Noureddine Kanzari

ISO/IEC 27002:2022

Master the Essentials of Information Security Controls

Your Path to Achieving ISO/IEC 27001 Certification

Learn How to Avoid Minor and Major Non-Conformities

PART 1/4

Learn by Doing: Practical Guide

About the author

Noureddine Kanzari is a cybersecurity expert with an extensive background in IT risk management and cybersecurity instruction. With a diverse range of certifications that includes being a PECB Certified Trainer, DORA Senior Lead Manager, NIST Cybersecurity Consultant, Senior Lead Incident Manager, Senior Lead SOC 2 Analyst, Data Protection Officer (DPO), DORA Senior Lead Manager, ISO 42001 Senior Lead Auditor, ISO 42001 Senior Lead Implementer, Senior Lead SCADA Security Manager, ISO 22301 Senior Lead Implementer, ISO 22301 Senior Lead Auditor,EBIOS Risk Manager, ISO 27005 Senior Lead Risk Manager, ISO 27001 Senior Lead Implementer, ISO 27001 Senior Lead Auditor, Cisco Certified Specialist in Security Core and Enterprise Core, NSE4 Network Security Professional, Palo Alto Instructor, Devops Tools Engineer, LPIC-3 Enterprise Professional Security, LPIC-3 Enterprise Professional Virtualization & High Availability, LPIC-2, LPIC-1, Suse Certified Linux Administration, and a Certified Security Auditor in computer security,

Noureddine Kanzari's professional journey is characterized by a series of impactful roles and accomplishments. Throughout his career, he has held various pivotal positions, including:

Chief Information Security Officer (CISO)

Audit Team Leader

Cybersecurity Instructor

Technical Manager

Training Manager

His extensive experience and leadership have contributed significantly to enhancing cybersecurity practices, risk management strategies, and organizational resilience.

Contents

1. Introduction

In an era where information is a cornerstone of organizational success, safeguarding it has become a paramount concern. Cyber threats, data breaches, and regulatory demands have escalated, compelling organizations to adopt robust frameworks to protect their information assets. Among the myriad standards available, ISO/IEC 27002:2022 stands out as a globally recognized and authoritative guide for implementing information security controls. This book aims to serve as a comprehensive resource for understanding and applying the 93 essential security controls outlined in ISO/IEC 27002, empowering organizations to build resilient and secure environments.

ISO/IEC 27002 offers detailed recommendations for security controls that organizations can tailor to their specific needs, risk profiles, and operational contexts. These controls are not prescriptive but serve as a flexible blueprint, enabling organizations of all sizes and industries to address their unique security challenges effectively.

The 93 controls in ISO/IEC 27002 are thoughtfully organized into four thematic groups:
Organizational Controls: These focus on governance, policies, and processes that form the backbone of an organization's information security strategy. They address areas such as risk management, compliance, and security roles and responsibilities.

People Controls: Recognizing that human factors are often the weakest link in security, these controls emphasize training, awareness, and personnel management to mitigate risks arising from human behavior.

Physical Controls: These cover the protection of physical assets, facilities, and equipment to prevent unauthorized access, theft, or damage that could compromise information security.

Technological Controls: These address the technical measures, such as encryption, access controls, and system monitoring, that safeguard digital assets and IT infrastructure.

This book is designed to provide a deep dive into each of these controls, offering practical insights into their purpose, implementation, and alignment with the broader objectives of information security.

For each control, we will explore:
What the control entails: A clear explanation of the control's scope, objectives, and relevance to information security.
Implementation guidance: Step-by-step recommendations for applying the control effectively, including best practices, tools, and techniques.
Real-world applications: Case studies and examples illustrating how organizations across industries have successfully adopted the control.
Challenges and considerations: Common pitfalls, resource requirements, and strategies for overcoming obstacles during implementation.

By following the guidelines in ISO/IEC 27002, organizations can not only enhance their security posture but also demonstrate compliance with international standards, build stakeholder trust, and achieve a competitive edge. Whether you are a security professional, an IT manager, a compliance officer, or a business leader, this book will equip you with the knowledge and tools to navigate the complexities of information security.

2. Essential Concepts of Information Security

2.1 Information Security

The term information security is clearly defined in ISO/IEC 27000, which is a standard focused on vocabulary and definitions related to information security.

According to this standard, information security is about preserving three critical aspects of information:

Confidentiality: Making sure that information is only accessible to people, systems, or processes that are authorized. In simple terms, unauthorized users shouldn’t be able to see or access the data.

Integrity: Ensuring that the information remains accurate and complete. It must not be altered in an unauthorized or undetected way.

Availability: Making sure that authorized users can access and use the information whenever they need it.

2.2 Asset

An asset is anything that has value and needs to be protected. For example, a server that stores customer data is an asset. Even the information inside the server is an asset because losing it could cause big problems.

2.3 Integrity

Integrity means making sure information stays correct and unaltered. It’s like writing a message to a friend — you want to be sure that nobody changes your words before your friend reads them. In cybersecurity, we protect integrity to make sure that important data, like bank account numbers, are not changed by accident or by hackers.

2.4 Confidentiality

Confidentiality means keeping information secret from people who are not supposed to see it. Imagine sending a private letter: you don’t want just anyone to read it. In cybersecurity, we protect confidentiality by using passwords, encryption, and access controls.

2.5 availability

Availability means making sure that information is accessible when needed. It’s like having a 24/7 grocery store: you expect it to be open whenever you need it. In cybersecurity, we use backup systems, and protection against attacks to keep information and systems available at all times.

2.6 Vulnerability

A vulnerability is a weakness that can be exploited. Imagine leaving your house door unlocked: that's a vulnerability because someone could walk in easily. In cybersecurity, vulnerabilities could be outdated software, weak passwords, or missing updates, which hackers can use to get into systems.

2.7 Threat

A threat is anything that can cause harm to your information or assets. It's like a thief planning to break into your house. In cybersecurity, threats include hackers trying to steal data, viruses damaging computers, or even natural events like floods that destroy servers.

2.8 Impact

Impact is the damage or harm caused if a threat succeeds. For example, if a hacker steals a company's customer list, the impact could be loss of customer trust, financial losses, and legal problems. In simple words, the bigger the impact, the more serious the consequences.

2.9 Security Objectives

Security objectives are the goals we want to achieve, like keeping information secret or making sure it is always available.

2.10 Classification of Security Measures

Security measures can be grouped into types, like technical (firewalls, antivirus), organizational (security policies, training employees), or physical (locks, cameras). For example, using a password is a technical measure, while teaching employees not to click on suspicious links is an organizational measure.

3. Security Objectives and Their Corresponding Controls

In information security management, it is essential to link security objectives (what we want to achieve) to appropriate security controls (what we implement to achieve it). The ISO/IEC 27002:2022 standard provides clear guidance by offering controls aligned with these objectives.

The table below presents 10 simple examples showing how a security objective leads to the selection of specific controls:

Security Objective	What We Want (Goal)	Example Controls	ISO/IEC 27002 Clause	Text (Simplified)
Protect sensitive information	Make sure sensitive info is protected	Information classification and handling rules	5.12	Information must be classified and handled according to its importance.
Manage access to systems	Only authorized people access systems	Access control policies, user access management	5.15	Access must be limited based on needs and job roles.
Protect against malware	Avoid infection by viruses and malware	Install antivirus, update systems	8.7	Malware protection must be used and kept up-to-date.
Backup important data	Prevent data loss	Regular backups, restore testing	8.13	Important data must be regularly backed up and tested for recovery.
Secure mobile devices	Protect phones and laptops outside the office	Mobile device policies, encryption	6.2	Devices must be protected against loss, theft, or misuse.
Ensure secure communications	Keep communications private and safe	Use encryption for emails and chats	8.23	Protect information in networks and communication links.
Manage changes safely	Avoid errors when changing systems	Change management procedures	8.32	Changes must be controlled and tested before being applied.
Protect user passwords	Make passwords strong and safe	Password rules, multi-factor authentication	8.3	Use strong passwords and protect authentication information.
Monitor system activities	Detect problems early	System monitoring, audit logs	8.15	Activities must be monitored to detect and respond to incidents.
Control supplier risks	Make sure suppliers protect information too	Supplier security agreements	5.19	Risks from suppliers must be identified and managed properly.

4. Understanding ISO/IEC 27002 Controls

In information security, a control is a safeguard or a countermeasure that helps to manage risks to information. ISO/IEC 27002:2022 organizes controls into different types depending on how they protect information. Understanding these types helps you choose the right control for each risk you face. This standard provides a comprehensive set of guidelines for implementing information security controls across various domains within an organization. The controls are categorized into four main types: Organizational, People, Physical, and Technological:

4.1 Organizational Controls

Organizational controls focus on the policies, procedures, and management practices that ensure information security is integrated into the organization's operations.

Example Control from ISO/IEC 27002:

Information Security Policy (Control 5.1): Organizations must define, approve, publish, and communicate security policies. Developing a clear policy that outlines the organization's commitment to information security, including roles and responsibilities.

4.2 People Controls

People controls address the human aspects of information security, including training, awareness, and personnel management.

Example Control from ISO/IEC 27002:

Information Security Awareness, Education and Training (Control 6.3): Conducting regular training sessions for employees on recognizing phishing emails, reporting security incidents, and understanding their role in maintaining information security. All employees must be trained on security risks and good practices.

4.3 Physical Controls

Physical controls focus on protecting the physical environment where information is processed, stored, and transmitted. Physical controls protect buildings, servers, devices, and documents from physical threats like theft, fire, or unauthorized access.

Example Control from ISO/IEC 27002:

Physical Security Perimeter (Clause 7.1): Security perimeters must be defined and used to protect areas containing information and other associated assets.

4.4 Technological Controls

Example Control from ISO/IEC 27002:

Technological controls involve the use of technology to protect information and systems from threats and vulnerabilities.

Cryptography (Control 8.24): Encrypting sensitive data both at rest and in transit to prevent unauthorized access, even if the data is intercepted, and regularly reviewing and updating encryption algorithms.

5. Preventive, Detective, and Corrective controls

The ISO/IEC 27002 standard provides essential guidelines for implementing information security controls within organizations. It structures these controls into four main categories: organizational controls, people-related controls, physical controls, and technological controls.

However, it is also crucial to understand that these controls can be classified from another perspective: preventive, detective, and corrective measures. This dual classification helps better understand how each control contributes to overall information security. In information security, protective measures are classified into three main types based on their purpose:

Organizational Controls (Section 5) include policies and procedures that define how the organization manages information security. These controls are often **preventive**, as they aim to establish rules and practices that prevent security incidents before they occur.

People-Related Controls (Section 6) focus on training, awareness, and human resource management. They can be both **preventive**, by training employees to recognize threats, and **detective**, by encouraging the reporting of suspicious incidents.

Physical Controls (Section 7) protect the physical environments where information is processed and stored. These controls are primarily **preventive**, by preventing unauthorized access, but can also include **detective** measures such as surveillance systems.

Technological Controls (Section 8) use tools and technologies to secure information and systems. They encompass **preventive** measures (such as encryption), **detective** measures (such as intrusion detection systems), and **corrective** measures (such as incident response plans).

By combining these two classification approaches, we obtain a comprehensive and integrated view of information security. Preventive measures aim to prevent incidents, detective measures enable rapid identification of incidents, and corrective measures intervene to limit damage and restore normalcy.

6. Information Security Management System (ISMS)

An Information Security Management System (ISMS) is a structured framework that helps an organization protect its information assets through policies, procedures, guidelines, resources, and activities.

It is managed systematically with the goal of managing risks and ensuring information security across the organization.

Then an ISMS includes:

- Policies (rules about protecting information),
- Procedures (detailed steps to follow),
- Resources (people, technology, …),
- Activities (risk assessments, training, monitoring …).

The main international standard for ISMS is ISO/IEC 27001.

When a company wants to implement and even certify its ISMS, it must follow ISO/IEC 27001 requirements. These requirements cover many key areas, such as:

- Risk assessment and risk treatment plans,
- Setting information security objectives,
- Top management's commitment,
- Documenting the ISMS (policies, records, reports),
- Performing internal audits and management reviews,
- Managing nonconformities,
- Measuring and improving performance

ISO/IEC 27001 includes a list of security controls (found in Annex A). These controls help organizations protect against threats to confidentiality, integrity, and availability of information. However the controls in ISO/IEC 27001 are written briefly, they do not provide detailed explanations. That's why organizations also use ISO/IEC 27002, a guidance standard that explains each control in more detail and gives practical advice on how to implement the controls properly.

By following ISO/IEC 27001 requirements and applying the guidance of ISO/IEC 27002, organizations can protect their valuable information assets efficiently and continuously improve their security posture.

7. ISO/IEC 27002 clauses

This standard guides organizations on how to implement security controls effectively. ISO/IEC 27002 is a best practices guide that explains in detail the security controls listed briefly in ISO/IEC 27001.

