[check 5.1] Objective of the information security policy

Ourorganization deals with analyzing the industrial and commercial data of client companies in order to support management in the process of taking management decisions.

Politicsappropriate to the purposes of the organization

Aware thatthe customer data, the results of their analysis, the addresses suggested to the customer and the survey methods (statistical analysis algorithms) constitute information whose value represents the corporate assets of our organization and that of the customer, we have implemented a management system for information security by providing for the development of all security controls applicable to the processing of information.

Policy forset safety goals

Thanks to the implementation of the management system, we have determined the information security objectives that will see us committed, in each business process, to the preservation of:

- Confidentiality of data released by the customer
- Integrity of the information released by the customer and those relating to the data processing procedures we use to carry out the analyzes
- Availability of such information to persons authorized to manage and use them

Commitment policycompliance with applicable requirements

The commitment of top management and of all those who in various capacities are involved in the activities of the management system is to comply with all the requirements set out in the International Standard ISO 27001: 2017. For this reason, top management undertakes to exercise leadership in accordance with the provisions of this standard.

Commitment policy for thecontinuous improvement of the management system

The client's information assets and that relating to the know-how of our organization will henceforth constitute the focal points of everyone's commitment. A commitment made by each and every one.

This commitment will be manifested through the "security performances" which must show how effective our organization and our information security management system are in recording continuous improvement.

RISK IDENTIFICATION AND ASSESSMENT

MOD-610-A

IDENTIFICATIONAND RISK ASSESSMENT IN PRIMARY PROCESSES

PRIMARY PROCESSES

Oflater we highlighted the primary processes. Such are those that characterize the typical activity of the organization (business)and which govern the operational activities related to the provision of the service and production

PROCESSES	INFORMATIONFROM TO PROTECT	DOCUMENTSTO PROTECT	ACTIVE ROLES
▪ Requirements ▪ Design ▪ Outsourcing ▪ Production ▪ Preservation ▪ Check output	▪ Data commercial ▪ Contracts ▪ Partnership agreements ▪ Projects ▪ Project requirements ▪ Design mode ▪ Strategiesand needs ▪ Launch of new products ▪ Costsand production times ▪ Financial informationAnd contractual ▪ Customer names and suppliers ▪ Technical data ▪ Patents, tooin progress registration ▪ Designs and solutions of design ▪ Plansand production schemes ▪ Plansand design schemes ▪ Plansand analysis schemes e development requirements ▪ Supply specifications And of opera ▪ Technical drawings ▪ Algorithm specifications ▪ Project performance (times, technologies, results) ▪ Plansand control mode in general activity productive ▪ Processes, formulas ▪ Personal data details "Sensitive" according to Art.9 of European regulation 679/2016 (GDPR) ▪ Intellectual property governed by title IX of Civil Code- of the rights on intellectual worksand on industrial inventions	***LABELING*** ***IC-A= level A critical information*** **MANAGEMENT PROCEDURES** PROC-812 Requirements PROC-813 Design PROC-814 Outsourcing PROC-815 Production PROC-816 Preservation PROC-817 Control of non-conforming outputs **FORMS IN WORD** MOD-812-A Collectionand review of requirements MOD-813-A Project plan MOD-813-B Project inputs MOD-813-C Design review MOD-813-D Design verification MOD-813-E Design validation MOD-813-F Design outputs MOD-813-G Design changes MOD-814-B Supplier evaluation sheet MOD-814-C Request for quotation MOD-814-D Purchase order MOD-814-E Change request MOD-814-F Controlsin entrance MOD-815-A Production plan MOD-815-C Validation of production MOD-815-D Product release MOD-815-E Product delivery MOD-815-F Customer Property MOD-815-G Intervention request MOD-815-H Intervention report MOD-817-A Quality control **FORMS IN EXCEL (APPLICATIONS MANAGEMENT)** MOD-814-A List of suppliers MOD-815-B Identification and traceability MOD-817-B Non-compliant products	▪ High management ▪ RDP (marketing) ▪ RDP (design) ▪ RDP (production) ▪ RDP (assistance) ▪ RDP (purchases) ▪ RGSI (responsible management system safety information) ▪ OP (production)

