IRIS IAM Service Level Agreement (SLA)

This document is a template for creating a Service Level Agreement (SLA). Version 1.0 (2014-02-21)

Comments & usage guidance

- *This template provides a generic structure to be applied for defining and documenting a Service Level Agreement between a service provider and a customer or group of customers.*
- *For this template and its contents, the terminology (terms and definitions) according to FitSM-0 applies.*
- *The following template assumes that the SLA will be agreed for a single service, but it may be easily adapted to cover multiple services.*

This file is part of the FitSM series of standards for lightweight service management in federated IT infrastructures. It is intended to form the basis of documentation for those implementing (IT) service management following the FitSM approach or related frameworks. It may be edited to fit the needs of the specific area of application.

For more information on FitSM visit www.fitsm.eu.

SLA For IRIS-IAM

1. General

This agreement is made between IRIS-IAM user, represented by IRIS and IRIS-IAM management team, represented by STFC SCD Federation Enabling Service Group to cover the provision and support of the service as described hereafter.

This SLA is valid from [date(pending)] onwards.

1.1. Named Parties:

- IRIS IAM Product Owner: Tom Dack
  thomas.dack@stfc.ac.uk

- IRIS IAM Service Manager: Donald Chung
  donald.chung@stfc.ac.uk
- IRIS Project Manager: Anjali Bhatt
  anjali.bhatt@stfc.ac.uk

2. Scope & description of the service

This SLA applies to the following service:

- IRIS-IAM Service

The IRIS Identity and Access Management (IAM) is a single sign on service created for use by IRIS systems and related organisations. It uses federated identities from university credentials to allow users to log on to a service without having to create new accounts.

This service is maintained and managed by the Federation Service Team, Scientific Computing Department, STFC.

3. Service hours & exceptions

The service operates during the following hours:

- The IRIS-IAM login service aims to provide 24/7 access to a login service for the user

The following exceptions apply:

- General maintenance hours between **9:00AM – 11:00PM (Europe/London) every Wednesday**
  - Operation should be considered **At-Risk** during this period where our system administrator may perform the necessary maintenance needed for IRIS-IAM.
- Service may be interrupted due to reasons such as but not limited to the list below

- o Application of updates and performing necessary maintenance to the IRIS-IAM service at a time decided by the IRIS-IAM service manager
  - o Suspension of service due to factors outside the control of the service provider (STFC SCD Federation Enabling Service Group) such as but not limited to the following
    - ▪ Maintenance or failure of the underlying hardware at the data centre
    - ▪ Maintenance or failure of the network
    - ▪ Maintenance or failure of the database owned by STFC data service team that host the user data of IRIS-IAM
- Any planned maintenance or interruption of service will be communicated to the customer as detailed in section 6, Service Level Targets
  - o For these maintenance/upgrade, we will aim to deliver these changes via a robust change control process using the Tier 1 Grid PP change control framework. (Please share).

4. Service components & dependencies

The service covered by this SLA is made up of the following (technical and logical) service components:

- User registration and account activation
- Provision and access to IRIS-IAM management dashboards
- Provision and access to the IRIS-IAM federation login service through OAuth and SAML
- Provision and access to the IRIS-IAM token API

5. Support

The services covered by the scope of this SLA are provided with the following level of support:

- The IRIS-IAM support team provides working-hours support. The team will operate in accordance with STFC business hours at RAL with holidays and site closure observed.
  - o STFC core hours:
    - ▪ Mon-Thur: 10:30 AM – 15.30 PM
    - ▪ Fri: 10:30 AM – 15:00 PM

5.1. Incident handling

Disruptions to the agreed service functionality or quality will be handled according to an appropriate priority based on the impact and urgency of the incident. In this context, the following priority guidelines apply:

- Priority level 1 (PL1) - A failure of the IRIS-IAM with high impact on customer or a core service a customer is running. The customer is unable to operate at all. Or customer will operate at a high level of security risk
  - o Example:
    - ▪ Full IRIS-IAM shutdown where user is unable to reach the website

