# SECURITY POLICY

TALENTOMOBILE

# Content

# 1. Introduction

TALENTO MOBILE is a global technology company. We are defined by our innovative spirit, our desire to do things well done and our experience in digital projects and solutions.

Although we have already exceeded 5 years of life, we like to live each day as if it were the first. This makes us feel freer, enhances innovation and the flow of ideas and most importantly, ensures that our team is as comfortable as possible, which is directly proportional to the results that clients get from our developments and projects.

The values that describe TALENTO MOBILE are the following:

- Simplicity: We make it simple and effective
- Agility: We use agile methodologies while maintaining quality
- Inspiration: We care about the value of details
- Motivation: We are passionate about our work and it shows

Our solutions apply to the Fintech and Insurtech industry:

- ID Verification: Intelligent and automated identity verification (OCR) tool. Remotely extract and validate information from **personal identification documents** for opening accounts or registering as a new customer.
- Liveness & Facial Biometrics: Software for validating users remotely, comparing biometric features in video and photographs to **avoid identity theft**.
- Digital Onboarding: Unified solution of ID Verification and Liveness & Facial Biometrics in a single product of easy integration into applications. Everything you need for the **creation of remotely verified clients.** The first low code digital onboarding platform on the market.
- Clicquote (Chatbot): Our end-to-end Chatbot solution for **product and service contracting** processes. You will be able to offer a unique user experience in any digital channel Web, Mobile, WhatsApp in record time.
- Perito Digital: Our **computer vision solution for the detection of vehicles, claims and license plates**, which allow to accelerate and digitize the processes of expertise and insurance contracting.
- Videoanalytics: Video and real-time analysis for **multiple biometric identification** and **detection of objects** such as masks or weapons, helping to create safer open spaces.

Our services are adapted to the needs of each project with personalized services:

- UX/UI Design (User Experience): **User-centered** design through quantitative and qualitative research techniques, to offer solutions that really impact our users.

- Custom Development (Development to Create Impact): We help our clients discover and take advantage of technological innovations.
  Providing experience in all phases of life of digital **product** or **service** development.
- Digital Kit Program (Help for the digitization of SMEs and Self-employed): The government of Spain launches the special program **Acelera Pyme**, with which Talento Mobile collaborates as a provider of services and digital transformation.

# 2. Regulatory Framework

The regulatory framework on information security in which TALENTO MOBILE carries out its activity, essentially, is the following:

- Royal decree 3/2010, of 8 January, by which regulates the National Scheme of Security in the field of the Electronic Administration.
- Royal decree 951/2015, of 23 October, of modification of the Royal decree 3/2010, of 8 January, by which regulates the National Scheme of Security in the field of the Electronic Administration.
- CCN-STIC 821 Safety Guide: Safety Standards.
- CCN-STIC 804 Security Guide: Implementation Guide.
- GDPR (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data.
- Organic Law 3/2018, of December 5, protection of Personal Data and guarantee of digital rights.
- UNE ISO/IEC 27001:2014 Information security management systems. Requirements

# 3. Scope

The scope of this policy is defined as follows:

***Information security management system used in:***
***Development, Maintenance, and Implementation of Computer Services in mobile and web applications. For large and small businesses***

TALENTO MOBILE relies on its ICT systems to achieve its objectives. These systems must be managed diligently, taking appropriate measures to protect them against accidental or deliberate damage that may affect the availability, integrity, confidentiality, authenticity or traceability of the information processed, or of the services provided.

The objective of information security is to guarantee the quality of information and the continuous provision of services, acting preventively, supervising daily activity and reacting promptly to incidents.

## 3.1 Mission and objectives

At least the following objectives shall be developed:

a) Use of corporate ICT resources, such as e-mail, Internet access, computer and communications equipment.

b) Management of information assets inventoried, categorized and associated with a manager.

c) Necessary mechanisms so that any person who accesses, or can access the information assets, knows their responsibilities and thus reduces the risk derived from an improper use of said assets.

d) Physical security, so that information assets will be placed in secure areas, protected by physical access controls appropriate to their level of criticality. The information systems and assets contained in such areas shall be sufficiently protected from physical or environmental threats.

e) Security in the management of communications and operations, so that the information transmitted through communications networks must be adequately protected, taking into account its level of sensitivity and criticality, through mechanisms that guarantee its security.

f) Access control, limiting access to information assets by users, processes and information systems through the implementation of identification, authentication and authorization mechanisms according to the criticality of each asset.

g) Acquisition, development and maintenance of information systems, taking into account the aspects of information security in all phases of the life cycle of these systems.

h) Management of security incidents by implementing appropriate mechanisms for the correct identification, recording and resolution of security incidents.

i) Continuity management by implementing appropriate mechanisms to ensure the availability of information systems and maintaining the continuity of their business processes.

## 3.2 Prevention

To defend against threats, departments must apply minimum security measures, as well as ensure that ICT security is an integral part of every stage of the system lifecycle.

Security requirements and funding needs should be identified and included in planning, bids, and tender specifications for ICT projects. Departments must be prepared to prevent, detect, react and recover from incidents.