It helps organizations choose, implement, and manage security measures in a practical and structured way.

ISO/IEC 27002 organizes its security controls into four major categories, covering all important aspects of information security:

Category	Number of Controls	Focus Area
Organizational Controls	37 controls	Company-wide policies, processes, governance (e.g., risk management, supplier relationships, roles and responsibilities).
People Controls	8 controls	Measures focused on employees and contractors (e.g., training, background checks, and awareness).
Physical Controls	14 controls	Protection of physical environments (e.g., offices, data centers, equipment security, access restrictions).
Technological Controls	34 controls	Protection using technology (e.g., encryption, access control systems, network security, software updates).

Each ISO/IEC 27002 control comes with attributes that explain:

- **Control type**: When it acts (Preventive, Detective, Corrective),
- **Information security properties:** What security property it protects (Confidentiality, Integrity, Availability),
- **Cybersecurity concepts:** Which phase of cybersecurity it supports (Identify, Protect, Detect, Respond, Recover),
- **Optional capabilities:** Which operational area it belongs to (Governance, Physical security, Access management, etc.),
- **Security domains:** Which domain it relates to (Governance, Protection, Defence, and Resilience).

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Preventive Detective Corrective	Confidentiality Integrity Availability	Identify Protect Detect Respond Recover	Governance Asset management Information protection Human resource security Physical security System and network security Application security Secure configuration Identity and access management Threat and vulnerability management Continuity Supplier relationships security Legal and compliance Information security event management Information security assurance	Governance and ecosystem Protection Defence Resilience

Scenario: you run a small online store. One of the risks you face is the potential for customer credit card information to be stolen during a transaction

Attribute Type	What it Means	Example for Online Store
1. Control Type	WHEN the control acts: before, during, or after an incident.	° **Preventive:** Using SSL/TLS encryption to protect data before theft occurs. ° **Detective:** Monitoring transactions to catch suspicious activity. ° **Corrective:** Resetting passwords after a breach.
2. Information Security Properties	WHAT you want to protect: confidentiality, integrity, availability.	° **Confidentiality:** Protecting customer credit card info.
3. Cybersecurity Concepts	WHICH phase of security the control helps: Identify, Protect, Detect, Respond, Recover.	° **Identify:** Knowing where customer data is stored. ° **Protect:** Encrypting credit card details. ° **Detect:** Setting alerts for unusual purchases. ° **Respond:** Acting quickly if a theft happens. ° **Recover:** Restoring service after an attack.
4. Operational Capabilities	Which specific operational area the control belongs to.	° **Asset Management:** List and protect systems that store credit cards. ° **System and Network Security:** Secure your online checkout page. ° **Identity and Access Management:** Only allow authorized employees access to customer data.
5. Security Domains	The broader expertise area: Governance, Protection, Defense, Resilience.	° **Protection:** Making sure customer data cannot be stolen. ° **Defense:** Detecting attacks as they happen. ° **Resilience:** Recovering quickly from a security incident. ° **Governance:** Having clear security rules and responsibilities.

Then every time you want to protect something in your online store:

Step	Question	Example
1	When should I act? (Control Type)	Before the hack happens (Preventive)
2	What should I protect? (Security Property)	Confidentiality of credit cards
3	Which phase am I in? (Cybersecurity Concept)	Protect phase
4	Which part of operations? (Operational Capability)	Secure the network and systems
5	Which expertise area? (Security Domain)	Protection

When choosing a security control in ISO/IEC 27002, the five attributes help you quickly filter the best option based on your risk. First, the control type (preventive, detective, or corrective) tells you whether you need to stop, detect, or fix a threat. Then, the information security property (confidentiality, integrity, availability) helps you focus on protecting what matters most, like keeping customer data secret. The cybersecurity concept (identify, protect, detect, respond, recover) guides you to the right stage of protection. Operational capabilities, such as system and network security or asset management, direct you to the correct technical area. Finally, security domains (protection, defense, resilience, governance) show you the broader family of controls. For example, if you run an online store and want to protect customer credit cards, you would filter for preventive controls focused on confidentiality, protection, and system security — such as encrypting transactions with HTTPS.

It's important to know that not all controls need to be chosen — for example, if your organization doesn't develop software, you don't need to apply controls related to secure software development. You should only select controls that are relevant to your activities and your risks. For instance, in a small online store, focusing on customer data protection and payment system security is much more critical than managing development environments.

8. Steps to Select Security Controls

8.1. Define the Scope (What do you want to protect?)

Goal: Identify which parts of your organization are covered by information security.

How to do it:

- List your organization’s main activities.
- Define which information, systems, processes, and locations need protection.

Examples:

An online store → **scope** = website, customer database, payment system.

8.2. Assess the Risks (What could go wrong?)

Goal: Understand the threats, vulnerabilities, and impacts related to your assets.

How to do it:

- Identify the risks for each important asset.
- Evaluate for each risk:
  - How likely is it to happen?
  - What would be the impact if it happened?

Examples:

Online store: Risk = credit card theft → impact = loss of customers, GDPR fines.

8.3. Define Security Objectives (What do you want to achieve?)

Goal: Clarify what you want to protect for each identified risk.

How to do it:

- Set clear objectives to reduce or eliminate risks.

Examples:

Online store: "Protect the confidentiality of customer payment information."

8.4. Choose ISO/IEC 27002 Security Controls (How will you achieve it?)

Goal: Select appropriate controls from ISO/IEC 27002 to achieve your objectives.

How to do it:

- Review the 93 controls of ISO/IEC 27002.
- Select only controls relevant to your scope, activities, and risks.
- Use the 5 attributes to filter:
  - Type of control (preventive, detective, corrective)
  - Information properties (confidentiality, integrity, availability)
  - Cybersecurity concepts (identify, protect, detect, respond, recover)
  - Operational capabilities (access management, physical security, etc.)
  - Security domains (governance, protection, defense, resilience)

Examples:

Online store:

- Risk: Credit card theft
- Objective: Secure payment information
- Controls selected: Access control (A.5.15) + Data encryption (A.8.24)

8.5. Document and Justify Control Selection

Goal: Clearly explain why each control was selected, linking it to risks and objectives.

How to do it:

For each selected control, document:

- The identified risk,
- The security objective,
- The ISO/IEC 27002 control selected,
- The reason for choosing it.

9. Business Scenario: "Tech Solutions" organization

The business scenario "Tech Solutions" will serve as the basis for our case study. Through this study, we will show you how to choose and apply the security measures outlined in the ISO 27002 standard.

Objectives of the Case Study

- Identifying Risks:

  We will start by identifying the specific risks that SafeTech Solutions faces, taking into account the security constraints and challenges mentioned.

- Defining Security Objectives:

  For each identified risk, we will define clear security objectives aimed at reducing or eliminating these risks.

- Selecting Security Controls:

  We will select the appropriate security controls from the ISO 27002 standard that meet the defined security objectives.

  For example, to protect health data, we might choose controls related to cryptography and access management.

- Applying the Controls:

  We will explain how to practically apply these controls within the context of SafeTech Solutions. This will include concrete examples of implementation, such as configuring firewalls, using VPNs to secure remote connections, and establishing security policies for remote work.

- Continuous Evaluation and Improvement:

  Finally, we will discuss the importance of continuously evaluating security controls and improving measures based on the results obtained and the evolving nature of threats.

Company Overview:

- Name: Tech Solutions
- Size: 100 employees
- Business Sectors:
  - Software development (mobile and web applications for the medical sector)
  - Secure cloud hosting for clients
  - Online sales of its own solutions
- Target Audience: Hospitals, private clinics, analytical laboratories
- Location: 2 physical offices + internally hosted servers and servers in an external data center

Key Infrastructures and Elements:

- Departments:
  - General Management
  - IT Development
  - Customer Support
  - Human Resources
  - Sales and Marketing
  - IT Infrastructure (Servers, Networks)
  - Information Security and Compliance

Resources:

- Critical Applications (Online Medical Platform)
- Customer Database Containing Sensitive Medical Data
- Financial Systems for Billing and Payments
- Internal Networks and VPN
- E-commerce Website
- Internal Servers (for Development) and Cloud Servers (for Client Hosting)
- Mobility: Remote Work for 40% of the Workforce

Security Constraints and Challenges:

- Protection of Health Data (Legal Obligation - GDPR and HIPAA)
- Maintaining the Availability of Cloud Services (Demanding Client Contracts)
- Confidentiality of Source Code and Ongoing Projects
- Regulatory Compliance with ISO 27001, NIS 2
- Software Development Security (DevSecOps)
- Securing Remote Work and Mobile Devices
- Physical Security of Premises and Internal Data Center

10. ORGANIZATIONAL CONTROLS

5.1 Policies for information security

Control description:

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventif	• Confidentialité • Intégrité • Disponibilité	Identifier	Gouvernance	• Gouvernance et Écosystème • Résilience

Control attributes:

- **Control type:** When it acts : Preventive
- **Information security properties:** Confidentiality, Integrity, Availability
- **Cybersecurity concepts:** Which phase of cybersecurity it supports : Identify
- **Optional capabilities:** Which operational area it belongs to : Governance
- **Security domains:** Which domain it relates to : Governance et Écosystème, Resilience

Control requirement:

1. **Define the policies**
   - Organizations must create a general Information Security Policy (main rules and principles)
   - And create detailed, topic-specific policies (e.g., acceptable use, access control, remote work, etc.).
2. **Get management approval**
   - Policies must be formally approved by top management
3. **Publish the policies**
   - Once approved, policies must be formally documented

4. **Communicate the policies**

   ➢ Organizations must actively communicate these policies to all relevant employees and sometimes to external interested parties (contractors, partners, etc.).

5. **Acknowledge**

   ➢ Personnel and relevant interested parties must acknowledge they have received and understood the policies (e.g., through a signed form, email confirmation, training attendance).

6. **Review the policies**

   ➢ Policies should be regularly reviewed:

   - At planned intervals (e.g., every year)
   - When significant changes happen (e.g., changes in organization, risks, laws, or technologies).

The policy should consider three important sources:

a) Business strategy and requirements

➔ The policy must support the organization's business goals.

b) Regulations, legislation, and contracts

➔ It must comply with laws, regulations, and obligations in contracts (for example: GDPR, industry standards, clients' security requirements).

c) Current and projected risks and threats

➔ It should be based on the organization's risk environment (what risks exist today and what could appear in the future).

The policy should contain statements that address the following points:

a) Definition of information security

➔ Explain what "information security" means for the organization (usually: protecting confidentiality, integrity, availability).

b) Information security objectives or the framework for setting them

➔ Either define the security goals directly or describe how goals will be set later.

c) Principles to guide all activities

➔ High-level rules to be followed in all information security efforts (like "risk-based approach," "least privilege," "security by design").

d) Commitment to satisfy applicable requirements

➔ A promise to follow laws, regulations, and other mandatory obligations regarding security.

e) Commitment to continual improvement

➔ A promise to keep improving the Information Security Management System (ISMS) over time.

f) Assignment of responsibilities

➔ Clarify who is responsible for information security (roles, not just job titles).

g) Procedures for handling exemptions and exceptions

➔ Define how to formally request and approve exceptions to security rules when needed.

The organization must have a main information security policy — like a "big guide" that explains the overall security rules.

But the big guide is not enough. So, we also need to create smaller, more detailed policies about specific security topics — topic-specific policies — to give clearer instructions for certain groups of people or areas.

These smaller policies must match the main security policy and support it, not contradict it.

Examples of specific topics for these smaller policies are:

- Who can access what (Access control)
- How to protect buildings and equipment (Physical security)
- How to manage company assets like laptops and phones (Asset management)
- How to transfer information safely (Information transfer)
- How to configure and protect user devices (Secure configuration)
- How to protect networks (Network security)
- How to handle security incidents (Incident management)
- How to back up important data (Backup)
- How to use encryption (Cryptography)
- How to classify and handle information (Information classification)
- How to fix technical problems quickly (Vulnerability management)
- How to develop software securely (Secure development)

The main security policy is the "big picture," and topic-specific policies are the "detailed rules" for particular needs. They all must work together to keep information safe.

The policies must be written in a way that is easy to read, easy to find, and understandable.

If the policies are sent outside the company, be very careful not to accidentally share confidential information.

The Information Security Policy (Main Policy) is written down clearly, explaining the organization's overall security goals, principles, and commitments. Formally approved by Top Management. The highest leaders (like CEO, CIO, and Board) must officially review and approve it, showing that security is a serious priority for the whole organization.

The topic-Specific Policies (Detailed Policies like password policy, remote work policy, etc.) is documented for each specific area (like access control, email use). These are approved by managers who are responsible for that specific area, for example: The IT manager may approve the password policy. The HR manager may approve the employee onboarding security policy.