- Security flaw discovered in IRIS-IAM and downstream identity management that will result in threat to the global IRIS-IAM service
- Priority level 2 (PL2) - A major service component of IRIS-IAM is impacted. Some functions can continue but it is a major issue for users
  - Example:
    - Customer is unable to reach or control via dashboard but still able to provide direct login services
- Priority level 3 (PL3) - A global failure in auxiliary functionality of IRIS-IAM is impacted
  - Example:
    - Unable to retrieve desired attributes from IRIS-IAM API
- Priority level 4 (PL4) - A singular failure in auxiliary login functionality of IRIS-IAM is impacted
  - Example:
    - A failure for users to login via SAML federation using login from users' institution but the issue is limited to a specific or a specific group of institutions.
- Priority level 5 (PL5) - A minor issue with known technical workarounds, which the IRIS-IAM management team will develop.
  - Example:
    - A user is unable to log-on to their account via SAML, but encounters no issue via direct login using IRIS-IAM username and password
- Priority level 6 (PL6) - A minor issue, with planned or pending fixes
  - Example:
    - If a user inquires about the ability for IAM service admin to disable OIDC reply for client but not remove it where it is a feature or fix planned to be added in future releases of INDIGO IAM.

Response and resolution times are provided as service level targets (see section 6).

5.2. Fulfilment of service requests

In addition to resolving incidents, the following standard service requests are defined and will be fulfilled through the defined support channels:

- Initial response to user inquiry. For example, account issues such as forget passwords
- Request for user registration and on-boarding including decision to accept, reject or on hold for user to provide more information/justifications; documentation to aid user to login/ navigating to different service.
- Request for group management such as creating a or new membership request a group
- Responding to Privacy and Security concerns
- Technical support for IAM such as assistance for integrating IAM to other services.

Response and fulfilment times are provided as service level targets (see section 6).

6. Service level targets

The following are the agreed service level targets for IRIS-IAM, the timeframe specified in target begins when IRIS-IAM support team receive report from users and when the issue is escalated/resolved:

Service level parameter	Target
Incident handling	
Priority level 1 (PL1) - Full IRIS-IAM failure	Restore service within 3 business hours of report received, if the incident is reported within STFC RAL business hours. If the 3 hours window exceed the core business hours of the day, this period will continue when the next working day start.
Priority level 2 (PL2) - A major management component of IRIS-IAM is impacted	Issue resolved within 1 working day.
Priority level 3 (PL3) - A global failure in auxiliary functionality of IRIS-IAM	Initial reply to customer within 1 working day and issue resolved within 3 working days.
Priority level 4 (PL4) - A singular failure in auxiliary login functionality	Initial reply to customer within 3 working days and issue resolved within 5 working days.
Priority level 5 (PL5) - A minor issue with known workarounds	Initial reply to customer within 5 working days and methods developed by IRIS-IAM management team communicated to customers 3 weeks.
Priority level 6 (PL6) - A minor issue with planned or pending fixes	This will be dealt with in accordance with the INDIGO IAM development cycle.
Upgrade, Maintenance and Downtime management	
Emergency maintenance to carry out urgent work essential to the security or operation of IRIS-IAM.	Endeavour to notify customer at least 2 working days in advance.
Communication of service at-risk period where **interruption to service is not expected** but there is a non-negligible risk to the service.	At least 1 week of notice via agreed communication channels.
Communication of service downtime period where interruption to service is expected to be **less than 6 hours**.	At least 2 weeks of notice via agreed communication channels.
Communication of service downtime period where interruption to service is expected to be **more than 6 hours**.	At least 3 weeks of notice via agreed communication channels.
User service request handling	
Initial response to user inquiry For example, account issues such as unable to login and forget passwords.	Reply to customer request within 5 working days with follow up reply after customer response within 5 working days until the enquiry is resolved.
Request for user registration and on-boarding	Initial decision to accept/reject the request or request for additional information for user identity/intention will be made within 2 working days The changes will be applied within 1 working day in accordance with the decision.

Request for group management	
	Group management for groups with a delegate manager, response times fall out of the scope of this SLA. For a central request managed by the IAM team: Initial decision to accept or reject, or a request for further information to be made within 2 working days. Follow up decision should be made within 2 working days, upon receipt of requested information For a request with a delegated manager: If a request has not been processed within 2 working days, the IAM team will escalate this to the relevant managers. If there is no response within the following 2 working days, the IAM team will re-escalate. This process shall repeat as required.
Responding to Privacy and Security concerns	Reply to customer requests within 4 hours, in line with IRIS security policy with issues forwarded to the INDIGO IAM developer team or other relevant parties. Aim to resolve and address the concerns within 3 weeks.
Technical support for IAM such as integration support	Reply to customer request within 5 working days with follow up reply after customer response within 5 working days until support is no longer required.