To ensure compliance with the policy, departments must:

- Authorize systems before entering into operation.
- Request periodic review by third parties in order to obtain an independent evaluation.

## 3.3 Detection

Since services can be rapidly degraded due to incidents, ranging from a simple slowdown to their arrest, services must monitor the operation on an ongoing basis to detect anomalies in the provision of services and act accordingly.

Detection, analysis and reporting mechanisms will be established that reach those responsible regularly and when there is a significant deviation from the parameters that have been pre-established as normal.

## 3.4 Answer

TALENTO MOBILE and its departments must:

- Establish mechanisms to respond effectively to security incidents.
- Designate a point of contact for communications regarding incidents detected in other departments or in other agencies.
- Establish protocols for the exchange of information related to the incident.

## 3.5 Recovery

To ensure the availability of critical services, departments should develop ICT systems continuity plans as part of their overall business continuity and recovery activities plan.

# 4. Security organization

The implementation of the Security Policy in TALENTO MOBILE requires that all members of the organization understand their obligations and responsibilities depending on the position held.

As part of the Information Security Policy, the main roles are identified and detailed as follows:

- Head of Security: César Castillo
- Responsible for Information: Karla
- Head of Service: César Castillo
- Systems Manager: Javier Román
- DPO: Datages Consulting

The following sections specify the roles assigned to each of these roles.

## 4.1 Committees: Roles and Responsibilities

Information Security is an organizational responsibility that is shared with the management of TALENTO MOBILE. Accordingly, it promotes the composition of an Information Security Committee, in order to establish a defined path and support security initiatives.

This Committee is composed of each of the above-mentioned figures and a chairman who will be ultimately responsible for the decisions taken and who will direct the meetings of the Security Committee, informing, proposing and coordinating the activities and decisions.

This role of president initially falls to the head of Security.

The functions of the Information Security Committee are as follows:

- Review of the Information Security Policy and the main responsibilities and proposal for approval to senior management.
- Define and promote the strategy and planning of information security by proposing the allocation of budget and precise resources.
- Supervision and control of significant changes in the exposure of information assets to the main threats, as well as the development and implementation of controls and measures aimed at ensuring the security of such assets.

- Approval of the main initiatives to improve Information Security.
- Supervision and monitoring of aspects such as:
- Main incidents in Information Security.
- Preparation and updating of continuity plans.
- Compliance and dissemination of Security Policies.

## 4.2 Security Manager

It is responsible for the definition, coordination and verification of compliance with the information security requirements defined in the strategic objectives.

The functions of the Information Security Officer are as follows:

- Assistance to the Chairman of the Security Committee in drawing up the agenda for the meetings to be held.
- Coordinate and control the information security and data protection measures of TALENTO MOBILE.
- Supervise the implementation, maintain, control and verify compliance with:
- The information security strategy defined by the Security Committee.
- The rules and procedures contained in the Information Security Policy of TALENTO MOBILE and implementing regulations.
- Supervise the security incidents produced in TALENTO MOBILE.
- Disseminate in TALENTO MOBILE the rules and procedures contained in the Information Security Policy and development regulations, as well as the functions and obligations in terms of information security.
- Supervise and collaborate in the internal or external audits necessary to verify the degree of compliance with the Security Policy, development regulations and applicable laws on the protection of personal data and information security.
- Advise on information security matters to the different operational areas of TALENTO MOBILE.

## 4.3 Systems Manager

It is responsible for ensuring the execution of measures to protect the assets and services of the information systems that support the activity of TALENTO MOBILE.

The functions of the Systems Manager are as follows:

- Develop, operate and maintain the Information System during the life cycle, specifications, installation and verification of its correct operation.
- Define the topology and management system of the Information System establishing the criteria of use and the services available in it.
- Ensure that specific security measures are properly integrated within the overall security framework.
- Select and establish the functions and obligations to the IT Technical Managers in charge of personifying a security management of the assets of TALENTO MOBILE in accordance with the defined security strategy.
- Guarantee that the implementation of new systems and changes in existing ones complies with the security requirements established in TALENTO MOBILE.
- Establish the processes and controls for monitoring the state of security that allow detecting the incidents produced and coordinating their investigation and resolution.
- The person responsible for the System may agree to suspend the handling of certain information or the provision of a certain service if it is informed of serious security deficiencies that could affect the satisfaction of the established requirements.
- This decision must be agreed with those responsible for the affected information, the affected service and the person responsible for Security, before being executed.

## 4.4 Responsible for Information

It is responsible for ensuring the execution of measures for the protection of information, own or of the clients, that are used in the activity of TALENTO MOBILE.

The functions of the Data Controller are as follows:

- It establishes the security requirements for the information managed. If this information includes personal data, the requirements arising from data protection legislation must also be considered.

- Determines information security levels.

## 4.5 Responsible for the Development of the service

He is responsible for ensuring the use of security measures in the services and projects developed by the TALENTO MOBILE teams.

The functions of the person responsible for the development of the service are the following:

- Has the power to establish the security requirements of the services provided related to development
- Describes Development requirements
- Ensures compliance with THE development methodologies of TALENTO MOBILE, as well as the product safety requirements
- Determines the security levels of the service.