Checks to be performed	Evidence
➢ If there is an approved Information Security Policy (ISP) by management ➢ If the ISP is supplemented by specific complementary policies ➢ If the ISP and specific policies are published and communicated to relevant personnel and stakeholders ➢ If recipients of the policies are required to confirm their understanding of these policies and agree to comply with them when applicable ➢ If the ISP is reviewed at planned intervals or when significant changes occur to ensure that the ISP and specific policies remain relevant, adequate, and effective.	➢ Approved Information Security Policy (ISP) document by the General Management ➢ Approved specific policy documents by the appropriate management level ➢ Sample acknowledgments (or emails) confirming that users have received a copy of the ISP or applicable specific policies, with confirmation of their understanding of these policies and acceptance to comply with them ➢ History of ISP and specific policy updates

In a company (or "organization"), to protect information, we create rules called policies. These policies are organized into three levels:

- General high-level policies (strategic):
  - These are the big-picture rules about how the organization will protect information.

  Example:

  "We want to protect all important information to avoid any interruption of our activities."

  It gives a vision or a framework, but without detailed instructions.

- High-level policies on specific topics (tactical):
  - These are more specific rules, focused on a particular subject (like computers, employee security, etc.).
  - They must follow the general policy.

  Example:

  "We will require strong passwords on all computers."

  It explains how to protect a specific area (here, computers).

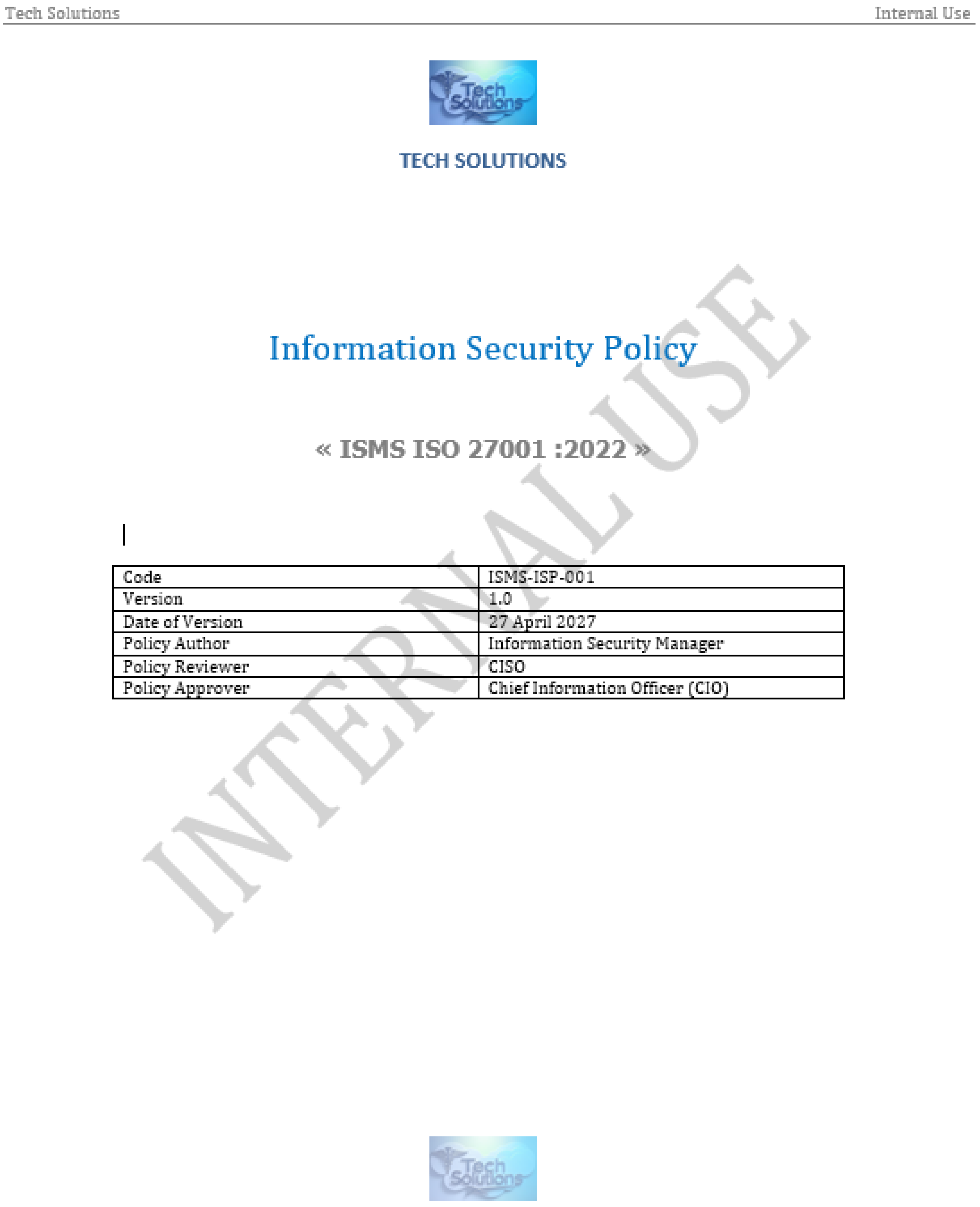
- Detailed policies (operational)
  - These are the very detailed rules that employees must follow every day.
  - They explain exactly what to do and how to do it.

  Example:

  "Passwords must have at least 12 characters, including letters, numbers, and symbols. They must be changed every 3 months."

→While the final signature on the security policy might come from an individual (usually the CEO), the actual approval process for the policy can involve a group or committee within the organization, such as the Board of Directors, the Management Board, or a specific committee focused on security governance. This ensures that the policy has been reviewed and endorsed by the right people or groups within the organization before it is finalized.

5.2 Practical Application of Clause 5.1: Case Study



Tech Solutions Internal Use

TECH SOLUTIONS

Information Security Policy

« ISMS ISO 27001 :2022 »

Code	ISMS-ISP-001
Version	1.0
Date of Version	27 April 2027
Policy Author	Information Security Manager
Policy Reviewer	CISO
Policy Approver	Chief Information Officer (CIO)

Contents

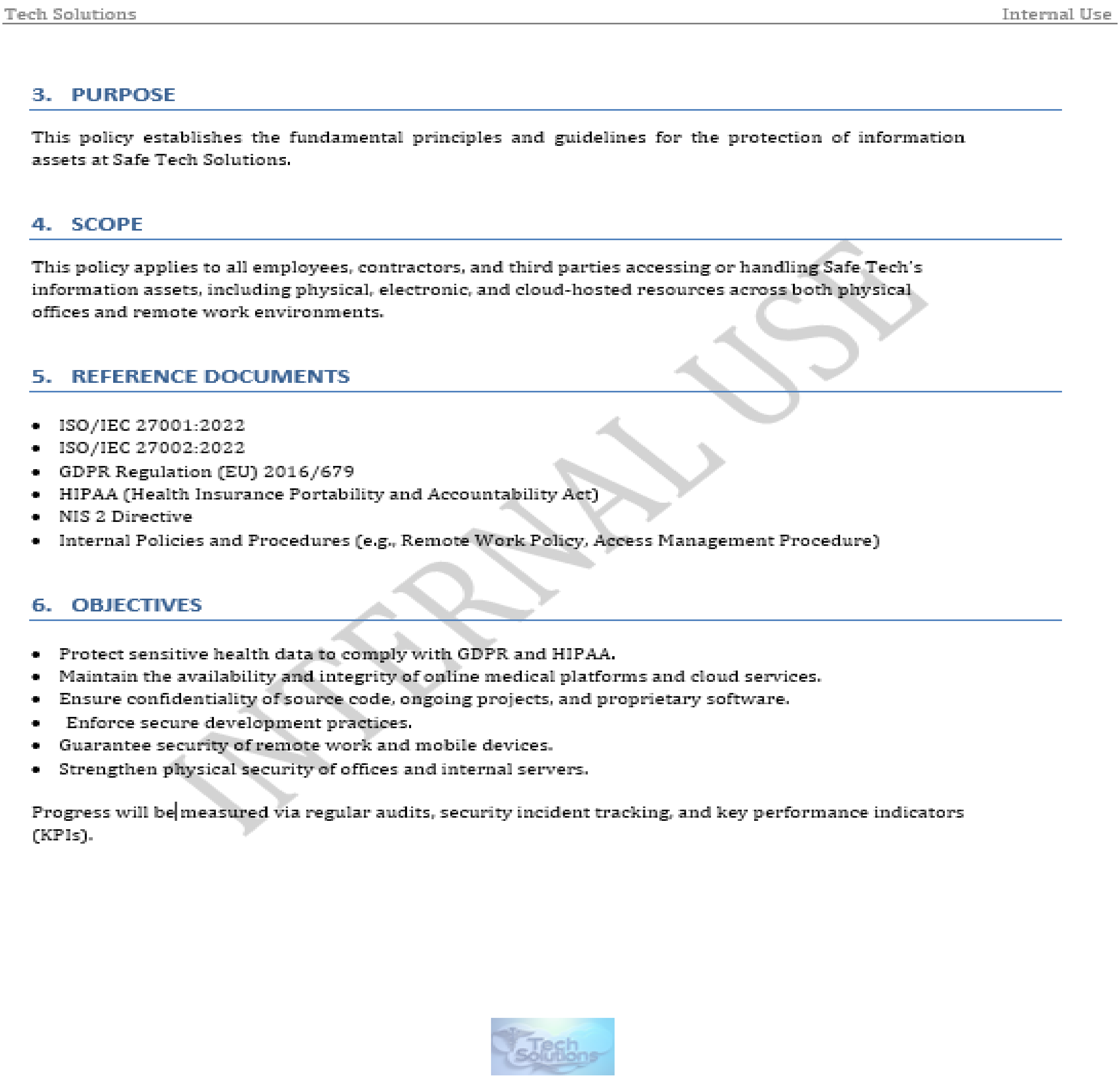
1. Copyright

This documentation contains information regarding the activities, structures, and systems of Tech Solutions. It is protected under intellectual property laws and is subject to strict restrictions regarding its use, reproduction, and distribution.

Any reproduction, whether total or partial, by any means (copying, scanning, recording, transcription, or otherwise) without the prior written consent of Tech Solutions is strictly prohibited.

2. Change History

Version	Date	Action	Created by
1.0	27 April 2025	Basic Document	Information Security Manager



3. PURPOSE

This policy establishes the fundamental principles and guidelines for the protection of information assets at Safe Tech Solutions.

4. SCOPE

This policy applies to all employees, contractors, and third parties accessing or handling Safe Tech's information assets, including physical, electronic, and cloud-hosted resources across both physical offices and remote work environments.

5. REFERENCE DOCUMENTS

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- GDPR Regulation (EU) 2016/679
- HIPAA (Health Insurance Portability and Accountability Act)
- NIS 2 Directive
- Internal Policies and Procedures (e.g., Remote Work Policy, Access Management Procedure)

6. OBJECTIVES

- Protect sensitive health data to comply with GDPR and HIPAA.
- Maintain the availability and integrity of online medical platforms and cloud services.
- Ensure confidentiality of source code, ongoing projects, and proprietary software.
- Enforce secure development practices.
- Guarantee security of remote work and mobile devices.
- Strengthen physical security of offices and internal servers.

Progress will be measured via regular audits, security incident tracking, and key performance indicators (KPIs).

7. INFORMATION SECURITY PRINCIPLES

Tech Solutions commits to protecting information assets by maintaining:

- **Confidentiality:** Ensuring information is accessible only to authorized individuals.
- **Integrity:** Safeguarding the accuracy and completeness of information and systems.
- **Availability:** Ensuring that authorized users have reliable access to information when needed._

8. RESPONSIBILITIES

- Management: Ensure enforcement and resourcing of security initiatives.
- Employees: Comply with security practices and participate in trainings.
- Information Security Officer: Monitor risks, incidents, and propose improvements.
- Top Management: Formally approve policies and oversee compliance.
- Data Owners: Define data classification, access rights, protection needs, and ensure regulatory compliance
- System Owners: Ensure secure system configuration, availability, access control implementation, and incident response.
- Application Owners: Oversee application security, enforce access control, ensure compliance, and manage application lifecycle.

9. POLICY COMMUNICATION

The policy is communicated to all staff through onboarding sessions, periodic trainings, internal newsletters, and is available via the company's intranet. Relevant external parties (contractors, partners) are also informed when necessary.

10. VALIDITY AND DOCUMENT MANAGEMENT

This policy is reviewed annually or when significant changes occur (organizational changes, emerging risks, legal updates).

Next review date: 27/04/2026.

11. ACKNOWLEDGMENT

All employees and relevant external parties must acknowledge receipt and understanding of this policy by signing a formal acknowledgment form or electronic confirmation.

5.3 Information security roles and responsibilities

Control description:

Information security roles and responsibilities should be defined and allocated according to the organization needs.

