



TECHNICAL & ORGANIZATIONAL MEASURES FOR INFORMATION SECURITY & DATA PROTECTION

<i>Code</i>	DOC-006
<i>Version</i>	1.0
<i>Document owner</i>	Patrick Nollet
<i>Confidentiality level</i>	Business use only

Approval process

	<i>Name</i>	<i>Date</i>
<i>For the Executive Committee</i>	Laurent Mélon (CIO)	

Update history

VERSION	DATE	AUTHOR	DESCRIPTION OF MODIFICATION
1.0	23/11/2023	Thomas Brichant	First version
1.1	04/09/2024	Thomas Brichant	Adding subcontractor list
	22/10/2025	Patrick Nollet	Annual review, no change
1.2	06/02/2026	Patrick Nollet	Reflecting organization change (Ibexa1) Update subprocessor list

Table of content

1	<i>Introduction</i>	4
1.1	What is Actito?	4
1.2	Why this document?	5
1.3	Audience of the document?	5
2	<i>Information Security Management System (ISMS)</i>	5
3	<i>Organisation of information security</i>	5
4	<i>Risk Management</i>	5
5	<i>Human Resource Security</i>	6
5.1	Candidate selection and Screening	6
5.2	Onboarding process	6
5.3	Security awareness and continuous education	6
5.4	Offboarding process	6
5.5	Confidentiality clause in employments contracts	6
6	<i>Asset management</i>	6
6.1	Asset inventory	6
6.2	Information classification	7
7	<i>Access control</i>	7
7.1	Actito's access control policy	7
7.2	Actito's account protection	7
7.3	Segregation of duty	8
7.4	Least access privilege	8
7.5	Need to use	8
7.6	Onboarding, offboarding, change of position & periodical reviews	8
7.7	Users accountability	9
7.8	Multi-tenant and chinese wall	9
8	<i>Cryptography</i>	9
9	<i>Physical and environmental security</i>	9
9.1	Data processing facilities	9
9.2	Actito's offices	9
9.3	Actito's laptops	10

9.4	USB Mobile Storage Device	10
10	<i>Operations Security</i>	11
10.1	Backup Policy	11
10.2	DDoS and firewalls	11
10.3	Logging & Monitoring.....	11
10.4	Remote access control & Intrusion detection & Prevention	12
11	<i>Communications security.....</i>	12
11.1	HTTPS and SSL.....	12
12	<i>Information Systems Acquisition Development and Maintenance</i>	12
12.1	Secure Development Lifecycle (SDLC)	12
12.2	Teams.....	13
12.3	Development practices	13
12.4	Separation of environments	13
12.5	Environments accesses	13
12.6	High level architecture	14
12.7	Code review & Testing	14
12.8	Release Management.....	15
12.9	Production Data	16
13	<i>Information Incident Management</i>	17
13.1	Service Level Agreement	17
13.2	Status Page	17
13.3	Customer Support.....	17
13.4	Technical vulnerabilities management and Patching policy	18
13.5	Fair use policy	19
14	<i>Business Continuity & Disaster Recovery</i>	19
15	<i>Compliance</i>	19
15.1	Security Audits & Reports.....	19
15.2	Insurances	20
16	<i>Data protection and privacy.....</i>	20
16.1	Actito as “data processor”	20
16.2	Organizational measures to ensure security and protection of PII	21
16.3	Transfer of PII to the customer	24

17	<i>Technical measures to ensure security and protection of PII</i>	24
17.1	Privacy by design and by default.....	24
17.2	Deletion of PII	24
17.3	Restricted access to production Personal Data	25
17.4	Physical access to our offices.....	25
17.5	Computers.....	25
17.6	IT security controls.....	25
18	<i>Contractual agreements with customers</i>	25
18.1	Data Processing Agreements.....	25
18.2	Records of Processing activities.....	25
19	<i>Actito's subcontractors</i>	26
19.1	Sub-contractors list.....	26

1 Introduction

1.1 What is Actito?

Actito is the agile activation platform that enables any marketer to deploy high-performance, data-driven marketing campaigns, without any technical knowledge, in complete autonomy. And all without sacrificing power or performance.

Actito's ease of use, performance and quick learning curve make it unique. Our portal is at the heart of the user experience: customer data management, form creation, scripted campaign construction, access to dashboards and campaign reports, and much more. All our applications are just a click away.

Delivering the right message through the right channel increases conversion rates and guarantees a high return on investment. By taking your customers' preferences into account and personalizing your messages, you offer them an experience that lives up to their expectations, whatever the channel: email, sms, push notification, paper, call center,....

The RGPD has put the spotlight back on the importance of brands protecting their customers' data. Much more than a contract of trust, it's a pledge of quality and respect and, above all, a legal obligation. Respecting your customer is no longer a "nice to have" but a "must have". Today, it's impossible to offer a quality customer experience without a marketing stack. Governance and connectivity therefore represent a real challenge for marketers, but also for software publishers. We've always been ahead of our time, thanks to our extensive connectors and APIs, as well as the personalized support provided by our teams and partners.

1.2 Why this document?

This document aims to provide an overview on the Information Security Management System (ISMS) in place within Actito. It will help prospects, customers and suppliers to assess the maturity of Actito's information security.

