TOLUNA OPERATION & SUPPORT PROCESS

1 INTRODUCTION

1.1 PURPOSE

This document describes the processes used to monitor the technical platform and provide Client support for the Toluna Start™ service offerings.

This process describes the:

- Structure and roles of Toluna's support organisation
- Tools used for providing Client service
- Instructions for clients to effectively interact with Toluna's support organisation.

This document will address three main areas:

a. Client support;
b. Default management and systems platform monitoring;
c. Maintenance.

1.2 SCOPE

Any Toluna Digital Platform stakeholder can submit a support request:

- Functional queries to help improve Toluna Start™;
- Technical issues: follow-up and supporting information;
- Bug report: follow-up and delivery plan.

This monitoring and support control process applies to:

- Software that has been released to production.
- Hardware used with Toluna Start™
- Security organisation

The following product types are not included in this monitoring and support control process:

- Beta and test applications and systems platforms
- Interim or temporary products created during the course of a project
- Any specific items or products intended for individual use only

1.3 DEFINITIONS

Term	Definition
Issue	An item that someone has submitted to the monitoring and support control system that describes a problem, a requested enhancement, a proposed change in requirements for a product under development, or a new project being proposed.
Stakeholder	Someone who is affected by or who can influence the project.

1.4 ROLES AND RESPONSIBILITIES

Role	Description
Client support team	Receive and manage all Client requests. This team is composed of 3 service levels, ranging from assisting Client with daily usage of the application, assisting with workarounds due to system limitations, triaging with R&D for hotfix needs and keeping Client informed as needed. Support is restricted to general technical support to assist Client in performing business functions on their own. Support does not include extensive training on how to use the software, nor does it include scripting of Surveys or input of content.
Infrastructure team	Responsible for monitoring the Toluna Start™ platform. They will handle all network and infrastructure issues on the Toluna Start™ platform.
IT Management Team	Person(s) in charge of all production and support operations and especially in charge of guaranteeing availability and performance of the Toluna Start™ platform.

2 SUPPORT PROCESS

2.1 OBJECTIVES

Support services are available during the following business hours Monday to Friday:

In Europe and Asia from 9.00 to 18.00 CET:
France: + 33 1 4089 7171
UK: +44 (0) 20 8832 1725
DE: +49 (0)69870019940

In North America from 9.30 to 18.30 EST (14:30 to 23:30 CET): North America: + 1 (866) 315 1456
Email: customer-support@toluna.com

95% of all email requests should be responded to within 4 business hours from submission of request.

2.2 PROCESS

Support process is based upon a helpdesk tool which includes the following features:

- Each request is tagged with a unique ticket number for tracking and management purposes.
- All exchanges, even phone conversations will be confirmed by mail and logged within Toluna's support system.
- After initially reporting an issue, the requester will receive a unique ticket number. Email requests will receive an automatic confirmation email with the associated unique ticket number.
- The requester is automatically informed by email when a ticket is closed.
- The status of tickets will be as follows:
  - New - Open and handled
  - Pending - Waiting for Client feedback
  - On hold – waiting system correction/development
  - Closed
  - Deleted

  A closed ticket can be re-opened in the case of a misunderstanding.

  Each mail sent to customer-support@toluna.com automatically creates a ticket with the 1st level of Client Support.

3 PLATFORM MONITORING

3.1 OBJECTIVES

Services provided by the monitoring process are:

- Guarantee a 24/7 monitoring and supervision of Toluna Start™
- Guarantee 99.5% availability rate for Survey access excluding planned maintenance.
- Guaranteed performance relates to the following services:
  - Mailing of invitations
  - Survey participation
  - Website availability

3.2 INCIDENT ESCALATION PROCESS - THIS IS FOR EMERGENCY SITUATIONS ONLY

The escalation process is handled by the infrastructure and/or Client support teams in charge of monitoring the platform and will react as fast as possible to alert based on the nature of the issue.

A Level 1 infrastructure team is available on a 24/7 basis. Based on the actual issue, there is an on-call team available for enhanced support emergency needs.

Alerts are escalated appropriately in less than an hour to the appropriate resource for further action.

3.3 MONITORING PLATFORM

Platform monitoring is based upon different tools:

- Pingdom performs automatic check on portal availability and alerts by email
- Netscaler monitors all services and alerts on failure
- SolarWinds Orion is used for application monitoring and troubleshooting
- Various application logging

4 MAINTENANCE OPERATIONS

4.1 OBJECTIVES

The maintenance operations organisation provides:

- Planning of technical operations, including anticipated impact and duration of each operation
- Confirmation communication after all technical operations are completed.

4.2 PROCESS

Operations and communications are planned as bellow:

- Minor maintenance operations requiring no downtime need not be communicated to clients.
- Major operations requiring less than 4 hours of downtime should be communicated at least 1 week before the planned event. Toluna digital services team will send an email to inform all customers that will be affected. This email contains the schedule information (day, start time, planned duration) and the reason for the operation.
- Highly complex operations requiring more than 4 hours should be communicated a minimum of 1 month prior to scheduled operation. Toluna digital services team will send an email to inform all customers that will be affected. This email contains the schedule information (day, start time, planned duration) and the reason for the operation. At the end of the operation Toluna sends a communication to inform customers that the service is up and running again.

TOLUNA'S SECURITY POLICIES

Below you will find an overview of **Toluna Start Platform Security Architecture.**

Information security is of paramount importance to Toluna and our Toluna Start Platform (the "Application"), is designed with high security standards.

Application is designed based on Secure SDLC and secure programming standards. Application related risks are mitigated as per OWASP guidelines. Application is subject to annual vulnerability assessment and penetration testing as part of continuous security assessment. Internal security assessment is also conducted by Toluna's security team based on release schedule.

Application is hosted out of AWS EU region, with high availability and robust security. All requests to application go thru various security check designed as part of defence-in-depth architecture. Web Application Firewalls are used to inspect any incoming request with malicious payloads, any malformed request is filtered before reaching to application.

Application servers, database and any associated schema is stored in EU region and not replicated outside. Toluna also follows robust backup process, all backups are managed within AWS infrastructure.

To ensure credential security of our Clients/panellists sensitive data like passwords are always encrypted with salt, which makes it highly secure. As per Clients' requirements other sensitive data and PIIs can be also stored as encrypted. Data transfer on public channels is always encrypted with TLS using strong encryption.

Toluna has extensive experience in running ISO 27001 accredited applications and the Enterprise Community Application and complies with the ISO 27001 requirements.

Toluna has also institutionalised various security polices as part of internal security program. Toluna has well documented Information Security Policy, Acceptable Usage Policy, Data Destruction policy among other technical and administrative policies to ensure effective security program.

There is a documented Incident Response Procedure which is followed by Toluna to address any security incident/breach.

All Toluna staff attends annual training on incident response plan as well as security awareness. Toluna ensures that it responds in a consistent manner, with appropriate leadership and technical resources, to any incident that threatens the availability, confidentiality and integrity of information resources.

The following is the typical lifecycle of a security incident response:

- Discovery
- Reporting
- Escalation
- Containment
- Investigation
- Eradication and Restoration
- Reporting
- Business Stakeholder Communication
- Client Communication