7. Limitations & constraints

The provisioning of the service under the agreed service level targets is subject to the following limitations and constraints:

- Support is limited to business hour of RAL, on-call support is out of scope for this service.
- Failure or maintenance of RAL data centre such as power cut or network issue
    - The underlying hardware is provided by the STFC RAL data centre thus issues and service interruptions in relation to this factor is governed by the SLA between the IRIS-IAM service management team and hardware provider
- Failure or maintenance of database cluster
    - The database is provided by the STFC data service thus issues and service interruptions in relation to this factor is governed by the SLA between the IRIS-IAM service management team and database provider
- Failure of wider UK network
    - The IRIS-IAM is an online service and subject to the status of wider internet.

- Failure of another component not directly under the control of IRIS-IAM service management team.

8. Communication, reporting & escalation

8.1. General communication

The following contacts will be generally used for communications related to the service in the scope of this SLA:

Customer contact for the service provider	IRIS Project Manager (Deputise: Anjali Bhatt (STFC,RAL,SC) <anjali.bhatt@stfc.ac.uk>)
Service provider contact for the customer	iris-iam-support@gridpp.rl.ac.uk
Service provider contact for service users	According to defined support channels such as but not limited to the following: - Email - Federation services customer portal https://stfc.atlassian.net/servicedesk/customer/portal/31/group/120 Contact Person: IRIS-IAM Product Owner: Tom Dack (STFC, SCD, RAL) IRIS-IAM Service Manager: Donald Chung (STFC, SCD, RAL)

8.2. Regular reporting

As part of the fulfilment of this SLA and provisioning of the service, the following reports will be provided:

Report title	Contents	Frequency	Delivery
Annual Service Report of IRIS-IAM	[Brief specification of the contents]	Annually at IRIS Collaboration meeting	IRIS Collaboration meeting

8.3. SLA violations

The service provider commits to inform the customer, if this SLA is violated or violation is anticipated. The following rules are agreed for communication in the event of SLA violation:

- Breaches of SLA will be handled within the IRIS governing framework.

8.4. Escalation & complaints

For escalation and complaints, the defined service provider contact point shall be used, and the following rules apply:

- If the customer/user is unsatisfied with our service and wishes to escalate the issue, they should contact the IRIS Management team.

9. Information security & data protection

The following rules for information security and data protection apply:

- Information security and privacy of IRIS-IAM is governed by the IRIS security and privacy policy
- User data are protected under the UK's Data Protection Act 2018.

10. Additional responsibilities of the service provider

The IRIS-IAM service team shall provide training and up-to-date documentation on how to utilise features of IRIS-IAM to enable users to fully take advantage of IRIS-IAM capabilities.

11. User responsibilities

The user shall:

- Sign and comply with the acceptable use policy of IRIS-IAM.
- Response to inquiry of IRIS-IAM service manager.
- Provide the necessary information for IRIS-IAM service manager to make decisions that guarantees the privacy, security and integrity of the IRIS-IAM ecosystem in an accurate and timely manner.
- Carry out essential security assessment to ensure the security of their system/service integrated with IRIS-IAM.

Failure to comply may result in suspension of service or customer accounts with further breach escalated within IRIS governing framework.

12. Review

There will be reviews of the service performance against service level targets and of this SLA at planned intervals with the customer according to the following rules:

- We aim to review our service performance with customer annually at the IRIS Collaboration Meeting.
- Any time in agreement between the IRIS governing body and the IRIS-IAM service management team.

13. Glossary of terms

For the purpose of this SLA, the following terms and definitions apply:

User: Refers to the user of IRIS-IAM service

Customer: Refers to IRIS who is the budget holder of this service

Reply: refers to non automated message from a member of the team to user

INDIGO IAM: The underlying software developed by INFN, to power the IRIS-IAM

Business Hours: Refers to STFC RAL core business hours observing any site closure and holidays

- STFC core hours:
  - Mon-Thur: 10:30 AM – 15.30 PM
  - Fri: 10:30 AM – 15:00 PM

Working Day: refers to the RAL working days excluding site holiday/closure

14. Document control

Document ID	IRIS-IAM/Service/SLA/0001/v0.3
Document title	SLA on IRIS-IAM
Definitive storage location	Confluence/Program it into HTTP in the about us page? URL: [fill this in]
Document owner	Thomas Dack (STFC, SCD, RAL), Donald Chung (STFC, SCD, RAL),
Version	V0.3
Last date of change	25th June 2024 (Europe/London)
Next review due date	[Date]
Version & change tracking	V0.3 – First public draft