1.3 Audience of the document?

This document is intended to 3rd party risk assessors, security departments, information security auditors, CISO, or IT departments of prospects, customers and suppliers.

2 Information Security Management System (ISMS)

The IT Security Team and DPO are managing respectively the Information Security and Data Protection at Actito by running a state-of-art ISMS (Information Security Management System) and PIMS (Personal Information Management System), following the ISO27001 international standard.

3 Organisation of information security

Information Security is managed at Actito by its CIO (Chief Information Officer), and the IT Security Team, directly reporting to the CEO (Chief Executive Officer).

A DPO (Data Protection Officer) has been appointed by Actito to answer questions related to the protection of PII (Personally Identifiable Information), directly reporting to the CEO.

These responsibilities are spread over multiple persons in order to provide a clear segregation of duty while operating the ISMS and PIMS.

Actito policies are approved by Director and CEOs of Actito for their adherence to the company's strategy before being rolled out to the company.

Senior Management is responsible for actively promoting information security within Actito and ensuring that information security responsibilities are allocated and complied with

4 Risk Management

The risk management methodology run by Actito is evaluating risks based on the impact if a risk is getting real, and the likelihood of its realization. Both, impact and likelihood, are scored on a scale of 1 to 5. The final score of a risk is then evaluated by multiplying its impact by its likelihood.

A risk appetite is defined with Management and risk above the risk appetite are treated.

The possible treatments of a risk are:

Mitigation: Selection of security control or controls from Annex A of the ISO 27001 standard or some other security controls

Transfer: Transferring the risks to a third party – e.g. by purchasing an insurance policy or signing a contract with suppliers or partners

Avoidance: Avoiding the risk by discontinuing a business activity that causes such risk

Acceptance: Accepting the risk – this option is allowed only if the selection of other risk treatment options would cost more than the potential impact should such risk materialize

The risk register is owned by the IT Security Team and is reviewed yearly. The risk appetite is decreased at each iteration of the risk assessment.

5 Human Resource Security

5.1 Candidate selection and Screening

Actito's staff is selected through a screening process where their skills and adherence to the culture of the company and background when allowed by local regulation are assessed.

5.2 Onboarding process

Each member of the staff is following an onboarding process during which he/she is following training (up to 4 weeks) in order to ensure that the resource has the skills needed to perform the job.

5.3 Security awareness and continuous education

Actito has deployed a training and awareness program towards its staff:

- Security and Privacy awareness session performed through eLearning platform
- Ad hoc training for limited audience

5.4 Offboarding process

Each leaver of the company will follow a strict offboarding process to ensure, thanks to the asset register, that every asset and user access are deprovisioned or returned to the company.

Exit interviews serve as reminders to former employees regarding their remaining employment restrictions and contractual obligations.

5.5 Confidentiality clause in employments contracts

All our employment contracts include mandatory confidentiality clauses in accordance with GDPR.

6 Asset management

6.1 Asset inventory

Actito's assets as well as 3rd party assets on which the company depends on are assessed once a year. All assets are logged into an asset inventory with the assignment of an owner and the classification of the asset based on its criticality for the company.

The responsibility for the asset inventory and its annual review is the responsibility of the IT Security Team.

6.2 Information classification

A formal “information classification” has been crystallised into a policy ruling, the classification of information, its owner, its treatment, handling procedures, disposal and destruction.

The current information classifications used by Actito are:

- **Public**
- **Business Use Only (default)**
- **Confidential**
- **Restricted.**

7 Access control

7.1 Actito’s access control policy

User administrators have real time access to the list of their users and can upgrade/downgrade rights & access. Default access right are :

- Admin
- Advance User
- User
- Restricted user
- Reviewer
- Transfer box

Administrator can disable an account at any time.

7.2 Actito’s account protection

7.2.1 Actito’s password policy

Password complexity : Password must meet all the following requirements:

- At least 12 characters long
- 3 out of 4 characters type : lowercase, uppercase, number and special character.

Brute force protection : After 5 wrong attempts, a one minute delay is required before the next attempt. Each subsequent wrong attempt increase this delay by 1 minute

Password encryption : All passwords are chosen by the user, encrypted in transit and stored as a hash at rest in our systems

Reset password:

- Password reset link is sent via email and is available 24 hours

- Password caching is not allowed
- Licence administrators can reset password at anytime

7.2.2 Single Sign-On (SSO)

Single Sign-On is available with Security Assertion Markup Language (SAML) 2.0 and Oauth.

7.2.3 MFA (Multi-Factor Authentication)

Actito provides a two-factor authentication (2FA) method using a time-based one-time password. This security layer is activated by default.

The time-based one-time password authentication applications supported are any OTP App, SMS or email. The link between the device and the account can be reset by the licence administrators in the back-office. Once enabled, the 2FA connection is mandatory for every login.

7.2.4 User creation

Invitation link is sent by email to the user. Link is available for 24 hours. If the user hasn't logged in after the link has expired, the user must start a reset password procedure.

The user will need to create a new password on the first login.

7.2.5 Session timeout

Back-office sessions last for 30 minutes (which is prolonged by any action performed on the interface eg: click, content edited, etc.)

7.3 Segregation of duty

Actito has implemented internal technical processes to restrict staff to access customer's licence. Only support team members and employees designated by customer might have access to customer's licence.