RISK IDENTIFICATION AND ASSESSMENT — MOD-610-A

IDENTIFICATIONAND RISK ASSESSMENT IN PRIMARY PROCESSES

ARISING THREATSBY PEOPLE EMPLOYED IN PRIMARY PROCESSES

THREATS / DANGERS	ASSESSMENT RISKS
▪ Stealing for use personaland for sale (profit) ▪ Aiding in the competition (infidelity) ▪ Attackto continuity operationalor reputation to the organization (retaliation) ▪ Trialof their skills computer science of intrusion ▪ Insufficient preparation technique inabout: management netand devices, system informative, database, malware, devices, techniques e strategies of protection, software development, management accidents ▪ Insufficient reliability ▪ Superficialityand carelessness (ex: voluntary disclosureor accidentalpassword) ▪ Absence of motivation to respectof the Policies security by the staff in general ▪ Unawarenesscriticality information and procedures of treatment ▪ Presence of vulnerability techniques in processes of managementand protection of information	**Analysesof the risks in relation to:** **the factors of the context factors, the needs and expectations of the parties interestedand the dangers identified** The information inherent to primary processes can generate large profits if: ▪ Used on their own ▪ Resoldto those who intend to use them Peopleemployed in primary processes possess, by reason of their role, sufficient skills to carry out effective attacks **RISK ASSESSMENT IN THE ABSENCEOF SECURITY CHECKS** **LOSS OF** / **P.** / **C.** / **R.** / **LEVEL** CONFIDENTIALI / 3 / 3 / 9 / Tall INTEGRITY / 3 / 3 / 9 / Tall AVAILABILITY / 2 / 3 / 6 / Medium **Chance** that the event occurs, possible values: 1,2,3,4 (unlikely, occasional, likely,very likely) **Consequence** and extent of damage resulting from the event, possible values: 1,2,3,4 (slight, medium, severe, very serious) **Risk:** up to and including 3: low; 4 to 8 inclusive: medium; 9 to 16 inclusive: high **Acceptability**: untilto 3 inclusive (if greater than 3, controls must be applied more)

RISK IDENTIFICATION AND ASSESSMENT

MOD-610-A

RELATIONFINAL ON THE IDENTIFICATION AND RISK ASSESSMENT

The organization hasimplemented all controls and documented their application in the MOD-610-B-document

The organization, thanks to the application of controls for the**safety**listed in Annex A (Annex A -ISO 27001: 2017), presents thefollowing general situation regarding information risks.

PRIMARY

RISKSFROM	BY PEOPLE				PHYSICAL			
	P.	C.	R.	LEVEL	P.	C.	R.	LEVEL
CONFIDENTIALITY	1	3	3	Bass	.	3	3	Bass
INTEGRITY	1	3	3	Bass	.	3	3	Bass
AVAILABILITY	1	3	3	Bass	.	3	3	Bass

PROCESSESSUPPORT

RISKSFROM	BY PEOPLE				PHYSICAL			
	P.	C.	R.	LEVEL	P.	C.	R.	LEVEL
CONFIDENTIALITY	1	2	2	Bass	.	2	2	Bass
INTEGRITY	1	2	2	Bass	.	2	2	Bass
AVAILABILITY	1	2	2	Bass	.	2	2	Bass

SECURITY PROCESSES

RISKSFROM	BY PEOPLE				PHYSICAL			
	P.	C.	R.	LEVEL	P.	C.	R.	LEVEL
CONFIDENTIALITY	1	3	3	Bass	.	3	3	Bass
INTEGRITY	1	3	3	Bass	.	3	3	Bass
AVAILABILITY	1	3	3	Bass	.	3	3	Bass

Allthe risks identified in the processes show an R value of no more than 3 and are therefore acceptable.

Signature of Senior Management	
Risk assessment date	
RGSI signature for information acquisition	

Information security related topeople

THREATS (DANGERS)

Thereinformation security that depends on people, their behavior, their intentions can be put at risk, as we have already documented in module MOD-610-A - Identification and evaluation **risk**,from the following threats:

- Stealing forpersonal use and for sale (profit)
- Aiding and abettingcompetition (infidelity)
- Attack on the business continuity or reputation of the organization (retaliation)
- Trialof their computer intrusion skills
- Insufficient technical preparation inabout: network and device management, information system, database, malware, devices, protection techniques and strategies, software development, incident management
- Insufficient reliability
- Inappropriate managementpasswords (voluntary or accidental disclosure)
- Lack of motivation for staff in general to comply with safety policies
- Errors and / or omissions in verifying the correspondence between: profiles determined by the accounts (roles) and related authorizations in accordance with that determined by management
- Unawareness of the criticality of informationand treatment procedures
- Presence of technical vulnerabilities in communication processesinformation

and data stealing from:

- USB sticks
- Send e-mail attachments
- Acquisition of paper documentsor copy them
- Revelationspoken or written to third parties
- Upload to the cloud personal
- Take photos and video footage
- Recordersvoice / audio
- Interception of network communication

coming from sourcesWhich:

- Persons authorized to access information
- Subjects notauthorized
- Events

Where the sourceis identified in unauthorized subjects, unauthorized access would also result.