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventif	• Confidentialité • Intégrité • Disponibilité	Identifier	Gouvernance	• Gouvernance et Écosystème • Protection • Résilience

Control attributes:

- **Control type:** When it acts : Preventive
- **Information security properties:** Confidentiality, Integrity, Availability
- **Cybersecurity concepts:** Which phase of cybersecurity it supports : Identify
- **Optional capabilities:** Which operational area it belongs to : Governance
- **Security domains:** Which domain it relates to : Governance et Écosystème, Protection, Resilience

Control requirement:

Every company must clearly decide who is responsible for protecting information and managing security. These roles must fit the company's real needs, and be based on its security rules (the security policy):

- Define clearly who does what for information security.
- Assign people specific security jobs (and not leave it to chance).
- Make sure everyone understands their responsibilities.

Give the right people the right security jobs and make sure everyone knows what they must do to keep information safe:

- **Top Management Decisions:**

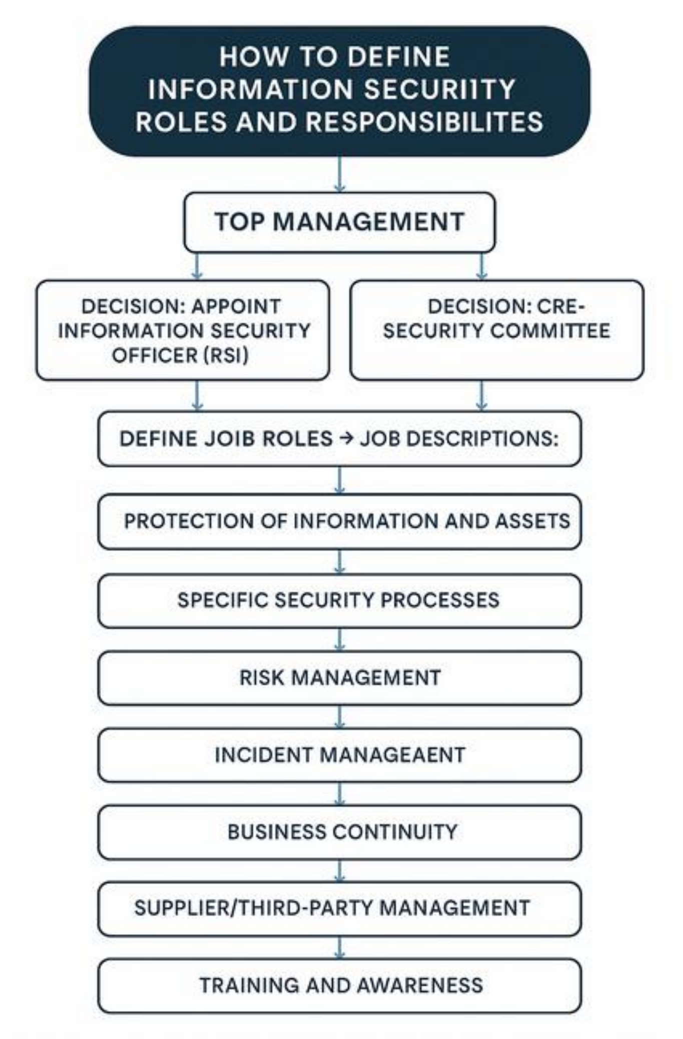
- Officially appoint an Information Security Officer (RSO).
- Form a Security Committee to oversee security matters.

- **Define Roles Clearly:**

- Create detailed job descriptions including each person's security tasks.

- **Assign Key Security Responsibilities:**

- Protect information and IT assets.
- Execute and manage specific security activities.
- Manage and approve security risks and residual risks.
- Train and guide all personnel on security best practices.
- …

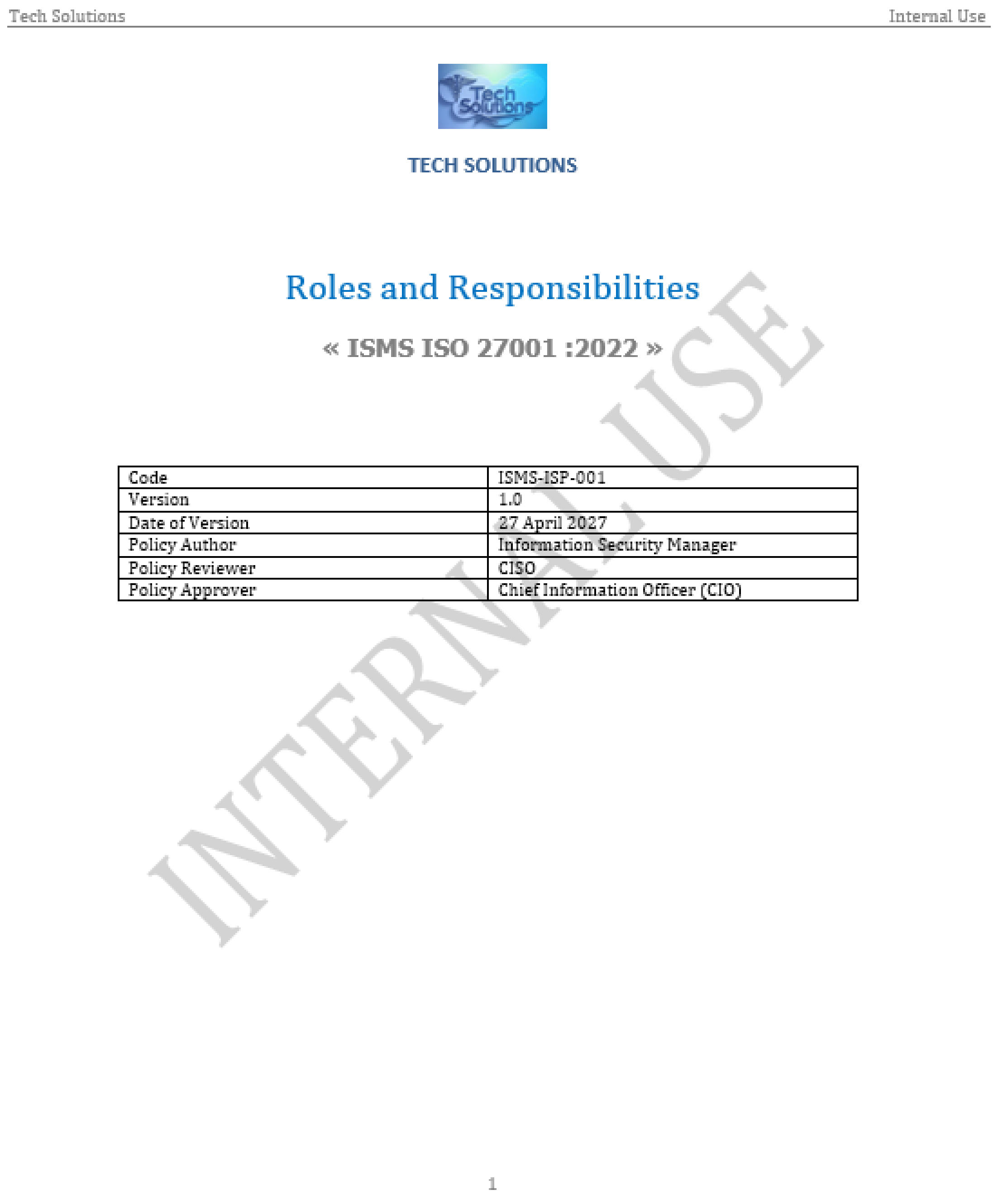

HOW TO DEFINE INFORMATION SECURIITY ROLES AND RESPONSIBILITES
TOP MANAGEMENT
DECISION: APPOINT INFORMATION SECURITY OFFICER (RSI)
DECISION: CRE- SECURITY COMMITTEE
DEFINE JOIB ROLES → JOB DESCRIPTIONS:
PROTECTION OF INFORMATION AND ASSETS
SPECIFIC SECURITY PROCESSES
RISK MANAGEMENT
INCIDENT MANAGEAENT
BUSINESS CONTINUITY
SUPPLIER/THIRD-PARTY MANAGEMENT
TRAINING AND AWARENESS

Checks to be performed	Evidence
➢ If an Information Security Officer (RSO), vested with decision-making authority and reporting directly to top management, is appointed. ➢ If a Security Committee is established. ➢ If information security roles and responsibilities are clearly defined and assigned to individuals with the required competencies	➢ Decision to appoint the Information Security Officer (RSO) ➢ Decision to establish the Security Committee ➢ Job descriptions

5.4 Practical Application of Clause 5.2: Case Study

This following document defines the roles, responsibilities, and authority within the Information Security Management System (ISMS) at Tech Solutions, based on ISO/IEC 27001:2022 requirements.

It identifies the key actors such as Top Management, Information Security Officer, Security Committee, Internal ISMS Auditor, and ISMS Manager and clearly details their actions for maintaining, monitoring, and continuously improving the ISMS.



Tech Solutions Internal Use

TECH SOLUTIONS

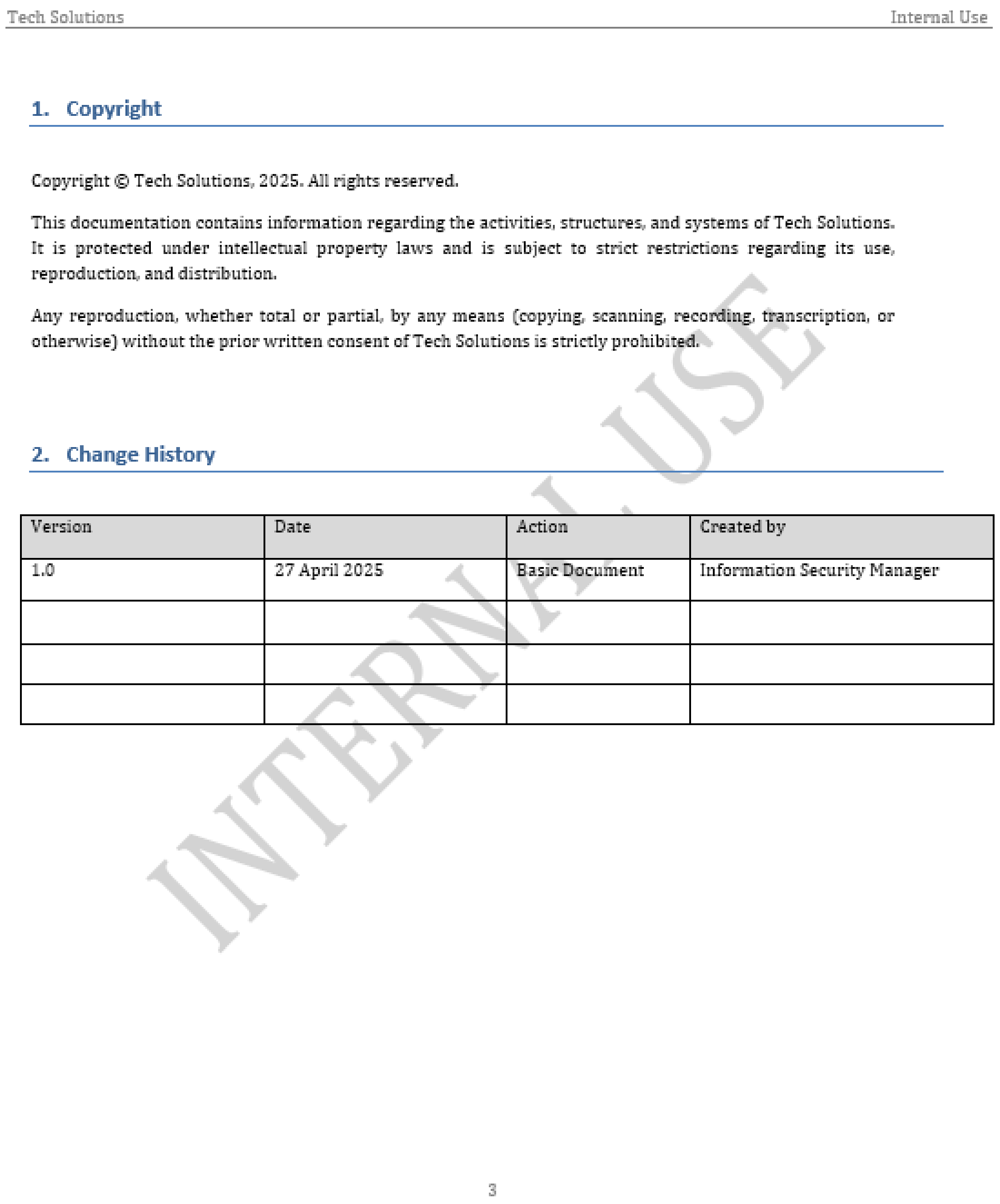
Roles and Responsibilities

« ISMS ISO 27001 :2022 »

Code	ISMS-ISP-001
Version	1.0
Date of Version	27 April 2027
Policy Author	Information Security Manager
Policy Reviewer	CISO
Policy Approver	Chief Information Officer (CIO)