7.4 Least access privilege

Actito staff members are provided with the minimal access required to perform their duty.

7.5 Need to use

Staff will only be able to access physical and logical facilities required for their role.

7.6 Onboarding, offboarding, change of position & periodical reviews

Organisational processes are in place to control the provisioning and deprovisioning in case a staff member is joining, or leaving, or changing his/her position in the organisation.

Accesses are reviewed periodically by asset owners in order to verify the accuracy of accesses to their assets.

7.7 Users accountability

Actito logs all actions that have a GDPR and/or access right impact (deleting data, access to statistics, update of access right, etc.)

7.8 Multi-tenant and chinese wall

Actito SaaS, as a multi-tenant solution, handling data from different customers. Each customer's data is separated from the other by a strict "chinese wall" that ensures, through logical controls, the isolation of each Actito's customer. Among other things in place, each Actito's customer owns his logical database.

8 Cryptography

The following requirements for cryptography have been defined:

- In transit : > TLS 1.2
- At rest : filesystem encrypted (AES-XTS for Linux based servers)

Sensitive data (API keys, SSO configuration variable, ...): sensitive data are encrypted with AES-256 with a key provided at runtime to the application.

Access to production servers: SSH Private key is mandatory in order to get access to production servers. These accesses are limited to a limited subset of Actito staff based on a "need to know" and "least access privilege" principles

User passwords are hashed using bcrypt 10 rounds

9 Physical and environmental security

Thanks to the asset inventory maintained by Actito, the location of each mission critical information and IT assets is known. A policy is rolling out in order to ensure that these assets are located in a data processing facility compliant with ISO27001 and/or SOC2 standards.

9.1 Data processing facilities

Our core-business applications are store on our own servers located inside Equinix datacenters. Backup are stored on our own servers located on Atlas Edge datacenters. Both are, amongst other, ISO27001 and SOC2 compliant, ensuring the use of:

Strict visitor policy
Alarm system
Video surveillance equipment (CCTV)
Fire prevention
Climate control systems
Redundancy of power and telecommunication supplies

9.2 Actito's offices

Access to our offices is secured

- Offices are locked outside of office hours
- No production data is hosted in our offices
- CCTV is in place

9.3 Actito's laptops

Actito laptops are governed by policies that enforce technical and operational measures to protect the device and its content. Laptops are verified periodically for their conformity with the policy.

The policy defines, amongst other measures:

- Hard drive encryption
- Antimalware and antivirus protection
- Software updates
- Clear screen, device locking and unattended devices

9.3.1 Hard drive encryption

Even though data cannot be stored locally, data encryption of hard drives is enforced to prevent data leakage due to theft of a Actito's laptop.

9.3.2 Antimalware and antivirus protection

Actito laptops are protected by an antimalware protection that is always active. This antimalware and antivirus protection is managed at the company level for all Actito laptops.

9.3.3 Software updates

Laptop must always be updated to the latest stable version of the software (application and operating system) provided by the editor.

9.3.4 Clear screen, device locking and unattended devices

If the authorized person is not in direct control of the device, all sensitive information must be removed from the screen.

In the case of short absence, the clear screen policy is implemented by locking out of all systems or locking the screen with a password or biometric security (fingerprint). Auto locking rule must be set to lock device automatically after a defined period of time.

In the case of longer absence (eg: holidays), the user must log out from his session.

The policy is also ruling the fact that laptops should never be left unattended if not in a secure area.

9.4 USB Mobile Storage Device

It's strictly forbidden to use any USB mobile storage device on any asset of the organization. Please refer to the data classification policy for the allowed platform to store or share (internally or externally) Actito's data.

10 Operations Security

10.1 Backup Policy

The following types of data are part of our backup policy:

Production data (databases)
Customers' and business information
Cloud software data
Application code

10.1.1 Backup of databases

Actito's databases host the most sensitive and mission critical information of the company. For this reason, all databases containing data are:

- **Replicated:** data are replicated in real time on at least two database nodes, located in distinct datacenters.
- **Backuperd:** data are replicated to our backup datacenter.

Backups testing: Backups are tested for integrity at least once a year

Backups frequency: Backups are performed once a day

Backups retention: Backup are kept for 30 days except Sunday backup that are kept 90 days.

RPO (Recovery Point Objective) and **RTO** (Recovery Time Objective): 24h

10.1.2 Customers' and business information

Documentation, internal files and emails are hosted on Microsoft Cloud in Europe.

Backup of these data is ensured by Microsoft.

10.1.3 Cloud software data

Backup of cloud software are managed by editors.

10.1.4 Application code

Application code is versioned through GIT, backup of the git repository is ensured via regular checkout of the repository.

10.2 DDoS and firewalls

The complete Actito's application infrastructure is protected against DDoS (Distributed Denial-Of-Service) by our firewall. After this line of defense, our infrastructure is protected by network equipment performing load-balancing and traffic throttling / rate limiting, as well as a firewall to deny access to non-public services and protect from common attacks.

10.3 Logging & Monitoring

Actito has put in place adequate tools to log, monitor and alert teams in real-time in case a suspicious behavior is detected.

All logs (application and system) are already shipped and aggregated inside an Elasticsearch cluster.