10 CRYPTOGRAPHY

10.1 Cryptographic checks

Objective: To ensure acorrect and effective use of encryption to protect confidentiality, authenticity and / orthe integrity of the information

POINT	CATEGORY	CHECKS	No.	IN	IMPLEMENTATION	RESPONSIBLE
10.1.1	Politics on the use of controls cryptograp hic	It needs to be developed and implemented a policy on the use of controls cryptographic for the protectionfrom the information	40	YE S	Therepolicy on the use of controls cryptographic for protectionfrom the informationwas developed and implemented in the organization and is been documented in the procedure	High management
10.1.2	Managem ent of the keys	It needs to be developed and implemented a policy on use, on protection and on the duration of key cryptographicthrough their wholelife cycle	41	YE S	Data under cryptographic protection are loadedvia API of automated applications in the software that manages the cryptographic "Software name"And are encrypted. The information is encrypted according to itadvanced standard AES256.The software handles all stages of the key life cycle cryptographic. Thephases are the following: ▪ Managementpre-active state ▪ Managementactive state ▪ Managementdeactivation ▪ Managementof destruction The ruleson protection and on durationcryptographic keys, throughout their entire life cycle, are documentedin the procedure fromPSI-05 security Encryption	High direction

12 SAFETY OF OPERATIONAL ACTIVITIES

12.4 Collectionof logging and monitoring

Objective: Record events and generate evidence

POINT	CATEGORY	CHECKS	No.	IN	IMPLEMENTATION	RESPONSIBLE
12.4.1	Collection of log of events	The registration of event log, of the activities of users, from the exceptions, of the malfunctions and of events relating to safetyfrom the information needs to be carried out, maintainedAnd reviewed	63	YES	The organization planned to install in network of a log management software called "Application name". As governed by the PSI-12 procedure - Operational safety, the organization carries out, maintains and reviews periodically logging through the application it allowsthe following security checks: ▪ Generation of log ▪ Storage of log ▪ Analyses of the logs ▪ Monitoring of log ▪ Protection of log	RGSI
12.4.2	Protection from the informatio n ni of log	The facilities for the collection of log and le information of log they must be protected by tampering And accesses Not	64	YES	Protection of log takes place considering the importance ofdata present in the logs. Like specifiedin the PSI-12 procedure - Operational safety, security measures applied consist in put control of authentication for access to thelog file and the checkdata encryption (encryption) concerning to the logs	RGSI
12.4.3	Log of administer s bulls And operators	The activitiesof the administrators And of the operators of system must be submittedto log, and these must be protected And reviewed periodically	65	YES	As governed by the PSI-12 procedure - **Safety operational**, the activities of all users (especially those of the administrator of system it has notable which has wide access rights) are submittedto the recording of the related logs. Such log are protected by the measures of the control of log in and are periodically reviewed for the purpose of identifying the business in progressand look for signs of problems imminent. This procedureit is expected from procedure PSI-12 -	RGSI

winple PRO MANAGEMENT SYSTEMS

TEMPLATES ISO/IEC 27001:2017 INFORMATION SECURITY

OBJECTIVE SHEET

MOD-620-A

Target

Objective name

Network securityand communications
Achieve an adequate level of security in the network and communications

Description of the objective

Theresecurity in the operation of the network and communications must be pursued in relation to:

- Threatsenvironmental physics
- Voluntary attacks from the outside
- Voluntary attacks from within
- Events fornegligence
- Events for incompetence

The safety index must have a value of not less than 5 (scale from 1 to 5) by 12/31/2021. It will be measured through the administration of evaluation questionnaires by users

Responsibility

RGSI

Objective coding through the SMART technique

Record an index ofsecurity that we can define "of the network and communications" which results not inferiorto 5, by 12/31/2021 being willing to invest 2,100 euros in innovation on the management system and information security