1

Contents



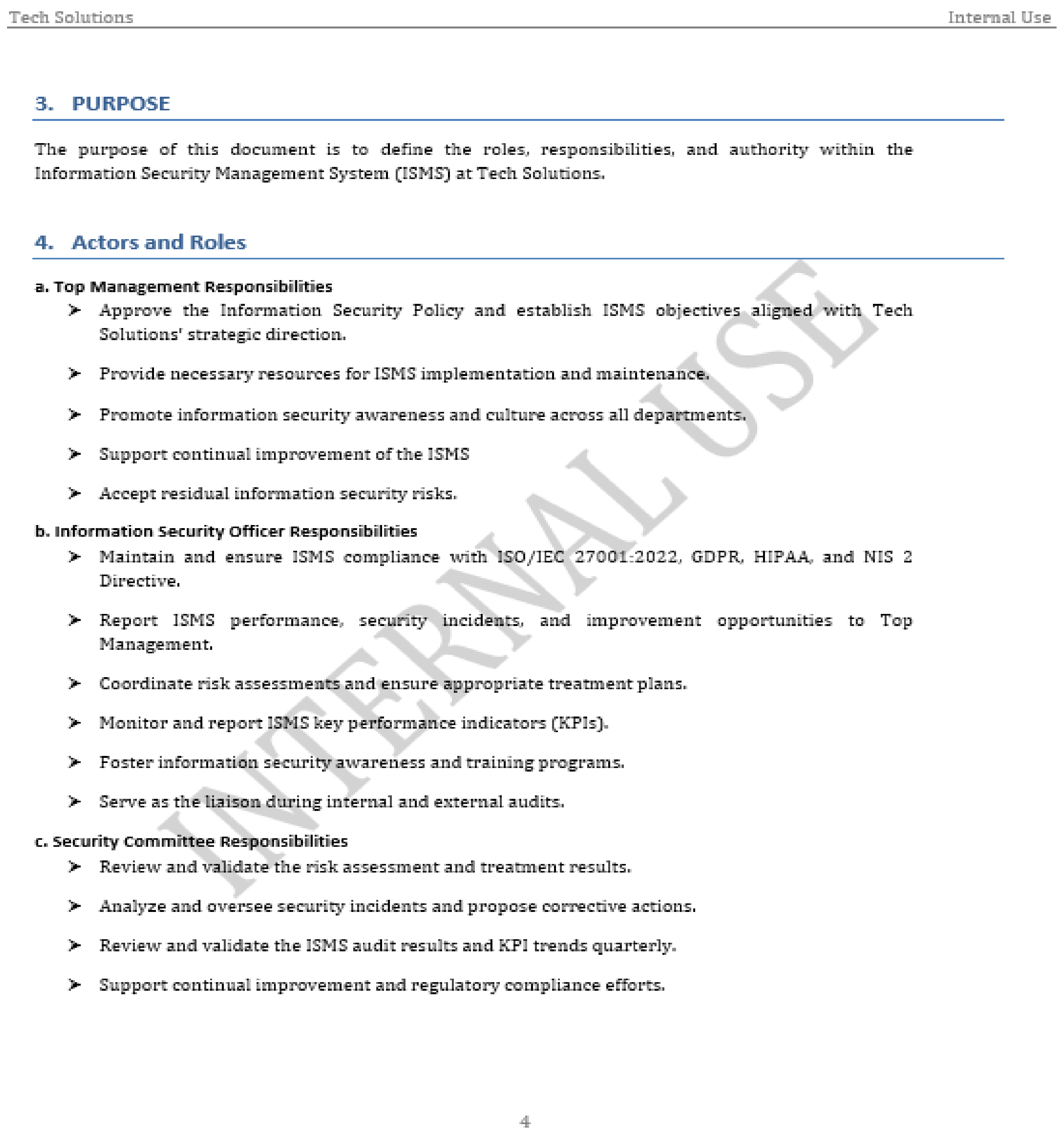
1. Copyright

This documentation contains information regarding the activities, structures, and systems of Tech Solutions. It is protected under intellectual property laws and is subject to strict restrictions regarding its use, reproduction, and distribution.

Any reproduction, whether total or partial, by any means (copying, scanning, recording, transcription, or otherwise) without the prior written consent of Tech Solutions is strictly prohibited.

2. Change History

Version	Date	Action	Created by
1.0	27 April 2025	Basic Document	Information Security Manager



Tech Solutions Internal Use

3. PURPOSE

The purpose of this document is to define the roles, responsibilities, and authority within the Information Security Management System (ISMS) at Tech Solutions.

4. Actors and Roles

a. Top Management Responsibilities

- Approve the Information Security Policy and establish ISMS objectives aligned with Tech Solutions' strategic direction.
- Provide necessary resources for ISMS implementation and maintenance.
- Promote information security awareness and culture across all departments.
- Support continual improvement of the ISMS
- Accept residual information security risks.

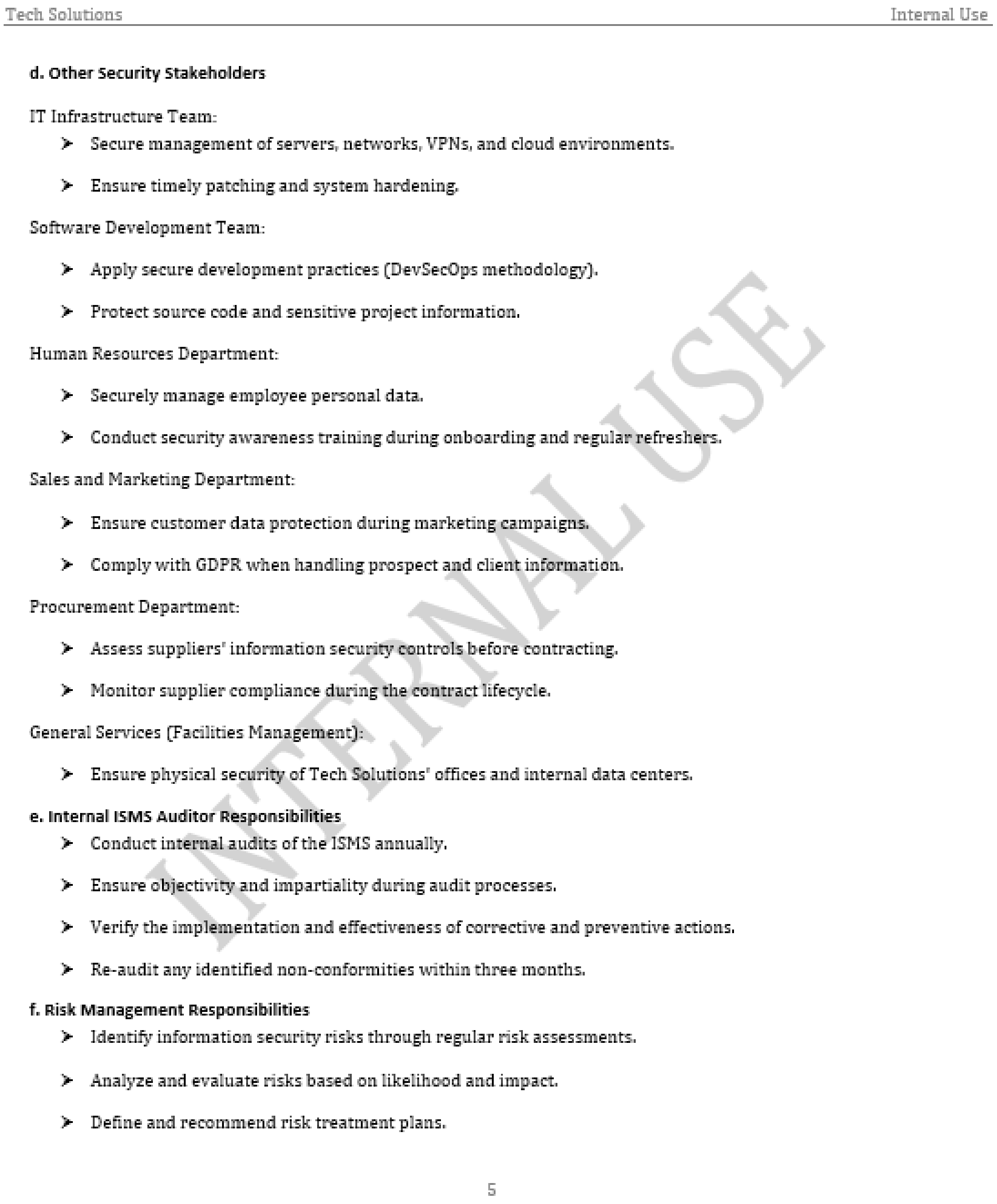
b. Information Security Officer Responsibilities

- Maintain and ensure ISMS compliance with ISO/IEC 27001:2022, GDPR, HIPAA, and NIS 2 Directive.
- Report ISMS performance, security incidents, and improvement opportunities to Top Management.
- Coordinate risk assessments and ensure appropriate treatment plans.
- Monitor and report ISMS key performance indicators (KPIs).
- Foster information security awareness and training programs.
- Serve as the liaison during internal and external audits.

c. Security Committee Responsibilities

- Review and validate the risk assessment and treatment results.
- Analyze and oversee security incidents and propose corrective actions.
- Review and validate the ISMS audit results and KPI trends quarterly.
- Support continual improvement and regulatory compliance efforts.

4



d. Other Security Stakeholders

IT Infrastructure Team:

- Secure management of servers, networks, VPNs, and cloud environments.
- Ensure timely patching and system hardening.

Software Development Team:

- Apply secure development practices (DevSecOps methodology).
- Protect source code and sensitive project information.

Human Resources Department:

- Securely manage employee personal data.
- Conduct security awareness training during onboarding and regular refreshers.

Sales and Marketing Department:

- Ensure customer data protection during marketing campaigns.
- Comply with GDPR when handling prospect and client information.

Procurement Department:

- Assess suppliers' information security controls before contracting.
- Monitor supplier compliance during the contract lifecycle.

General Services (Facilities Management):

- Ensure physical security of Tech Solutions' offices and internal data centers.

e. Internal ISMS Auditor Responsibilities

- Conduct internal audits of the ISMS annually.
- Ensure objectivity and impartiality during audit processes.
- Verify the implementation and effectiveness of corrective and preventive actions.
- Re-audit any identified non-conformities within three months.

f. Risk Management Responsibilities

- Identify information security risks through regular risk assessments.
- Analyze and evaluate risks based on likelihood and impact.
- Define and recommend risk treatment plans.

- Monitor and review risks periodically.
- Report major risks and residual risks to Top Management for approval.
- Maintain the risk register updated.

g. Incident Management Responsibilities

- Establish and maintain an incident response plan (IRP).
- Ensure all employees know how to recognize and report incidents.
- Coordinate the response to information security incidents.
- Analyze incidents to identify root causes and apply corrective actions.
- Maintain an incident log and produce post-incident reports.
- Escalate major incidents to Top Management and Security Committee.