10.4 Remote access control & Intrusion detection & Prevention

All our servers are protected against intrusions by exclusive access through a management VPN, in conjunction with a protection against brute force attacks. SSH access is always based on private-key authentication.

Services exposed to the internet only do so via the HTTP protocol and are protected by a Level 7 Filtering HTTP-proxy.

IDS is implemented through the use of Unix audit events gathered and centralised on a separate server from the one under surveillance.

11 Communications security

11.1 HTTPS and SSL

All customer's domains are only available through HTTPS.

Back-office is also exclusively accessed through the HTTPS protocol.

Traffic to end-users is encrypted using TLS 1.2 & 1.3 only

The cipher suite used is up-to-date.

12 Information Systems Acquisition Development and Maintenance

12.1 Secure Development Lifecycle (SDLC)

Agile and scrum methodology as well as Kanban frameworks are used in order to drive and manage our developments.

Each request is assigned a type being:

Features: A new feature for the product available to all our customers

Bugs: A correction to an existing feature of the product. Bugs also include incidents.

12.1.1 Features

All features are defined using "User Stories" created together with the Product owner, a representative of the development and QA teams.

Features are analyzed from a security and privacy perspective in order to ensure Privacy and Security by design and by default.

Features are scheduled into Sprints.

In order to ensure the quality of developments, Actito uses strict definitions of "Done" (story is ready to manual user testing).

12.1.2 Bugs

All bugs are evaluated by the Support and Product team and, based on their criticality, are scheduled in a future sprint or retrofitted in the current sprint.

12.2 Teams

We have multiple teams working together to develop, maintain and evolve the Actito software:

Product team (PT)

Agile Development team (Dev)

- Channel Team
- Data Team
- Portal Team

Infrastructure & devops team (IT)

Quality Assurance team (QA)

12.3 Development practices

Actito maintains and operates a single codebase for all its customers. This code is developed with a strong focus on quality and performance. To achieve these goals, different techniques and coding standards are used such as:

Pair programming

Test Driven Development

Code reviews

Actito try to avoid big-bang and/or reinventing the wheel. For these reasons Actito is:

Using continuous integration and deployment for small, incremental steps

Using framework and components whenever it's possible (mainly on new applications)

Evolving existing applications instead of re-starting from scratch

12.4 Separation of environments

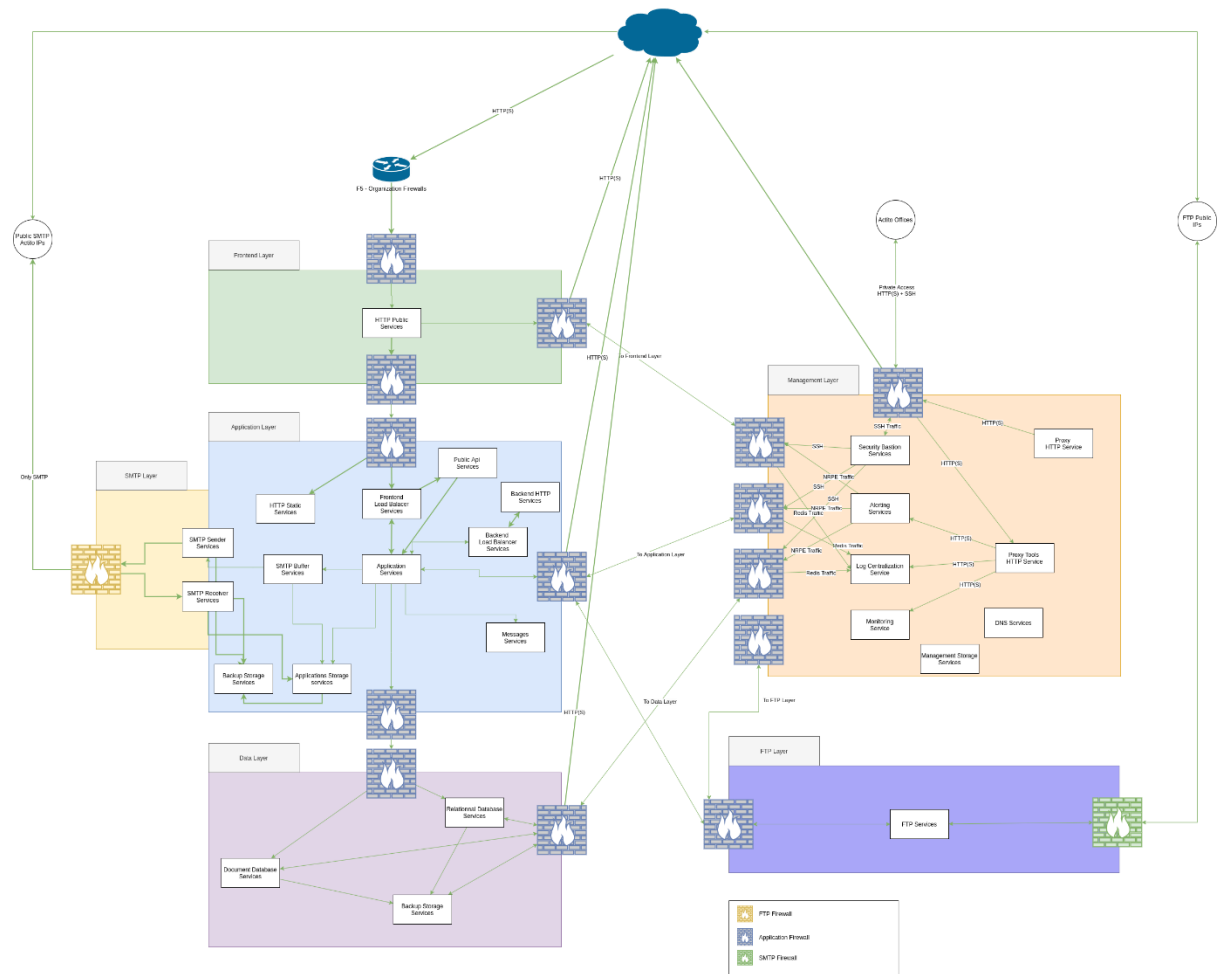
Environments are separated and only production servers contain real “personally identifiable information” (PII), developers and testers are working on dummy test data in the respective environment (local, build, development & pre-prod).

