(Template – will be adapted with minimal modifications to suit your specific application)
Some points will be developed, added, cut, or specified (in red)

Information security Manual

IS manual revision history

Page	Change	Revision	Author	Function	Approved	Function	Date
all	Creation	001					

This paper copy is a controlled document one day after printing.

1. Introduction

1.1 Presentation of our company

General

Name	…..
Legal form	…..
Authorized capital	…..
Registered office	…..
Siret	…..
VAT No.	…..
NAF	…..
Phone	…..
Fax	…..
Email	…..
Internet	…..
Director	…..
Sphere of activity	…..

Organization

Our company includes the following sites: ……

Our company includes the following departments: …… (cf. § 5.3)

Mission (finality)

Guarantee the confidentiality, integrity, availability and traceability of information
Reduce risks related to information security
…

Slogan

Irreproachable quality always on time at a low cost
The preventive approach is the rule, the corrective action is the exception
…

Products and services

Our products are: …

Our services are: …

History

History of the company: …..

Now the company: …..

1.2 Purpose of the manual

The purpose of this information security manual is to describe the provisions of our information security management system (ISMS) to maintain and improve:

- our ability to provide compliant products and services
- necessary resources
- compliance with applicable legal and regulatory requirements
- the satisfaction of customers and other interested parties
- our processes

The manual covers all of the activities of our organization including development, production, marketing and support services.

The manual is available internally and externally (on request, the IS manager handles the distribution history).

2. Standards and definitions

Our IS management system meets the requirements of the following standards:

- **ISO 9001 (2015): Quality Management Systems – Requirements**
- **ISO 27001 (2022): Information security, cybersecurity and privacy protection - Information security management system – Requirements**
- **ISO 31000 (2018): Risk management - Guidelines**

For internal audits, our reference is the standard **ISO 19011 (2018): Guidelines for auditing management systems**.

We use the definitions of the following standards as much as possible:

- **ISO 9000 (2015): Quality management systems - Fundamentals and vocabulary**
- **ISO 27000 (2018): Information technology - Security techniques - Information security management systems - Overview and vocabulary**

Some terms we use:

Availability: *property of information to be usable by an entity*
Backup: *copy of data in order to archive and protect*
Competence: *skills, knowledge and personal experiences*
Confidentiality: *property of information to be accessible to only one entity*
Conformity: *fulfillment of a specified requirement*
Corrective action: *action to eliminate the cause of nonconformity or any other undesirable event and prevent their recurrence*
Customer satisfaction: *top priority objective of every management system*
Customer: *anyone who receives a product*
Document (documented information): *any support allowing the treatment of information*
Effectiveness: *capacity to realize planned activities with minimum efforts*
Efficiency: *financial relationship between achieved results and used resources*
Indicator: *value of a parameter*, *associated with an objective, allowing the objective measure of its effectiveness*
Information security: *measures to protect the confidentiality, integrity and availability of information*
Integrity: *property of information to be unaltered*
Interested party: *person, group or organization affected by the impacts from an organization*
ISMS: *information security management system*
Issue: *any element of value to the organization*
Management system: *set of processes allowing objectives to be achieved*
Nonconformity: *non-fulfillment of a specified requirement*

Objective: *measurable goal to be achieved*
Organization (company): *a structure that satisfies a need*
Procedure (documented information to maintain): *document describing the actions to carry out a process*
Process: *activities which transform inputs into outputs*
Product (or service): *every result of a process or activity*
Quality: *aptitude to fulfill requirements*
Record (documented information to retain): *document providing objective evidence of achieved results*
Requirement: *explicit or implicit need or expectation*
Residual risk: *risk accepted*
Risk assessment: *risk analysis and assessment process*
Risk treatment: *risk modification activities*
Risk: likelihood *of occurrence of a threat or an opportunity*
Statement of applicability (SoA): *document describing the objectives and security measures*
Supplier (external provider): *an entity that provides a product*
System: *set of interacting processes*
Top management: *group or persons in charge of the organizational control at the highest level*
Vulnerability: *weakness of an asset that could lead to unauthorized access*

3. Process approach

3.1 The processes in the company

Top management provides, maintains and improves the resources and staff for the necessary processes. More details are provided in the process "Control documentation" and in the document (documented information to retain) "Process List". The processes are classified into 3 types (management, realization and support).

The management processes in our company are:

- assess risks
- treat risks
- communicate
- conduct an audit
- plan the ISMS
- establish process ownership
- develop strategy
- establish policy
- deploy objectives
- carry out management review
- improve

The realization processes are:

- meet information security requirements
- control outsources processes
- register and unsubscribe
- distribute access
- manage authentication
- develop and support security
- manage security continuity
- implement security