h. Training and Awareness Responsibilities

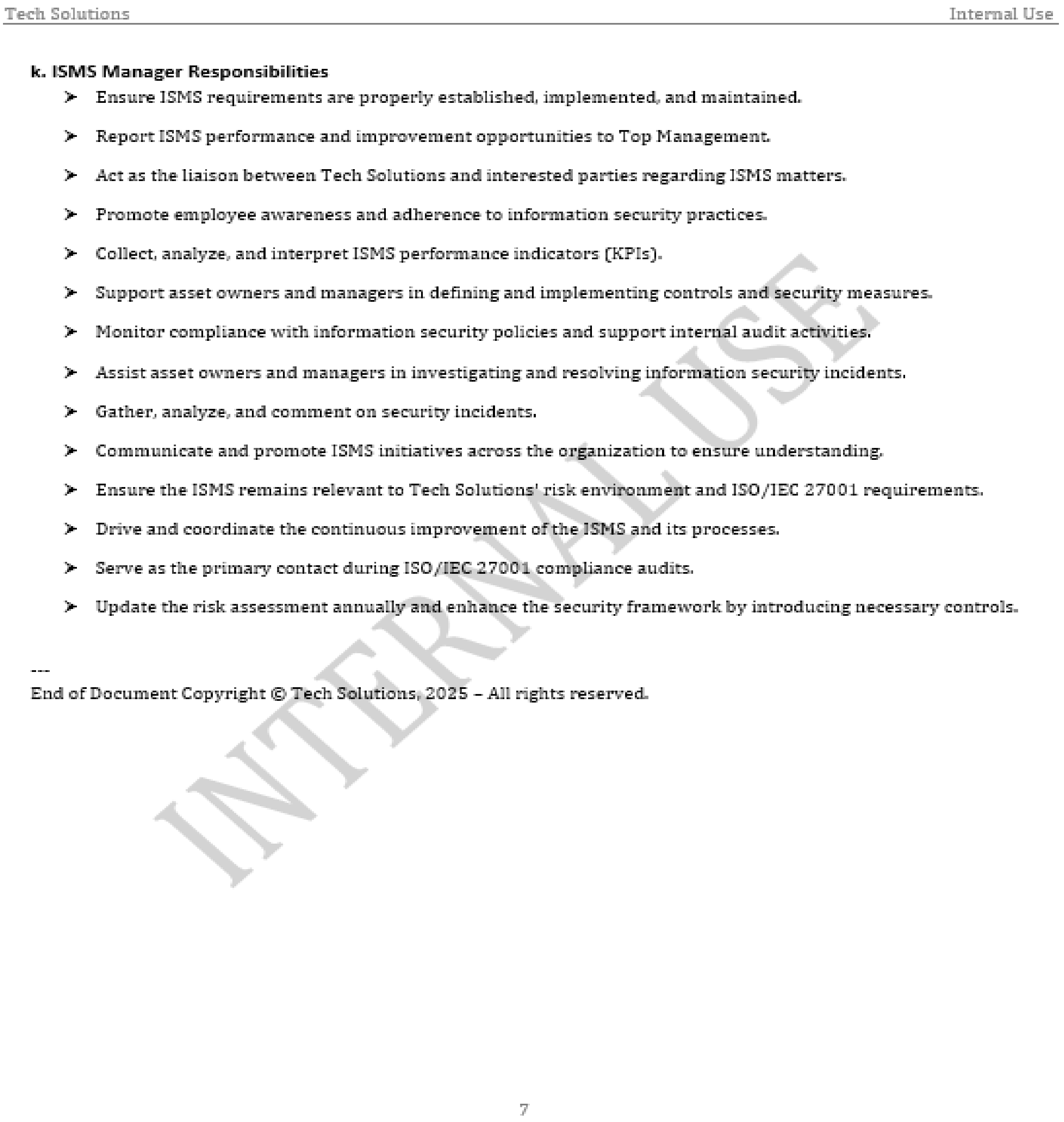
- Develop and deliver information security awareness programs.
- Conduct mandatory security training during onboarding.
- Organize periodic refresher sessions and phishing simulation campaigns.
- Maintain attendance and completion records for training.
- Update training materials to reflect new threats, regulations, or policies.

i. Third Party / Supplier Management Responsibilities

- Evaluate the security posture of suppliers and third parties before contracting.
- Include security requirements in supplier contracts (e.g., data protection clauses).
- Monitor supplier compliance during contract execution (through reviews or audits).
- Manage risks related to third-party access to information and systems.
- Maintain a register of suppliers and their information security agreements.

j. Legal and Compliance Management Responsibilities

- Monitor compliance with applicable laws and regulations (GDPR, HIPAA, and NIS2).
- Review and update information security policies to reflect legal changes.
- Coordinate with Legal advisors when data breaches or compliance issues arise.
- Maintain a repository of applicable regulatory requirements.
- Report compliance status periodically to Top Management and during ISMS reviews.

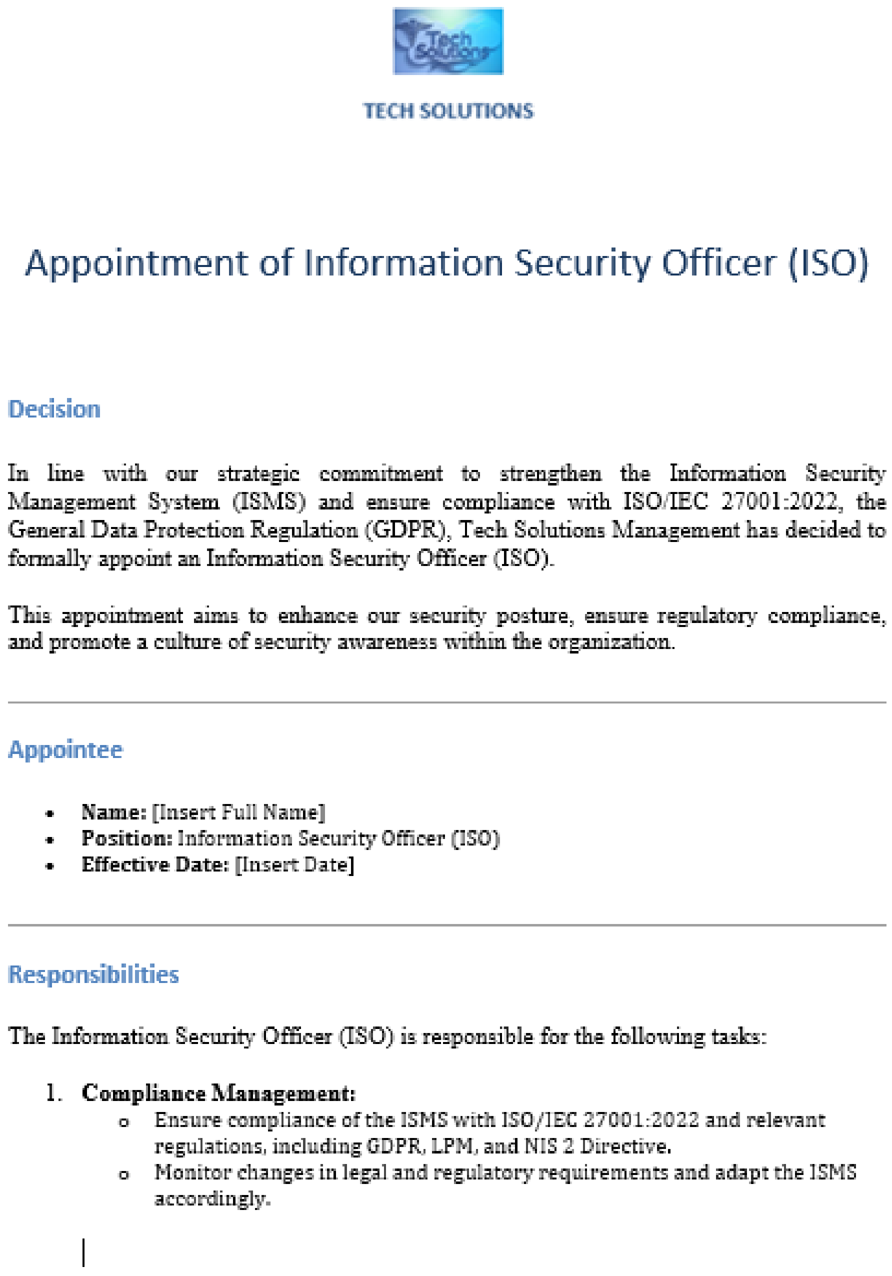


k. ISMS Manager Responsibilities

- Ensure ISMS requirements are properly established, implemented, and maintained.
- Report ISMS performance and improvement opportunities to Top Management.
- Act as the liaison between Tech Solutions and interested parties regarding ISMS matters.
- Promote employee awareness and adherence to information security practices.
- Collect, analyze, and interpret ISMS performance indicators (KPIs).
- Support asset owners and managers in defining and implementing controls and security measures.
- Monitor compliance with information security policies and support internal audit activities.
- Assist asset owners and managers in investigating and resolving information security incidents.
- Gather, analyze, and comment on security incidents.
- Communicate and promote ISMS initiatives across the organization to ensure understanding.
- Ensure the ISMS remains relevant to Tech Solutions' risk environment and ISO/IEC 27001 requirements.
- Drive and coordinate the continuous improvement of the ISMS and its processes.
- Serve as the primary contact during ISO/IEC 27001 compliance audits.
- Update the risk assessment annually and enhance the security framework by introducing necessary controls.

End of Document

The following document formalizes the appointment of an Information Security Officer (ISO) at Tech Solutions to strengthen the Information Security Management System (ISMS) and ensure compliance with key regulations such as ISO/IEC 27001:2022, GDPR, LPM, and the NIS 2 Directive.



TECH SOLUTIONS

Appointment of Information Security Officer (ISO)

Decision

In line with our strategic commitment to strengthen the Information Security Management System (ISMS) and ensure compliance with ISO/IEC 27001:2022, the General Data Protection Regulation (GDPR), Tech Solutions Management has decided to formally appoint an Information Security Officer (ISO).

This appointment aims to enhance our security posture, ensure regulatory compliance, and promote a culture of security awareness within the organization.

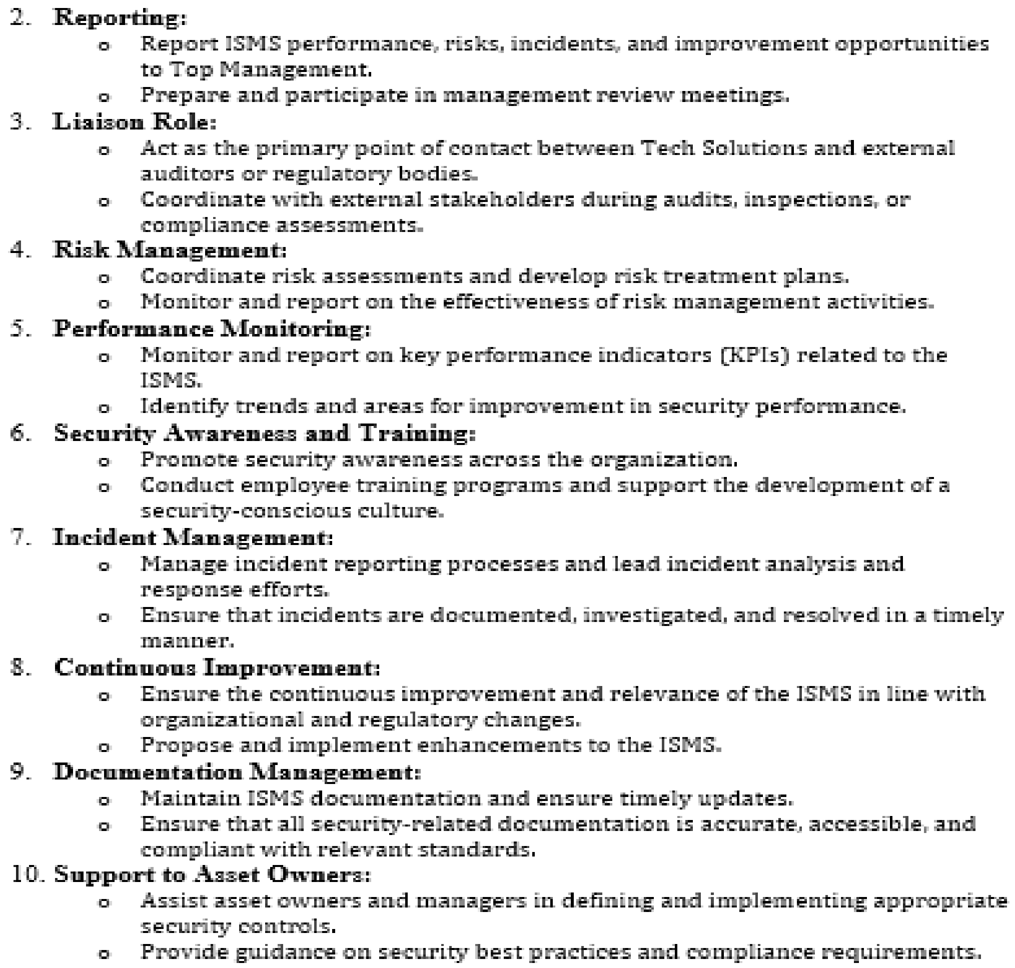
Appointee

- **Name:** [Insert Full Name]
- **Position:** Information Security Officer (ISO)
- **Effective Date:** [Insert Date]

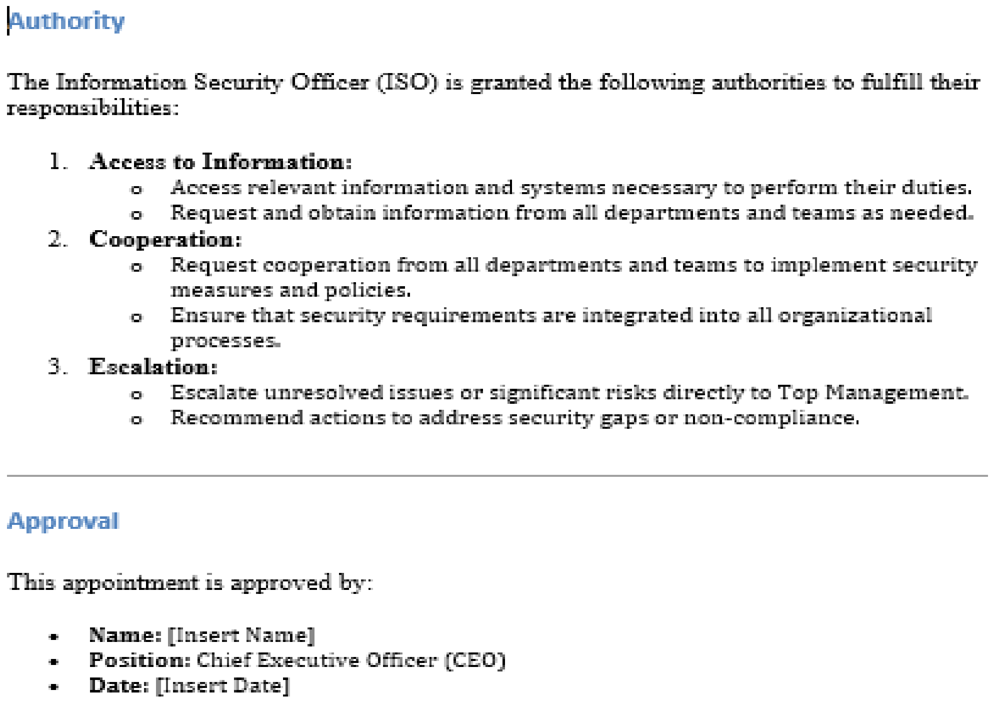
Responsibilities

The Information Security Officer (ISO) is responsible for the following tasks:

1. **Compliance Management:**
   - Ensure compliance of the ISMS with ISO/IEC 27001:2022 and relevant regulations, including GDPR, LPM, and NIS 2 Directive.
   - Monitor changes in legal and regulatory requirements and adapt the ISMS accordingly.