12.5 Environments accesses

Actito has different environments, for development, QA, client acceptance testing and production. Database access is restricted per user on an **assigned role** basis, and per application on a **scope** basis.

Access to the production database is limited to a very limited pool of users.

12.6 High level architecture



12.7 Code review & Testing

The technologies we use include the most advanced frameworks & software components: Java and React.js.

All Actio's components have been developed internally and are updated by our IT team located in Louvain-La-Neuve (Belgium).

12.7.1 Peer Code Review

Code ready for production is countersigned by another internal developers based on the project.

12.7.2 Testing

Testing is a crucial part of our product development, that's why we have a full-time team of QA internally. Testing is performed manually and automatically.

Actito uses a mix of:

Unit tests: automated, micro-service level

Integration tests: automated, application level

End-to-end tests: manual and automated

Regression tests: manual and automated

User acceptance tests: manual

We make use of automated tests whenever it's possible through a test platform (like ThunderClient for all API regression tests).

These tests are automatically triggered by our continuous delivery platform daily.

12.8 Release Management

12.8.1 What is Release Management?

Release management is the process of managing, planning, scheduling and controlling a software build through different stages and environments; including testing, deploying software releases and documentation management

Release management ensures that we are delivering new features while protecting the integrity of existing services.

12.8.2 Objectives

Ensure a high number of successful releases, i.e reducing the number of releases with unexpected outcomes or requiring roll-back.

Maintain a low number of incidents caused by releases.

Create a single documented process for managing all releases.

Ensure that the process is adopted and escalated to management if there are compliance issues.

Improve productivity by establishing standard release processes and tooling.

Harvest lessons learned from the release management process that could be applied to other areas of Service Management.

12.8.3 Policies

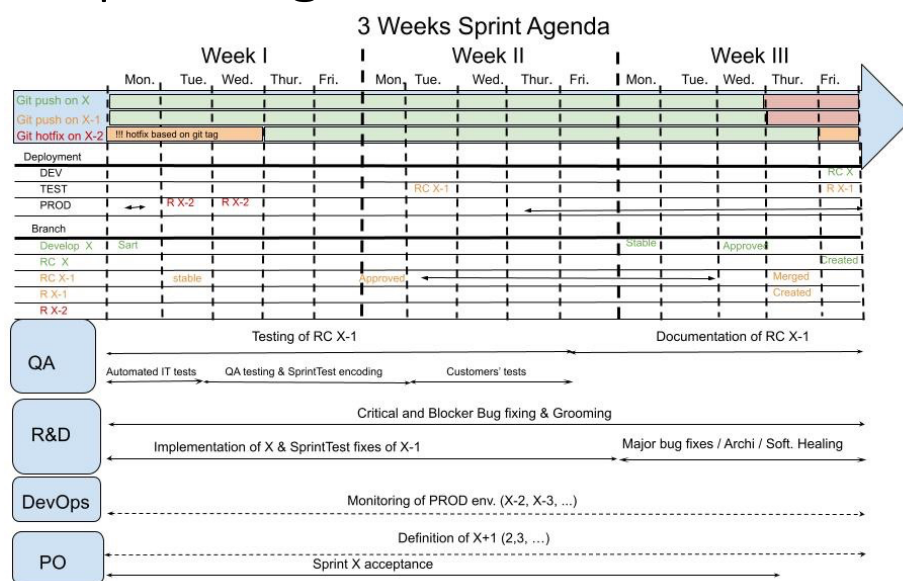
- All projects, bundled changes to an existing service (releases containing multiple enhancements/fixes) and critical changes to an existing service must go through the release management process with appropriate approvals (Product Team, DPO and IT Security Team).
- Whenever possible, changes to an existing service should be bundled together and released on a regular (every 3 weeks) basis using the release management process.
- A single "Release Manager" must be identified for each Release. The Release Manager will be responsible for successful coordination and execution of the Release, as well as ensuring all required documentation related to the Release exists.
- Each release should be well tested and verified prior to implementation by our QA team.

- All implementation work on the release should be completed by the planned End Date/Time.
- Validation that the release has been completed successfully should be confirmed through post-release testing.

12.8.4 Normal Release Workflow

Normal releases deployment has no impact for clients and follow below process:

Sprint Agenda Overview



12.8.5 Scheduled release with potential use impact

The customer is notified of any release that may have an impact on the use of the Actito via

- A notification on the status page: <https://status.actito.com/>
- A notification in Actito

12.8.6 Lesson Learned

Each release must have a post analysis on problems we encountered.