## 4.6 Designation Procedures

The person responsible for Information Security will be appointed by the Governing Body on the proposal of the ICT Security Committee. The appointment will be reviewed every 2 years or when the post becomes vacant.

The Department responsible for a service that is provided electronically in accordance with Law 11/2007 will designate the person responsible for the System, specifying their functions and responsibilities within the framework established by this Policy.

## 4.7 Dissemination, updating and revision of the information security policy

The mission of the ICT Security Committee will be the annual review of this Information Security Policy and the proposal for its revision or maintenance.

The Policy will be approved by the Governing Body and will be disseminated so that all affected parties are aware of it.

This Policy will be developed through safety regulations that address specific aspects.

The security regulations shall be available to all members of the organisation who need to know them, in particular those who use, operate or manage the information and communications systems.

## 5. Personal data

The Data Protection Policy and the Manual of Security Measures to which only authorized persons will have access, identify those responsible for the processing of personal data, detail these treatments and expose the corresponding security measures.

All the information systems of TALENTO MOBILE will comply with the security levels required by the regulations for the nature and purpose of the personal data collected in the Security Document.

In application of the principle of proactive responsibility established in the General Data Protection Regulation (GDPR), and the new LOPD, the activities of processing personal data will be integrated into the categorization of systems of the National Security Scheme, considering the threats and risks associated with this type of treatment.

Any other regulations in force on the protection of personal data will also apply.

## 6. Risk management

All systems subject to this Policy shall perform a risk analysis, assessing the threats and risks to which they are exposed.

This analysis will be repeated:

- Regularly, at least once a year
- When the information handled changes
- When the services provided change
- When a serious security incident occurs
- When serious vulnerabilities are reported

For the harmonization of risk analyses, the Safety Committee shall establish a baseline assessment for the different types of information handled and the different services provided.

The ICT Security Committee will boost the availability of resources to meet the security needs of the different systems, promoting horizontal investments. Risk management will be documented in the Risk Analysis and Management report.

## 7. Staff obligations

All members of TALENTO MOBILE have the obligation to know and comply with this Information Security Policy and the Security Regulations, being the responsibility of the Security Committee to provide the necessary means for the information to reach those affected.

All MEMBERS OF TALENTO MOBILE will attend a security awareness session at least once a year.

A continuous awareness program will be established to serve all members of TALENTO MOBILE, in particular those of new incorporation.

Persons with responsibility for the use, operation or administration of ICT systems will receive training for the safe operation of the systems to the extent that they need it to perform their work. Training will be mandatory before assuming a responsibility, whether it is your first assignment or if it is a change of job or responsibilities in it.

Failure to comply with this Information Security Policy may lead to the initiation of the appropriate disciplinary measures, without prejudice to the corresponding legal responsibilities.

## 8. Thirds

When TALENTO MOBILE uses third-party services or transfers information to third parties, they will be made participants in this Security Policy and the Security Regulations that concern said services or information.

This third party will be subject to the obligations established in said regulations, being able to develop its own operating procedures to satisfy it. Specific procedures for reporting and resolving incidents will be established.

It will be ensured that third-party personnel are adequately security-conscious, at least at the same level as that set out in this Policy.

When any aspect of the Policy cannot be satisfied by a third party as required in the previous paragraphs, a report from the Security Officer will be required specifying the risks incurred and how to treat them.

Approval of this report by those responsible for the information and services concerned will be required before proceeding forward.

## 9. Approval of the Document

Document: Security Policy Signed:

Status: Approved

TALENTOMOBILE

# Audit Trail

## Document Details

| | |
|---|---|
| **Title** | English TM_Security Policy_v1.pdf |
| **File Name** | English TM_Security Policy_v1.docx.pdf |
| **Document ID** | 4256b819ffa34e25b9a764fe6e01bbf8 |
| **Fingerprint** | 124e6a4bb11c3bbd5dbeabcc6aba26ad |
| **Status** | Completed |

## Document History

| | | |
|---|---|---|
| **Document Created** | Document Created by Talento Mobile (administracion@talentomobile.com)<br>Fingerprint: 124e6a4bb11c3bbd5dbeabcc6aba26ad | Jun 29 2022<br>09:20AM UTC |
| **Document Sent** | Document Sent to Cesar Castillo (cesar.castillo@talentomobile.com) | Jun 29 2022<br>09:20AM UTC |
| **Document Viewed** | Document Viewed by Cesar Castillo (cesar.castillo@talentomobile.com)<br>IP: 80.28.65.41 | Jun 29 2022<br>02:59PM UTC |
| **Document Viewed** | Document Viewed by Cesar Castillo (cesar.castillo@talentomobile.com)<br>IP: 178.60.128.5 | Jun 29 2022<br>02:59PM UTC |
| **Document Signed** | Document Signed by Cesar Castillo (cesar.castillo@talentomobile.com)<br>IP: 80.28.65.41 | Jun 29 2022<br>03:00PM UTC |
| **Document Completed** | This document has been completed.<br>Fingerprint: bfa435adcf169b8582ebc3cd5b798901 | Jun 29 2022<br>03:01PM UTC |