier Data

The company must incorporate the following measurements for handling supplier data in regulation with GDPR [2]. The procedures must apply to the security control for Supplier relationships (A.15).

a) GVT Book Publishing Company must ask for consent from any third-party supplier upon collecting essential data.
b) GVT Book Publishing Company must minimize the amount of data collected and not collect unnecessary data.
c) GVT Book Publishing Company must protect the data in its lifetime.
d) GVT Book Publishing Company must agree with any third-party regarding deletion of data upon agreement.

## Bibliography

[1] ISO/IEC 27002:2013, “Information technology — Security techniques — Code of practice for information security controls,” International Organization for Standardization/International Electrotechnical Commission, Geneva, Switzerland, 2013.

[2] European Parliament and Council of the European Union, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),” Official Journal of the European Union, vol. L119, pp. 1-88, May 2016.