12.9 Production Data

Production data is restricted only to the production environment. Developments and testing are performed on dummy test data.

13 Information Incident Management

13.1 Service Level Agreement

Actito shall guarantee a monthly availability level of 99.5% for his production environment. The uptime percentages and reports shall be available upon request.

Availability refers to the ability for a user to access or edit their campaigns, database, ...

13.2 Status Page

A status page is available at : <https://status.actito.com/>.

13.3 Customer Support

13.3.1 Ticket creation

All Actito's users can contact the Helpdesk by sending an e-mail to support@actito.com.

13.3.2 Office Hours

The period when the Actito Level 1 support is open minimum from 9AM to 6PM CET – during weekdays.

13.3.3 Ticket categorization

Every ticket registered in our ticketing system will be assigned one of the following categories:

User Support: An informative request from a customer to help him using the Actito product effectively and adequately. Ticket is assigned to Level 1

Incident: An unplanned system event, which adversely affects application processing or application deliverables. Ticket is assigned to Level 2

13.3.4 Level 1 support

Level 1 support helps customer to make an efficient use of Actito by referencing documentation whenever possible.

In case of bug, Level 1 identify and make a first investigation.

13.3.5 Level 2 support

When receiving ticket, Level 2 support will try to confirm incident by either witness it in production environment or reproduce it in development, testing or pre-prod environment.

He will then assign a priority depending impact incident has on Actito usability:

Interruption anomaly (P1): a fault that makes it impossible to use an essential function of the software and for which there is no workaround.

Major anomaly (P2): a fault that makes it impossible to use an essential function of the software and for which there is no workaround.

Minor anomaly (P3): a bug that does not affect an essential functionality of the software (e.g. campaign reporting is not considered an essential function as long as it does not prevent campaigns from being sent) or for which there is a workaround that only moderately affects the productivity of the operator

13.3.6 Response Time

The response time measures how long it takes Actito to respond to a support request raised via sending an e-mail to support@actito.com.

Targeted response time is depending of incident severity level :

- **Interruption anomaly:** 2 office hours
- **Major anomaly:** 4 office hours
- **Minor anomaly:** 8 office hours

13.3.7 Incident mitigation

Mitigating an incident aims to minimize the degree of loss or harm due to the occurrence of the undesired event (incident). Mitigation could include temporary solutions such as workarounds, patches, hotfixes or any action that could reduce the impact of the incident (up to putting offline some feature or the full application).

Mitigation time is the targeted time between the handling of the ticket by Actito and the mitigation put in place by our teams and is depending of incident severity level :

- **Interruption anomaly:** Restoration to P2 level within 8 office hours
- **Major anomaly:** Restoration to P3 level within 72 office hours
- **Minor anomaly:** 15 days

13.3.8 Incident remediation

After the mitigation is in place, the root cause of the incident is analyzed in order to create a final solution to the incident to prevent any future occurrence.

Remediation time is the targeted time between the handling of the ticket by Actito and the remediation put in place by our teams and is depending on incident severity level

- **Interruption anomaly:** 32 office hours
- **Major anomaly:** 15 days
- **Minor anomaly:** 60 days

All remediations includes an automatic test set to avoid future regression bugs

13.4 Technical vulnerabilities management and Patching policy

13.4.1 Technical vulnerabilities patching

Technical vulnerabilities patching is prioritized based on the "Common Vulnerability Scoring System"(CVSS) as follows:

BLOCKER	CRITICAL	MAJOR	MINOR	TRIVIAL
---------	----------	-------	-------	---------

PATCHING DELAY	Next business day	5 business days	15 business days)	30 business days	60 business days
-------------------	-------------------	-----------------	-------------------	------------------	------------------

13.4.2 Other patches and updates

Patches are handled whenever developer is working on related project.

13.4.3 Major version changes

- **Major version changes** have to be planned and handled through a project included in the team's roadmap.
- **Time frame:** 6 months
- **How:** detailed project included in the roadmap

13.5 Fair use policy

Actito systems work like a distributed application, with the system using a load balancer to direct the user to a computer node. However, the fairness rules implemented prohibit one user from using all the resources without leaving any for the others.

Hardware is sized so that they can respond synchronously when necessary, thanks to the load balancer.

Resources usage is monitored 24/7. The memory usage of the VMware cluster is targeted at a 75% usage, leaving room for peak activity. If needed, additional units can be deployed. Additional physical resources may be injected into the VMware system in 1 hour if needed.

14 Business Continuity & Disaster Recovery

In order to ensure its high SLAs,

PODs (instances of Actito able to handle up to 500 clients) are highly redundant from hardware to UI.

Actito makes use of 4 data centers

- 2 in France
- 2 in Belgium

One POD is in "standby mode" operational within 24 hours after backup restauration

15 Compliance

15.1 Security Audits & Reports

Actito is running periodic assessments on the security of the product. They can be performed by a 3rd party (external audit) or internally (internal audit).

15.1.1 External audits

15.1.1.1 Penetration test

A penetration test is an authorized simulated cyberattack on Actito's infrastructure and application, performed to evaluate the security of its platform. The test aims to identify vulnerabilities, including the potential for unauthorized parties to gain access to the system's features and data, as well as strengths, enabling a full risk assessment to be completed.