Date	
Author	

2021 PLANNING INFORMATION SECURITY

TARGET	RESULT	EXPIRATION	RESOURCES	RESPONSIBLE	CHECK
Safetyof resources human	Indexsafety = 5	31/12/2021	2,100€	RGSI	☐
Safetyof the network and of the communications	Indexsafety = 5	31/12/2021	2,100€	RGSI	☐
Safetyof the quality of the formation	Indexsafety = 5	31/12/2021	2,100€	RGSI	☐
Software security	Indexsafety = 5	31/12/2021	2,100€	RGSI	☐
Device security from processing	Indexsafety = 5	31/12/2021	2,100€	RGSI	☐
Safetyof the headquarters and of the archives	Indexsafety = 5	31/12/2021	3,100€	RGSI	☐
Safetyof plants and devices of safety	Indexsafety = 5	31/12/2021	3,100€	RGSI	☐

Date	
HIGH MANAGEMENT	

Assessment

AREAOF WORK	DATE	PERSON
Ex:administrative offices		

Our organization intends to preserve securityof the software

We are giving you this questionnaireso that, in relation to his experience, he can express his personal one evaluation in this regard.
We also ask youto describe any shortcomings especially in cases where the evaluation was not positive. The values in increasing sense range from 1 to 5 and express the following evaluations:

SCORE	EVALUATION (expressed through the indicative sentence)
1	Security is notit is absolutely adequate, it needs to be redesigned
2	The securityit is poorly adequate, needs intervention
3	The securityit is sufficient but needs improvement
4	The securityit is adequate
5	The securityit's excellent

INDICATORS (indicates the level protection that you recognize against the following		ASSESSMENT				
No.	**Requirement**	**1**	**2**	**3**	**4**	**5**
1	Physical threats environmental	☐	☐	☒	☐	☐
2	Attacks volunteers from outside	☐	☐	☐	☒	☐
3	Attacks volunteers from within	☐	☒	☐	☐	☐
4	Events due to negligence	☐	☐	☐	☐	☒
5	Events for incompetence	☐	☐	☐	☐	☐

REPORT ANY POSSIBLE	
DANGERS	
INEFFICIENCIES	
DEFICIENCIESOF CAPACITY	
TECHNICAL VULNERABILITIES	

WANTED PROFILE

MOD-720-A

WANTED PROFILE

ROLE WANTED

Responsible of process: ICT

TASKSTO ASSIGN

1 Management and maintenance of the organization's IT network 2
Server management and maintenance
3 Maintenance of electronic devices (PC and device) 4
Repair and maintenance of hardware devices
5 Checking the wiring

TITLEOF STUDY

Degree in information science or computer engineering

EXPERIENCE

At least two years in the field

REQUIREMENTSRELIABILITY

1 Letter of presentation of reliability (from authoritative contact person eg: former employer, former manager) 2 Absence of criminal proceedings related to cybercrime

PREVIOUS KNOWLEDGE NECESSARY

1 TongueEnglish
2 Techniques of descriptive and inferential statistics

INTERNAL COMPETENCETO ACQUIRE

1 Project management
2 Processes productive
3 Process operational activities

INTERNAL AWARENESSTO ACQUIRE

1 Information security policy 2 Objectives
for information security
3 Information security risks and controls to address them 4
Context of the organization
5 Benefits of the information security management system

Date	
Signature	

winplePRO MANAGEMENT SYSTEMS

TEMPLATES ISO/IEC 27001:2017 INFORMATION SECURITY

TRAINING TEST | **MOD-720-D**

TEST FOR THE DETECTION OF THE COMPETENCE AND AWARENESS OF THE Learner

INFO BOX

This module is for the trainerto carry out the test to be submitted to company staff at the end of the training sessions.
In relation to the contentsof the course, the trainer creates the questions and the related set of answers of which only one will be the valid one. For each question, the person examined will have to select the answer they deem correct and therefore, at the end of the 5 requirements we will have 5 answers selected.

The trainer will match a point for each answerin such a way that, in the face of the 5 questions, the score can vary from zero to five. The score obtained in the test will come then reported by the trainer in the form MOD-720-C-Training Register in order to keep the results of the formationand measure the results.