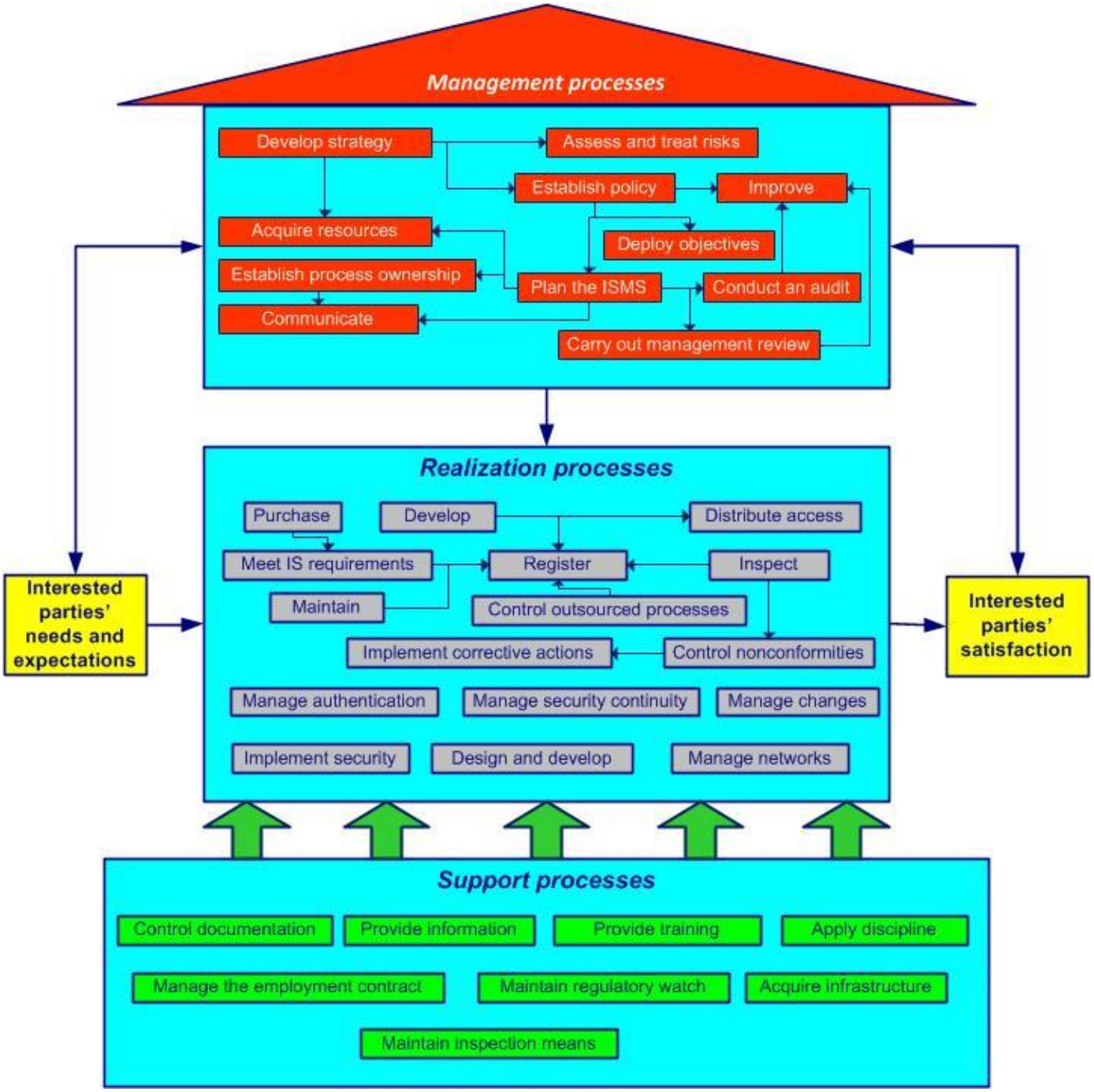
- inspect security
- design and develop
- purchase
- maintain equipment
- manage networks
- manage changes
- control nonconformities
- implement corrective actions

The support processes are:

- apply discipline
- manage the employment contract
- maintain regulatory watch
- acquire and maintain infrastructure
- manage inspection means
- provide training
- provide information
- control documentation

3.2 Process mapping

The process mapping is shown below:



A process review (for key processes) is conducted periodically by the process owner. More details in the process “Establish process ownership”.

4. Context of the company

4.1 Issues

Top management has made a diagnosis of the context in which our company exists and takes into account the external and internal issues relevant to our strategic direction and our ability to achieve ISMS objectives (see the "Scope of the ISMS" and “Regulatory watch” procedures).

We regularly monitor and review information related to the issues and factors that may influence the achievement of our objectives.

4.2 Interested parties

Top management has determined the relevant interested parties for our company and our ISMS (see "List of interested parties") and their requirements for our company. These requirements relate to information security and applicable laws and regulations.

4.3 Scope

This IS manual applies to:

- all areas of our business, including supplier relations
- assets (information, equipment, people)

More details in the "Scope of the ISMS" procedure.

The scope of our company is: …..

The concerned sites are: …..

The following requirements of ISO 27001 .... are not applicable (sub-clause xx). These requirements do not affect our ability or responsibility to ensure information security and improve customer satisfaction.

The justification is: .....

4.4 Description of the ISMS

This IS manual describes processes, policies and documented information to be maintained (procedures) and to be retained (records) that are necessary to establish, implement, maintain and continually improve our ISMS in accordance with ISO 27001. The purpose of the manual is described in sub-clause 1.2.

5. Leadership

5.1 Management commitment

Top management determines the information security policy in a written declaration. This declaration is posted in some key places, to be seen by personnel and customers. The IS policy supports our strategic direction and is defined by a commitment from management.

Declaration of top management

The director's personal commitment to improving the effectiveness of the ISMS includes the promise to:

- ensure our success imperatively meets the satisfaction of all interested parties who are expecting a faultless performance in terms of:
  - our information security
  - our time frames
  - our costs
- our efforts to be fair and competent in listening, understanding, anticipating and fulfilling customer wishes
- strive for continual improvement of our performance
- the correct application, maintenance and continuous improvement of our information security management system (ISMS)
- the pursuit of market conquest