Actito is contracting with external parties to conduct penetration tests missions once a year.

A declassified version of the latest pen test report is available upon request for our active customers.

15.1.1.2 Customers on-demand Audits

Actito works with more than 350 enterprise and organizations across Europe in various sectors (media, banking, retail, FMCG, etc.). Each of our customers has high security and data protection standards. This is why Actito is willing to share the results of audits (with them in order to guarantee the existence, monitoring and continuous improvement of its management systems related to the Information Security (ISMS) and PII (PIMS) by external auditors.

Additional on-demand security audits requests (security assessment and penetration tests) or requirements can be analysed by our IT Security Team.

15.1.2 Internal audits

At the same time, Actito is running audits internally. These audits include:

Vulnerability scan: Actito is constantly scanning its infrastructure against open ports or well known vulnerabilities.

Static Code Analyzer: Sonarqube is used as Static code analyser

15.2 Insurances

Actito's activities are covered by the following insurances:

- Professional Indemnity Cover and Public Liability Cover
- Cybersecurity cover

16 Data protection and privacy

16.1 Actito as "data processor"

When personal data is asked to a campaign's participant, Actito acts as a « data processor », processing data on behalf of its customers (the « data controller »).

Accordingly, Actito has no direct relationship with the individuals whose information it receives from its customers. Actito does not control such information, does not select or determine the specific types of data it processes, and does not determine the purpose for which it is processed.

16.1.1 Data rectification

Actito enables data rectification via the user interface or import.

16.1.2 Data subjects erasure

Actito enables bulk participant erasure, in case the data subject wants to erase personal data (PII) from range of users or manual participant erasure, if the customer is looking to erase all PII concerning a specific user/profile based on their email, first name, last name,

16.1.3 Data subjects export

Actito enables its customer to easily export all data about a specific user (again, based on their email, first name, last name). This will include all data Actito owns.

16.1.4 Marketing consent

Actito helps its customers to obtain the explicit consent from the person whose data are processed, via a clear declaration. Moreover, Actito is able to provide the proof that the person whose data is processed gave them their consent via his "Audit Trail".

Actito enables its customers to manage the Marketing Consent, which is the global consent given by the person for their personal data to be processed for marketing purposes.

16.1.5 Tracking consent

Actito enables its customer to give the possibility to the profiles from their database to choose if they consent that their behavior be tracked for marketing purposes.

16.1.6 Restitution of Data at the end of the collaboration

Customers can export and delete Data at all times. At the end of the collaboration, the accounts & databases of the customer will be deleted withing 1 month.

16.2 Organizational measures to ensure security and protection of PII

16.2.1 Data Protection Officers

Actito commits to always having a DPO that is reachable through the email dpo@actito.com.

We ensure that our Data Protection Officer:

- is involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data.

- does not receive any instructions regarding the exercise of those tasks.

- is bound by secrecy or confidentiality concerning the performance of their tasks, in accordance with Union or Member State law.

- won't be dismissed or penalized by the Controller or the Processor for performing his tasks.

- doesn't perform any such tasks and duties t in a conflict of interests.

Actito will support the Data Protection Officer in performing the tasks referred to in Article 39 of the GDPR by providing the resources necessary to carry out those tasks and access to Personal Data and processing operations, and to maintain his or her expert knowledge.

16.2.2 Human resource measures

Confidentiality clause in employment contracts

See "Confidentiality Clause in Employments Contracts" section

16.2.2.1 Security awareness and continuous education of staff

See 'Security awareness and continuous education' section

16.2.3 Data Breaches procedures

16.2.3.1 Incident intake

Anyone can notify Actito of a security and/or data breach through the following email addresses: dpo@actito.com and/or security@actito.com.

The following information must be provided:

- the nature of the data breach
- categories of data impacted
- number of records
- number of data subjects concerned
- any other information that led you to presume the data breach
- contact details (DPO or any other contact point)

If the information is not sufficient, the person that is investigating the incident will request more information from the person that has reported the breach to Actito.

The DPO team and/or the Security team will acknowledge your request then immediately start to investigate your potential data breach case. An incident ticket will be created in the ticketing system of Actito.

16.2.3.2 Assessment of the incident

The DPO and/or Security team will assess the incoming incident. This investigation will classify the incident in the following cases:

- False positive
- Security breach without PII breach
- Security breach with a PII breach

In case of a "false positive", the incident will be updated in the ticket management system of Actito and the incident will be closed.

16.2.3.3 Incident handling

The security team will go through the following activities:

Containment: The impacted systems will need to be isolated from the operational environment in order to avoid the incident to spread to other assets

Mitigation (optional): The security team will provide a temporary solution in order to fix the issue until a remediation is available

Remediation: The security team will provide a permanent solution to fix the issue

The DPO team will perform the following activities:

Assess the breach: The DPO team with the needed resources will need to assess the breach. This assessment will need to conclude on:

- The category of data that has been breached
- The quantity of data that have been breached
- The impact on the data subject due to the breach

Notification: As a data processor, Actito will inform the data controller without undue delay with the following information:

- the nature of the data breach
- categories of data impacted
- number of records
- number of data subjects
- contact details (DPO or contact point) where more information can be obtained
- measures taken or proposed to be taken to address the personal data breach (including when appropriate, measures to mitigate possible adverse effects)

Document: Actito will also document the data breach detected in a record of personal data breaches and notify authorities

At any stage of an incident, and whatever its category, Actito could request the intervention of a digital forensics in order to collect legal evidence of the breach.