CANDIDATE	
FIRST NAMEAND	
OFFICE	

NAME OF THE TEST

SECURITY RISKS OF INFORMATION

1st QUESTION

<< Question to be inserted by the teacher >>

CORRECT ANSWER

☐ *Reply n ° 1*
☐ *Reply n ° 2*
☐ *Reply n ° 3*

2nd QUESTION

<< Question to be inserted by the teacher >>

CORRECT ANSWER

☐ *Reply n ° 1*
☐ *Reply n ° 2*
☐ *Reply n ° 3*

3rd QUESTION

<< Domanda to be inserted by the teacher>>

CORRECT ANSWER

☐ *Reply n ° 1*
☐ *Reply n ° 2*
☐ *Reply n ° 3*

DISCIPLINARY PROCESS	MOD-720-H

PROCESS

DISCIPLINARY PROCESS NO_____
RELATIONSHIPOF NC N °_

PERSON INQUIRED

Mario Rossi (administration operator)

VIOLATIONSVERIFY AND RELATED DOCUMENTATION

Unauthorized access attemptsinformation relating to the design process. Critical level information TO.
The documentation consists of:

- In the report issued on the occasion of the alert by the log management software
- In the form MOD-1020-A- Non-conformity report N °… filled in by the system administrator.

Defensive arguments of the suspect

None of relief

AFTERMATH ASCRIBABLE TO THE INDICATED VIOLATIONS

None

DISCIPLINARY MEASURES ESTABLISHED BY THE MANAGEMENT

Temporary suspension of the employment relationship (with suspension of pay) Report of what happenedto the competent authorities

Date	
Signature Top	
Signatureinvestigated	
RGSI signature	

winplePRO™ MANAGEMENT SYSTEMS

TEMPLATES ISO/IEC 27001:2017 INFORMATION SECURITY

Management System Manual

Description	Guy	Revision	Date	Position	Validity	Destruction
TO	TO	TO	TO	TO	TO	TO

Legend

Guy Insert if internal or external document
Revision Enter revision number (Example: 00)
Date Enter issue date
Position Insert position in the archive (Example: Folder X)
Validity To insert, if applicable, validity of the document (Example: 3 years)
Destruction Enter the retention years after the overrun (Example: 1 year)

Date	
AD signature for approval	

Transmitted

Sheetfor the transmission of controlled distribution documents

Please take charge of the attached documentation:

Number of	Description	Identification	Revision	Of the

☐ to take note of the content

☐ to return to the senderthis undersignedinspace provided together with the outdated document

Broadcast to	Signaturefor receipt	Date of receipt

Date **Signature**

Functional requirementsand information security

Code ofrequirement

Title of the

Specification of the requirement

<< describe in detail the function requested by the customer specifying, for example, what he asks to be able to do, in what circumstances, how, when, the actors, the times, the reasons, the limits, the conditions of

Importance of the requirement for the customer

<< explain the importance that the customer gives to the requirement and, if possible, the reasons for the importance considering the impact that the requirement has on customer satisfaction. In order to rank the requirement, give weight to importance using the following typology: high, medium, low >>

Criticality of the requirement for the organization

<< illustrate the critical issues that the organization will have to face for the subsequent treatment of the requirement. List any concerns due to present and / or future shortcomings and obstacles that the organization may encounter in the treatment of the requirement. If possible, also formulate a solution for each difficulty approach. To the in order to classify the criticality, to attribute an objective level of difficulty using the following typology: tall, medium low >>

Correlations with other requirements

<< indicate briefly what are the correlations of the requirement with the other requirements >>

organization operating system)

Name of the client

Client Order	
Design manager	
Report manager frompart of the customer	
Address tel./mail resp. by the customer	

Design goalsand information security requirements

Nature, duration and complexity of the design

Activitiesplanning

ACTIVITY'	RESPONSIBLE	EXPIRATION	PROJECT OUTPUTS
Graphic interface design	Ing. Guido Mariniello	23/09/2022	Interface style sheet graphics
Algorithm design Design of	Dr. Elena Lodigiano	09/28/2022	Structureof the formula in Matlab
functions ofmanagement	Ing. Claudio Storelli (Coordinator of the previous)	03/10/2022	Drawings

operating system of the organization

VERIFICATION OF THE DESIGN OF THE DAY	<<DATE>>

Name of the client

Client Shop assistant	
Process manager	
Report manager frompart of the customer	
Contact tel./mail resp. by thecustomer	