2. **Reporting:**
   - Report ISMS performance, risks, incidents, and improvement opportunities to Top Management.
   - Prepare and participate in management review meetings.
3. **Liaison Role:**
   - Act as the primary point of contact between Tech Solutions and external auditors or regulatory bodies.
   - Coordinate with external stakeholders during audits, inspections, or compliance assessments.
4. **Risk Management:**
   - Coordinate risk assessments and develop risk treatment plans.
   - Monitor and report on the effectiveness of risk management activities.
5. **Performance Monitoring:**
   - Monitor and report on key performance indicators (KPIs) related to the ISMS.
   - Identify trends and areas for improvement in security performance.
6. **Security Awareness and Training:**
   - Promote security awareness across the organization.
   - Conduct employee training programs and support the development of a security-conscious culture.
7. **Incident Management:**
   - Manage incident reporting processes and lead incident analysis and response efforts.
   - Ensure that incidents are documented, investigated, and resolved in a timely manner.
8. **Continuous Improvement:**
   - Ensure the continuous improvement and relevance of the ISMS in line with organizational and regulatory changes.
   - Propose and implement enhancements to the ISMS.
9. **Documentation Management:**
   - Maintain ISMS documentation and ensure timely updates.
   - Ensure that all security-related documentation is accurate, accessible, and compliant with relevant standards.
10. **Support to Asset Owners:**
    - Assist asset owners and managers in defining and implementing appropriate security controls.
    - Provide guidance on security best practices and compliance requirements.



Authority

The Information Security Officer (ISO) is granted the following authorities to fulfill their responsibilities:

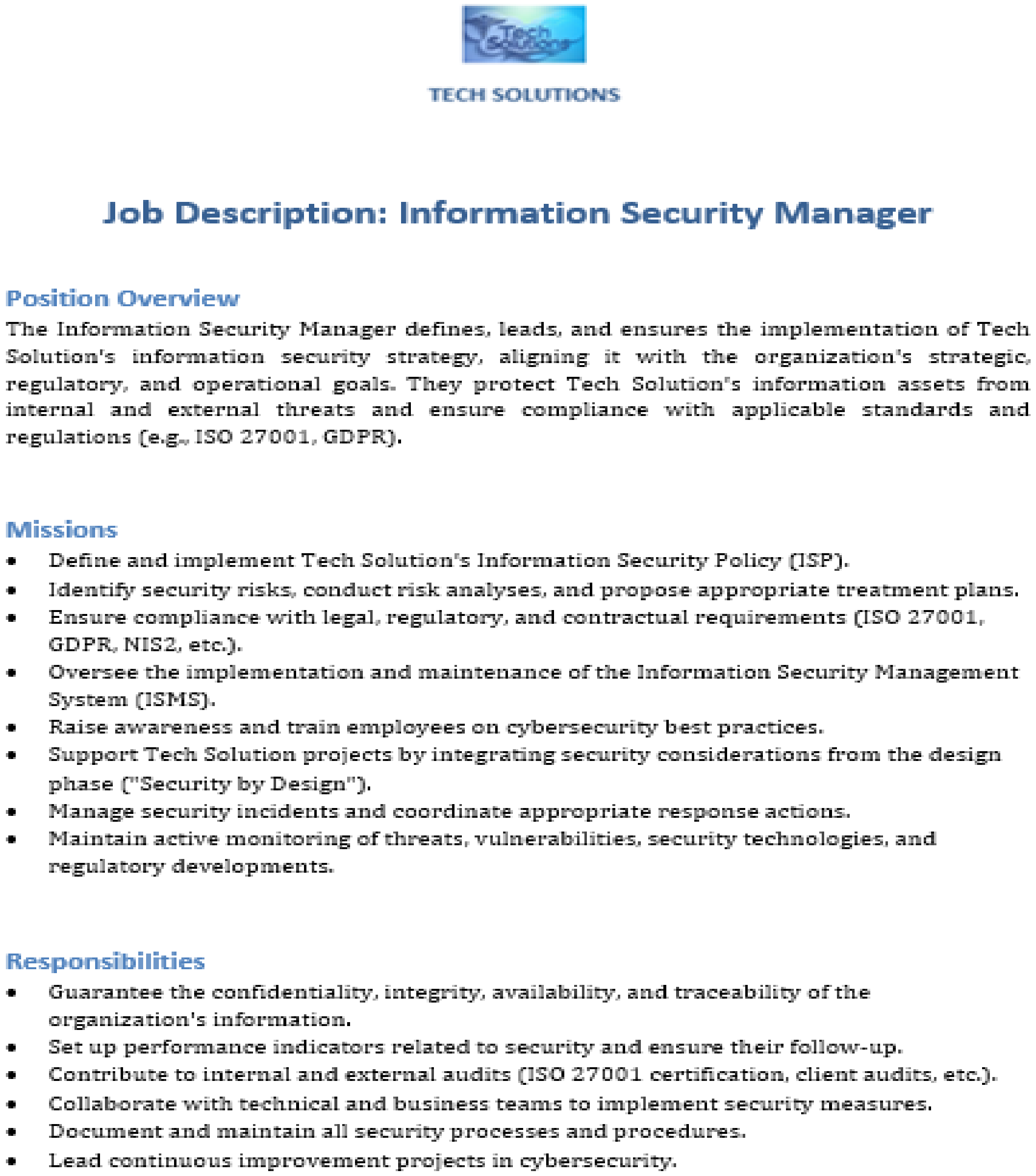
1. **Access to Information:**
    - Access relevant information and systems necessary to perform their duties.
    - Request and obtain information from all departments and teams as needed.
2. **Cooperation:**
    - Request cooperation from all departments and teams to implement security measures and policies.
    - Ensure that security requirements are integrated into all organizational processes.
3. **Escalation:**
    - Escalate unresolved issues or significant risks directly to Top Management.
    - Recommend actions to address security gaps or non-compliance.

Approval

This appointment is approved by:

- **Name:** [Insert Name]
- **Position:** Chief Executive Officer (CEO)
- **Date:** [Insert Date]

This following document outlines the formal appointment of an Information Security Officer (ISO) at Tech Solutions Management. It defines the ISO's role, responsibilities, and authority to ensure the strengthening of the Information Security Management System (ISMS) and compliance with key regulations such as ISO/IEC 27001:2022, GDPR. The appointment aims to enhance the organization's security posture, promote a culture of security awareness, and ensure continuous improvement in managing information security risks.



TECH SOLUTIONS

Job Description: Information Security Manager

Position Overview

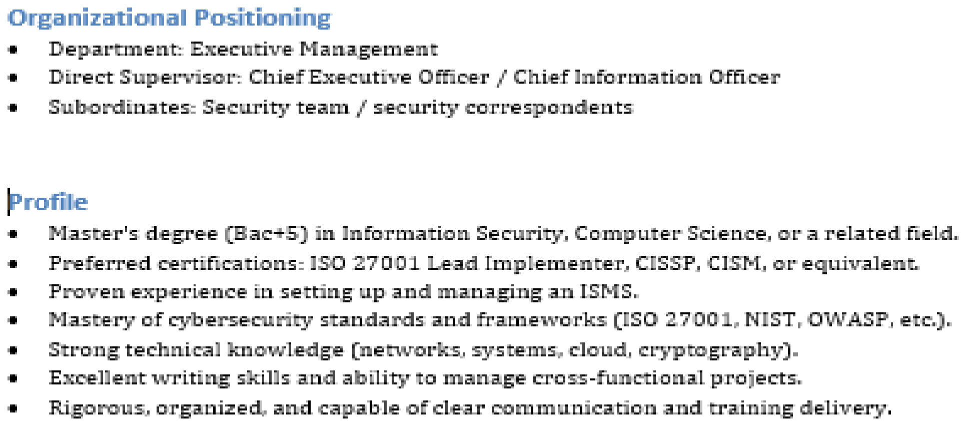
The Information Security Manager defines, leads, and ensures the implementation of Tech Solution's information security strategy, aligning it with the organization's strategic, regulatory, and operational goals. They protect Tech Solution's information assets from internal and external threats and ensure compliance with applicable standards and regulations (e.g., ISO 27001, GDPR).

Missions

- Define and implement Tech Solution's Information Security Policy (ISP).
- Identify security risks, conduct risk analyses, and propose appropriate treatment plans.
- Ensure compliance with legal, regulatory, and contractual requirements (ISO 27001, GDPR, NIS2, etc.).
- Oversee the implementation and maintenance of the Information Security Management System (ISMS).
- Raise awareness and train employees on cybersecurity best practices.
- Support Tech Solution projects by integrating security considerations from the design phase ("Security by Design").
- Manage security incidents and coordinate appropriate response actions.
- Maintain active monitoring of threats, vulnerabilities, security technologies, and regulatory developments.

Responsibilities

- Guarantee the confidentiality, integrity, availability, and traceability of the organization's information.
- Set up performance indicators related to security and ensure their follow-up.
- Contribute to internal and external audits (ISO 27001 certification, client audits, etc.).
- Collaborate with technical and business teams to implement security measures.
- Document and maintain all security processes and procedures.
- Lead continuous improvement projects in cybersecurity.



Organizational Positioning

- Department: Executive Management
- Direct Supervisor: Chief Executive Officer / Chief Information Officer
- Subordinates: Security team / security correspondents

Profile

- Master's degree (Bac+5) in Information Security, Computer Science, or a related field.
- Preferred certifications: ISO 27001 Lead Implementer, CISSP, CISM, or equivalent.
- Proven experience in setting up and managing an ISMS.
- Mastery of cybersecurity standards and frameworks (ISO 27001, NIST, OWASP, etc.).
- Strong technical knowledge (networks, systems, cloud, cryptography).
- Excellent writing skills and ability to manage cross-functional projects.
- Rigorous, organized, and capable of clear communication and training delivery.

5.5 Segregation of duties

Control description:

Incompatible tasks and areas of responsibility must be segregated to prevent any single individual from being able to perform potentially incompatible tasks alone.

Control type	Information security properties	Cybersecurity concepts	Optional capabilities	Security domains
Préventif	• Confidentialité • Intégrité • Disponibilité	Protect	#Gouvernance #Identity_and_access_management	#Gouvernance et Écosystème

Control attributes:

- **Control type:** When it acts : Preventive
- **Information security properties:** Confidentiality, Integrity, Availability
- **Cybersecurity concepts:** Which phase of cybersecurity it supports : Protect
- **Optional capabilities:** Which operational area it belongs to : Governance, Identity_and_ac-cess_management
- **Security domains:** Which domain it relates to : Governance et Écosystème

Control requirement:

The organization should decide which tasks must be separated between different people or teams.

The goal is to reduce risks of mistakes, fraud, or abuse of power.

If one person can perform all steps (for example: request, approve, and execute a system change), they could act incorrectly or maliciously without being detected.

By separating duties, the organization introduces cross-checks and better security.