16.2.3.4 Incident closure

After that the incident has been handled, a “post mortem” analysis will be performed and documented. This report will contain:

The root cause analysis

A timeline of the incident

Lessons learned

Action plan

The IT Security Team will make sure that the incident has been correctly documented in the ticketing system.

In case of a PII data breach, the DPO will make sure that the incident has been correctly documented in the personal data breach register.

16.3 Transfer of PII to the customer

16.3.1 Input of PII to customer's information system

Actito is able to push data collected in different ways:

Manual input through Actito interface

Survey completion

API / ETL

- One by one (REST over HTTPS)
- Bulk
 - 1..1 One shot
 - 1..2 Automated

16.3.2 Output of PII to customer's information system

Actito is able to export data in different ways:

Manual export through Actito interface

- Locally
- Remote FTP(s)

API / ETL

- One by one (REST over HTTPS)
- Bulk
 - 1..1 One shot
 - 1..2 Automated

All accesses (export and consultation) of customer data by the Actito staff are logged.

17 Technical measures to ensure security and protection of PII

17.1 Privacy by design and by default

We are also implementing a policy of 'Data Protection by Design and Default' to ensure we are systematically considering the potential impact that every project or initiative might have on the privacy of individuals. This is especially sensitive with the Product people at Actito (designing new features) and, of course, the IT team.

17.2 Deletion of PII

When a deletion request is triggered, the related PII are deleted or anonymized in order to keep them in an aggregated form in the statistical module.

This anonymization of PII is propagated to all database instances. The PII residing into our archives will be destroyed after the retention period of the backup.

All hardware containing PII that needs to be decommissioned will follow a secure deletion procedure of all its hard drives before being removed from our infrastructure.

17.3 Restricted access to production Personal Data

See "Production Data" section.

17.4 Physical access to our offices

See "Physical and Environmental Security" section

17.5 Computers

See Actito's laptop section

17.6 IT security controls

Please refer to sections:

- Asset management
- Access control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications security
- Information Systems Acquisition Development and Maintenance
- Information Incident Management
- Business Continuity & Disaster Recovery
- Compliance

18 Contractual agreements with customers

As part of our contractual agreements with customers, the following GDPR related documents will be issued:

18.1 Data Processing Agreements

Clear contractual agreements with customers according with article 28, namely impeding Actito to disclose, exploit or resell any personal data to third parties.

18.2 Records of Processing activities

In accordance with article 30 (2) of the Regulation, our record of Processing activities includes:

Our contact details, together with those of the Data Controller on whose behalf you are acting and, where applicable, of the Processor's representative and the Data Protection Officer

The categories of processing carried out on behalf of the Data Controllers.

Where applicable, any transfers of the Data to a third-party country together with documentation showing the existence of appropriate guarantees for each transfer.

A general description of Technical and organizational security Measures.

19 Actito's sub-processors

Clear contractual agreements with subcontractors, according with article 28, namely ensure that our processors provide sufficient guarantees to implement appropriate "Technical and Organisational Measures" in such a manner that processing will meet the requirements of this regulation and ensure the protection of the rights of the Data Subject.

Actito takes adequate safeguards when transferring personal data out of the European Economic Area (EEA) or outside any country for which an adequacy decision has been made. Standard Contractual Clauses from the European Commission (or other guarantees provided for in art 46 of the GDPR) are contractualized. Next to this, Actito assesses (Transfer Impact Assessment TIA) if there is anything in the law or practice of the destination country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools and identifies and adopts supplementary measures when needed (encryption with key management by Actito, split processing, ...).

Where that other Processor fails to fulfil its Data protection obligations, we shall remain fully liable for the performance of that other Processor's obligations.

Actito works with subprocessors to carry out processing activities necessary for the provision of services to the customer.

19.1 Sub-processors list

Clear contractual agreements with sub-processors, according with article 28, namely ensure that our Processors provide sufficient guarantees to implement appropriate Technical and Organisational Measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the Data Subject.

Where that other Processor fails to fulfil its Data protection obligations, we shall remain fully liable for the performance of that other Processor's obligations.

The list of sub-processor is present in the signed contract.

Annex 1: Definitions

“Data Breach” means a Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal data transmitted, stored or otherwise processed;

“Data Controller” means the natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of Personal data; where the purposes and means of such processing are determined by Union or Member State law, the Controller or the specific criteria for its nomination may be provided for by Union or Member State law;

“Data Processor” means a natural or legal person, which processes Personal data on behalf of the Controller;

“Data Protection Officer” (“DPO”) means a person who is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements;

“Data Subject” means an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

“Organisational Measures” mean the measures relate to the system's environment and particularly to the people using it.

“Personal Data” means any information relating to an identified or identifiable natural person (‘Data Subject’);

“Processing” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as

collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

“Supervisory Authority” means an independent public authority which is established by a Member State pursuant to Article 51;

“Technical Measures” mean the measures that directly involve the IT system.