Inputand design outputs

Giveevidence of the correspondence between design inputs and design outputs so that it can be demonstrated that all inputs were covered by the design

Code	Input	Code	Output
<< 01 >>		<< 01 >>	
<< 02 >>		<< 02 >>	
<< 03 >>		<< 03 >>	
<< 04 >>		<< 04 >>	
<< 05 >>		<< 05 >>	
<< 06 >>		<< 06 >>	

ASSESSMENT

NAME OF THE SUPPLIER AND TYPE OF SUPPLY

MARINO SPA - Hardware

1st FACTOR

Availability shown by the supplier towards the security needs of the organization

EXPRESSYOUR EVALUATION

☐ *1 - Poor* ☐*2 - Mediocre* ☒*3 - Sufficient* ☐*4 - Good* ☐*5 - Excellent*

2nd FACTOR

Effective presence and the actual functioning of its information security management system

EXPRESSYOUR EVALUATION

☐ *1 - Poor* ☐*2 - Mediocre* ☐*3 - Sufficient* ☒*4 - Good* ☐*5 - Excellent*

3rd FACTOR

Safety for information on its supplies, actual value to the organization

EXPRESSYOUR EVALUATION

☐ *1 - Poor* ☐*2 - Mediocre* ☐*3 - Sufficient* ☒*4 - Good* ☐*5 - Excellent*

4th FACTOR

Offer or possibility of information security assistance deemed necessary by the organization

EXPRESSYOUR EVALUATION

☐ *1 - Poor* ☐*2 - Mediocre* ☐*3 - Sufficient* ☒*4 - Good* ☐*5 - Excellent*

5th FACTOR

Convenience of the commercial conditions applied

EXPRESSYOUR EVALUATION

☐ *1 - Poor* ☐*2 - Mediocre* ☐*3 - Sufficient* ☐*4 - Good* ☒*5 - Excellent*

Enter the value of the arithmetic mean of the evaluationsand record it in the MOD-810-A SUPPLIER LIST **Ex: 4.5**

Date	
Signature	

INPUT CONTROL

MOD-814-F

INPUT CONTROL

Supplier:XXX

PO number:xxx

Delivery date:
xx / xx / xxxx

Inspection date:
xx / xx / xxxx

Product control

Code:XX

Product:XX

Elementcontrol	Unit from measur	Value detected	Value of reference	Result C /
Documentation	//	here I'm	//	C.
Times delivery	days	5	5	C.
Integrityof the packaging	//	suitable	//	C.

COMPLIANCEOF THE PRODUCT WITH THE SAFETY REQUIREMENTS		
REQUIREMENT	COMPLIANT	DESCRIPTION NON-COMPLIANCE'
Requirement 1	☒	
Requirement 2	☒	
Requirement 3	☐	*Product packaginghas been compromised during transportation. It highlights a danger of voluntary compromiseof the device received.*
Requirement 4	☒	
Requirement 5	☒	
Requirement no	☒	

N ° pieces

xx

Non-compliance

N: 1

(Evaluate if this non-conformity, in addition to relating to the product, detects any other non-conformities from process according to PROC-1010- ***Non-conformities and corrective actions****. Example: the purchasewas carried out from an unqualified supplier.*

Resultverification

☐ product acceptance
☐ product suspension
☐ waste product
☐ send to_____for internal treatment
☐ request for technical assistance from the supplier
☒madeto supplier
☐ other: _____

Actionto be implemented

Note

RDP (PURCHASES)
Name and signature

PRODUCTION PLAN DATA							
Name / Type product	Unit from to achieve	Peoplefrom use		Date Start estimat	Date end estimat	Date end effectiv	NoteAnd documentationfrom reference
		min.	max.				
Software for the management of land registry of the the	1	6	9	01/01/2022	03/06/2022	03/06/2022	**MOD-813-F- Output planningof the 11/11/2021**

Release	Expiration	Responsible	Check
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐

RISK MANAGEMENT OFPRODUCTION

- Indicaterisks relating to the continuity of production
- Indicate onlyrisks relating to the security of information relating to production activities contemplate in this planand not those that refer to production in general (the latter, in fact, are treated in the safety procedure governing operational safety PSI-12 - Operational safety.