Examples of activities that need segregation:

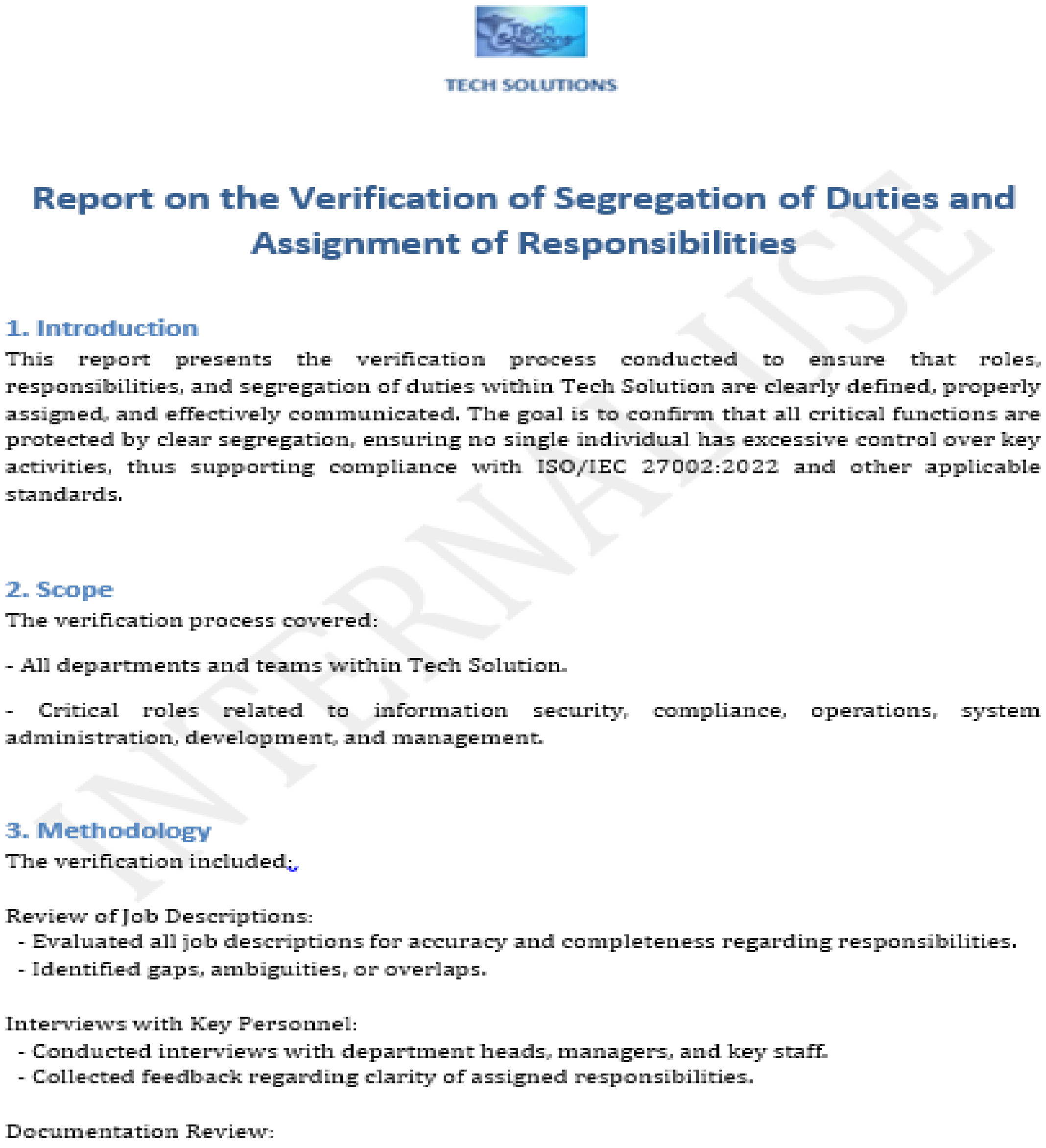
Activity	What should be separated?
Changing a system	Separate the roles for requesting, approving, and implementing changes.
Managing access rights	Different people should request, approve, and assign or remove access.
Writing software code	Separate the roles for designing, developing, and reviewing the code.
Using and administering applications	Users and administrators of an application should be different
Securing information	Separate those who design, audit, and ensure security controls.

➔ Do not give full control to a single person

Checks to be performed	Evidence
➢ If tasks that need to be separated are identified and responsibilities are assigned accordingly ➢ If a regular task of verifying, defining, and assigning responsibilities is planned and carried out ➢ If compensating controls are implemented in cases where incompatible tasks are assigned to the same person.	➢ Job descriptions ➢ Report on the verification of the definition and assignment of responsibilities

5.6 Practical Application of Clause 5.3: Case Study

This report titled "Verification of Segregation of Duties and Assignment of Responsibilities" provides a detailed assessment of how Tech Solution defines, assigns, and manages roles and responsibilities within the organization:



TECH SOLUTIONS

Report on the Verification of Segregation of Duties and Assignment of Responsibilities

1. Introduction

This report presents the verification process conducted to ensure that roles, responsibilities, and segregation of duties within Tech Solution are clearly defined, properly assigned, and effectively communicated. The goal is to confirm that all critical functions are protected by clear segregation, ensuring no single individual has excessive control over key activities, thus supporting compliance with ISO/IEC 27002:2022 and other applicable standards.

2. Scope

The verification process covered:

- All departments and teams within Tech Solution.

- Critical roles related to information security, compliance, operations, system administration, development, and management.

3. Methodology

The verification included:

Review of Job Descriptions:

- Evaluated all job descriptions for accuracy and completeness regarding responsibilities.
- Identified gaps, ambiguities, or overlaps.

Interviews with Key Personnel:

- Conducted interviews with department heads, managers, and key staff.
- Collected feedback regarding clarity of assigned responsibilities.

Documentation Review:

- Reviewed organizational charts, policies, procedures, and segregation matrices.

Gap Analysis:
- Identified overlaps and missing assignments.
- Provided recommendations to address findings.

Communication and Training Review:
- Assessed how responsibilities were communicated across the organization.
- Identified necessary awareness and training needs.

4. Findings

4.1. Strengths

- Most critical IT and compliance roles at Tech Solution have well-defined job descriptions.
- Clear reporting lines exist for incident response, access management, and risk management activities.
- Good segregation practices were identified between development and production system administration.

4.2. Gaps and Areas for Improvement

Gap 1: Incomplete Job Descriptions
- Certain operations and administrative roles lacked detailed task segregation.
- Recommendation: Update all relevant job descriptions to reflect distinct responsibilities.

Gap 2: Overlapping Responsibilities
- Minor overlaps between the Information Security Officer (ISO) and Compliance Manager roles were identified.
- Recommendation: Clearly define the boundaries between security assurance and regulatory compliance activities.

Gap 3: Lack of Training on Responsibilities
- Some employees were unaware of the importance of task segregation related to access rights and change management.
- Recommendation: Conduct targeted training programs on segregation of duties and related controls.

Gap 4: Misalignment with ISO 27002:2022
- Some activities such as code review and approval processes were not fully segregated as per the new ISO 27002 standards.
- Recommendation: Implement appropriate control mechanisms to ensure full alignment.

5. Recommendations

Update and Clarify Job Descriptions:
- Ensure segregation is explicitly stated where necessary.

Review and Adjust Responsibilities:
- Address any overlaps and ensure all critical processes have appropriate separation of duties.

Enhance Awareness and Training:
- Launch training sessions to reinforce the importance of clearly segregated responsibilities.

Implement Ongoing Monitoring:
- Establish periodic reviews to monitor roles and responsibilities against organizational and regulatory changes.

6. Conclusion

The verification confirms that Tech Solution has a strong framework for defining and assigning responsibilities but identified several areas where improvements are needed, particularly regarding the strict segregation of duties per ISO 27002:2022. Implementing the recommended improvements will enhance security, accountability, compliance, and operational effectiveness.

7. Approval

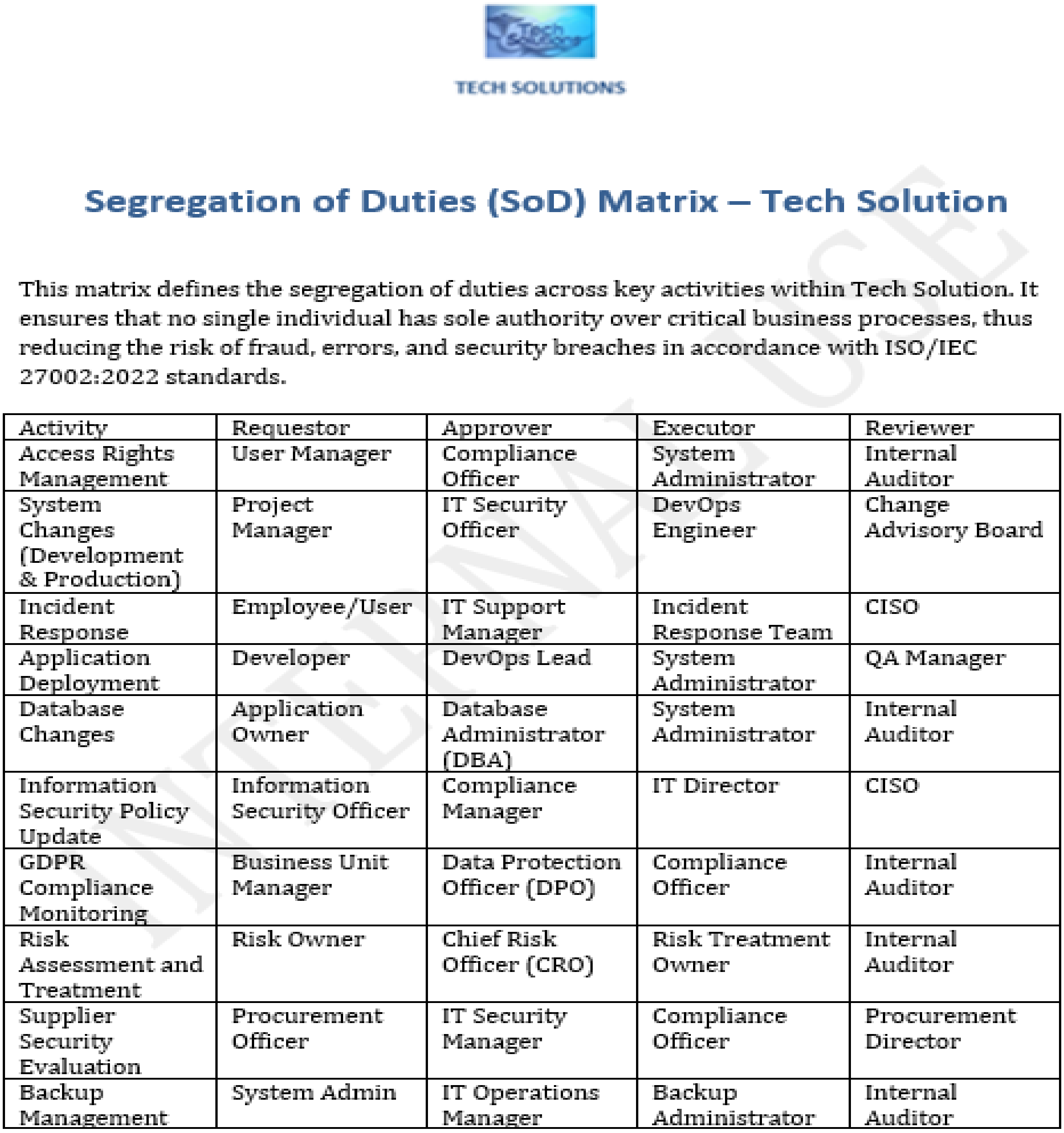
Approved by:

Name: [Insert Name]
Position: [Insert Position]
Date: [Insert Date]

Prepared by:
[Your Name]
[Your Position]
Tech Solution
[Date]

This document, titled "Segregation of Duties (SoD) Matrix – Tech Solution", provides a structured overview of how Tech Solution distributes key responsibilities across different roles to ensure strong internal controls.

The matrix is designed to prevent any single individual from having full authority over critical operations, thereby reducing risks related to fraud, errors, and security breaches:



TECH SOLUTIONS

Segregation of Duties (SoD) Matrix – Tech Solution

This matrix defines the segregation of duties across key activities within Tech Solution. It ensures that no single individual has sole authority over critical business processes, thus reducing the risk of fraud, errors, and security breaches in accordance with ISO/IEC 27002:2022 standards.

Activity	Requestor	Approver	Executor	Reviewer
Access Rights Management	User Manager	Compliance Officer	System Administrator	Internal Auditor
System Changes (Development & Production)	Project Manager	IT Security Officer	DevOps Engineer	Change Advisory Board
Incident Response	Employee/User	IT Support Manager	Incident Response Team	CISO
Application Deployment	Developer	DevOps Lead	System Administrator	QA Manager
Database Changes	Application Owner	Database Administrator (DBA)	System Administrator	Internal Auditor
Information Security Policy Update	Information Security Officer	Compliance Manager	IT Director	CISO
GDPR Compliance Monitoring	Business Unit Manager	Data Protection Officer (DPO)	Compliance Officer	Internal Auditor
Risk Assessment and Treatment	Risk Owner	Chief Risk Officer (CRO)	Risk Treatment Owner	Internal Auditor
Supplier Security Evaluation	Procurement Officer	IT Security Manager	Compliance Officer	Procurement Director
Backup Management	System Admin	IT Operations Manager	Backup Administrator	Internal Auditor