MANAGEMENT OF PRODUCTION RISKS ARISINGFROM PHYSICAL THREATS OR ASSETS MALFUNCTIONING				
Danger and / or risk for the information security dealt with in the process	**Control arranged indicated by the Annex A of ISO 27001: 2017**	**Responsible for effectiveness control**	**Expirationfor implementation control**	**Check**
				☐
				☐
				☐
				☐
				☐
				☐
				☐
				☐
				☐
				☐
				☐
				☐
				☐

PROPERTY'OF THE CUSTOMER | **MOD-815-F**

PROPERTY'OF THE CUSTOMER

Minutesacquisition of customer property (information and assets)				
Customer	**commonof Turin**			
Properties acquired	**State of the properties**	**Reasons for the acquisition**	**Date of acquisition**	**Expected date of**
HardDisk ▪ Intel 882/09/2341 ▪ Format database Microsoft Access ▪ Database documentation cadastral Cadastral documentation in finalized paper format to the design of the software of management of land registry	Harddisk intact and free from virus Databasevirus free The documentationgoes from protocol 56/2006 al protocol 231/2019	References documentary for determination of the design outputs of the software	06/08/2021	20/04/2022

Identificationand traceability of the customer's property				
Cadastral documentation				
Date	**Activities 'on the property'of the customer**	**Position**	**State**	**Checked**
12/12/21	Consultation	Design office	Intact	RDP (PROG)
19/12/21	Typing	Design office	Intact	RDP (PROG)
04/01/22	Segregation	Production office	Intact	RDP (PRO)
	Preparation for return to client	Administration secretariat	Intact	TO

RDP (PRO) for acquisition	RDP (PROG)by acquisition	Customerfor acknowledgment
Name and signature	*Name and signature*	*Name and signature*

QUALITY CHECK'

MOD-817-A

CHECK

Product / service nameand related code

North Area marketing strategy

By the quality control manager and the RGSI		*By the RDP*		
REQUIREMENT	**NOT CONF.**	**TYPE NC**	**ACTION**	**SIGNATURE RESPONSIBLE**
Normalizationdata	//			
Hypothesis testing on break even of the investment	//			
Analysessome data financial of investment	**Analysis is missing of the investments**	**The non-compliance is of omissive type in that the requirement was foreseen analysissome data financial to purpose of support the decisions of investment**	**Carry out the analysissome data financialfor investments**	**RDP. (PRODUCTION)**
Parameters of Statistical reliability	//			

Detection date	
Control manager	

SUBJECT OFMONITORING	RESPONSIBLE FOR PERFORMANCE	AT YOUR PLACE	RESPONSIBLE OF MONITORING	CHECK.
Rolesand in the requirements	RDP (human resources)	15FEBRUARY	RGSI	☒
Estateof responsibility	High management	17MARCH	RGSI	☐
Managementof the network and of the	Administrator of net	21MARCH	RGSI	☐
Software management	RDP (production)	APRIL 22	RGSI	☒
Device management of processing	IT manager	APRIL 22	RGSI	☐
Managementof the headquarters and of the	High management	APRIL 22	RGSI	☐
Managementof plants and devices of safety	IT manager	APRIL 22	RGSI	☒
Training managementturning point	RDP (human resources)	04 MAY	RGSI	☒
Managementtraining delivered	RDP (human resources)	04 MAY	RGSI	☒
Plan management formation	RDP (human resources)	07 MAY	RGSI	☒
Managementof communication (internaland	RDP (communication)	07 MAY	RGSI	☒
Selectionand the management of providers	RDP (outsourcing)	MAY 18	RGSI	☒
Product management not compliant	RDP (production)	MAY 18	RGSI	☒
Managementaudits and non compliance	RDP (production)	22JUNE	RGSI	☒

Date	
Signature	

INTERNAL AUDIT N °:	01
Audit execution date	22/01/2022
Purpose of the audit	**Theaudit purposes are as follows:** ▪ Verify existenceof the documentation relating to the indicated processes ▪ Verify compliance of documentation ai requirements of the standard 27001: 2017 ▪ Check the conformity of the work performedthe established procedures ▪ Check the application of the security checks established by procedures
Object of the audit	**Processesaudited** ▪ Teleworkingand information security ▪ Control of accesses ▪ Encryption ▪ Safetyphysical and environmental information ▪ Operational safety ▪ Safetycommunications ▪ Acquisition, systems development and maintenance ▪ Management of information security incidents ▪ Business continuity managementinformation security ▪ Compliance
Kind of audit	☒scheduled ☐ not programmed **reason** *(if not programmed)***:**
Audit Group	Responsible of audit: Eng. Marco Castaldi InternalAuditor: dr. Alessandro Rossi
Functionsinvolved in the verification	TO RGSI IT Manager Information system manager DPO Administrator of system RDP (asset manager)
Drafted on: 12/12/2021	*Name and signature:*

Date	
Author	

winplePRO MANAGEMENT SYSTEMS

TEMPLATES ISO/IEC 27001:2017 INFORMATION SECURITY

CALL OF MANAGEMENT REVIEW

MOD-930-A

Convocationmanagement review n._ _ _ _ _ **Date _ _ _ _ _**

We hereby inform interested managers that the day xx / xx / xxxx, from xx: xx, is called the meeting for theManagement review, as per point 9.3 of the ISO 27001 ed. 2017.

I aminvited	▪ RGSI ▪ RDP DESIGN ▪ RDP PRODUCTION ▪ RDP MARKETING ▪ RDP PURCHASES ▪ Administrator of system ▪ IT Manager ▪ Information system manager

During the meeting will be discussed the following order of the day

Theinformation security policies (levels A and B)	☒
Thestatus of actions resulting from previous reviews of direction	☒
Thestate of the context in which the organization is operating(changes in internal / external	☒
Do notcompliance and corrective actions	☒
Results of monitoring and measurement	☒
Results in achieving the objectives	☒
Return informationof interested parties	☒
The results of the risk assessment and the status of the floorInformation security plan	☒
The opportunities forcontinuous improvement	☒
Evidence relating to accidentssecurity	☒
Evaluations ofimpact on system changes	☒
Confidentiality Agreements or non-disclosure	☒
Analysis oflogs that trace the activities carried out on	☒
The access rights of users of the information system	☒

The presentconvocation is forwarded to those summoned in the form:

☐paper ☐digital ☐other:

SignatureTO _____

winplePRO MANAGEMENT SYSTEMS

TEMPLATES ISO/IEC 27001:2017 INFORMATION SECURITY

NON-CONFORMITY REPORT

MOD-1010-A

RELATIONSHIP		
Relationshipof NC n °: 08		**Date: 12/21/2022**
☒Greater ☐Minor ☒Danger		
NON-CONFORMITY RELATING TO THE STANDARD ISO 27001: 2017 [check 7.2.2] Awareness, information security education, training and training All organization staffand, when relevant, collaborators must receive adequate awareness, instruction, education and training and periodic updates on organizational policies and procedures, in a way relevantto their work activity.		
Detection of the NC *(anomaly, attack)*	Who took it over	Administrator of system
	At what day and at what	20/12/2022 at 18:30
	With which device	▪ Report of the log management software (alert) ▪ Video surveillance
	On the occasion of	Ordinary monitoring
	Criticality level of information potentially involved	☒Level A ☐Level B
Description of the NC *(anomaly, attack)*	An unauthorized access attempt was made from PC2 - Administration, across the information system, to the Central Server Design Disk. Mr. Mario Rossi (OP. Administration), identified by video surveillance, following your previous biometric identification for accessto the network, he ran the following operations to obtain access to the information system: ▪ He has accessed the login page of the information system ▪ Entered an incorrect password 5 times ▪ He restarted the computer ▪ He regained access to the network using biometric identification ▪ He has accessed the login page of the information system again ▪ He typed an incorrect password 3 times ▪ You have logged out from the network ▪ He turned off the computer	
Processes involved **Damage to devices** **Damage to the information**	The access attempt was made to the information processed by primary processes. The item from customer technical requirements and projects may be of interest. Do notdamage to systems and information is reported	
Analysis of the causes of the NC **(Investigative hypotheses)**	**Mr. Mario Rossi,in an attempt to stealthily access information relating to projects,attempted to access the area reserved for them.** **Hypothesis 1:** **Knowing the effectiveness of the authentication expected from the access control has hoped for temporary inefficiency or random checks that allowed him to take advantageof a technical weakness and stealing information without being identified**	

Executive document index

- Report on the data collected in the year 2022
- Methods of data analysis
- Results of the analysis
- Swot Analysis
- Definitionof the desired scenario
- Risk analysis
- Planninggeneral
- Executive planning

Relationon the data collected

Modeof data analysis