

Foundation Service Level Agreement For Computing Division IT Services

CD DocDB Document 4042-v2

Approvals

By signing below, all parties agree to the terms and conditions described in this Agreement.

Computing Division Management:

Name	Title	Signature	Date
Mark O. Kaletka	LSCS Quadrant Head		
(Stephen A. Wolbers)	(SCF Quadrant Head)	(quadrant not covered as yet)	
(Patricia McBride)	(SCP Quadrant Head)	(quadrant not covered as yet)	
(Robert S. Tschirhart)	(FPE Quadrant Head)	(quadrant not covered as yet)	
Victoria A. White	Division Head		

Computing Division Services:

Name	Title	Signature	Date
Chuck Hoffman	Service Desk Manager		
Brian McKittrick	Incident Manager		
Jack Schmidt	Service Level Manager		

Customer(s):

Name	Title or Customer Org.	Signature	Date

Agreement Schedule

Effective Date: 3/11/11
 Expiry Date: 3/11/12
 Review Cycle: Annual

Document Change Log

Revision	Date	Change Description	Prepared By	Approved By
V0.9	02/25/2010	Draft	Robert D. Kennedy	
V1.0	10/04/2010	Uniform v1.0 Drafts	Robert D. Kennedy	
V2	3/11/2011	Release	Jack Schmidt	

Table of Contents

1 INTRODUCTION.....4

 1.1 EXECUTIVE SUMMARY..... 4

 1.2 KEY DEFINITIONS..... 4

2 SERVICE OVERVIEW.....6

3 RESPONSIBILITIES.....6

4 COMPUTER SECURITY CONSIDERATIONS6

5 SERVICE SUPPORT PROCEDURE7

 5.1 REQUESTING CD SERVICE SUPPORT 7

 5.2 STANDARD ON-HOURS SUPPORT..... 7

 5.3 STANDARD OFF-HOURS SUPPORT..... 7

 5.4 SPECIAL SUPPORT COVERAGE..... 7

 5.5 SERVICE BREACH PROCEDURES..... 8

6 SERVICE TARGET TIMES AND PRIORITIES8

 6.1 RESPONSE TIME..... 8

 6.2 RESOLUTION TIME..... 8

 6.3 INCIDENT AND REQUEST PRIORITIES 8

 6.4 CRITICAL INCIDENT HANDLING..... 9

 6.5 VIP USERS..... 10

 6.6 DEFAULT ESCALATION PATH 10

7 CUSTOMER REQUESTS FOR SERVICE ENHANCEMENT.....10

8 SERVICE CHARGING POLICY10

9 SERVICE MEASURES AND REPORTING.....10

APPENDIX A – KNOWN ISSUES 10

1 Introduction

1.1 Executive Summary

The goal of the Foundation Service Level Agreement (Foundation SLA) is to collect in one place the definitions and common features of Computing Division Service Level Agreements. The Foundation SLA has three objectives:

- Set common service expectations with minimal document repetition to form a foundation for all other SLAs to re-use,
- Serve as a broad minimal SLA for all Computing Division IT services and their customers while detailed Service Level Agreements are drafted and negotiated.
- Serve as an SLA for the Service Desk to CD IT service customers.

1.2 Key Definitions

Many of the definitions below come from ITIL, a body of best practices in IT Service Management. For more ITIL terminology, please refer to [this online glossary](#).

1.2.1 Customer, Provider, and User Roles

The **Customer** is the recipient of a service, typically the role that negotiates and pays for a service on behalf of Users. For the purposes of this document, Customer usually refers to the organization which requests and receives a service for its members.

The **Provider** is role responsible for delivering and supporting a service for Users.

The **User** is typically an individual within a Customer organization who uses the service on a regular basis. A User, however, may also be a service maintained by the Customer such as a data reconstruction service which uses the Provider's service for its own implementation.

1.2.2 Hierarchic and Functional Escalation

In **Hierarchic Escalation**, a ticket is passed from the current point of contact up the management chain to someone with greater authority.

In **Functional Escalation**, the ticket is passed from the current point of contact to someone with greater technical expertise.

1.2.3 Incidents and Requests

"An **Incident** is any event which is not part of the standard operation of a service which causes, or may cause, an interruption to, or a reduction in the quality of that service," according to ITIL v2.

A **Critical Incident** is the highest priority incident, one in which a highly visible and important service depended upon by many users is no longer operable and there is no acceptable work-around. The exact definition of what constitutes a critical incident may be clarified by each service.

A **Request**, in a service management context, is a request for information, a standardized change to a service or access to a service. Unlike an incident, a request does not involve the interruption or threat of interruption of an already provisioned service.

Note that the Remedy tool has a different interpretation of these terms for historical reasons which can cause confusion. ITIL Incidents and Requests as defined above may be tracked by either Incident Tickets or by Request Tickets in Remedy, depending on which Remedy module created the ticket and how the ticket is being used. This document refers only to ITIL Incidents and Requests, not the ticket types used in Remedy.

1.2.4 Response and Resolution Times

The **Response Time** is measured from when the ticket is entered into the Remedy tool (by the user or the Service Desk personnel) to when an acknowledgement is returned to the user by e-mail and the ticket status is set to “in progress”. This is the amount of time required to record and acknowledge the ticket. Time is only counted during the on-hours support period for a service.

The **Resolution Time** is measured from when the ticket status is set to “in progress” in the Remedy tool to when the ticket status is set to “resolved” in the Remedy tool. Time spent in the “pending” state is not included in the resolution time. If a ticket is re-opened, then time is continues to be counted until the ticket is again set to “resolved”. Time is only counted during the on-hours support period for a service. This reflects the amount of time required to resolve, but not necessarily close, the ticket. Resolution means that a service is restored (if the ticket reports an incident) or a request fulfilled (if the ticket contains a request). After resolution, as a separate step, the user is asked whether the resolution is satisfactory and if the ticket may be closed. Time is only counted during the on-hours support period for a service.

1.2.5 Service Restoration and Request Fulfillment

Service Restoration refers to the resolution of an Incident. Restoration of a service is judged from the user view of the service that is delivered. An incident is resolved by either the provider solving the underlying error in the service or the provider delivering an acceptable work-around to the user while the underlying error is investigated. A service is restored so long as the user may continue to do their work which depends upon that service.

Request Fulfillment refers to the fulfillment of a Request, which occurs when the requested information is delivered, the requested change is made in the production system, or the requested access to a service is made available to the user.

Since restoring established services takes precedence over provisioning new services, service restoration tends to be treated with greater urgency than request fulfillment.

1.2.6 Standard Support Hours

The following are default definitions for service support hours to encourage uniformity:

- **8 x 5** Monday through Friday, 8am – 4:30pm U.S. Central Time, not including Fermilab work holidays.
- **12 x 7** Every day, 8am – 8pm U.S. Central Time, including Fermilab work holidays. The response time however may be slower on weekends and Fermilab work holidays, which should be clarified by those services offering this support.
- **24 x 7** Every day, all of the time. The response time however may be slower on weekends and Fermilab work holidays, which should be clarified by those services offering this support.

Service Response and Resolution Times are impacted by the stated service support hours. An 8 x 5 service with 8 hour response time is in effect promising to respond within 8 business hours (weekdays, 8am – 4:30pm, non-holidays), not 8 wall-clock hours. A ticket entered for this service on Friday at 2pm may not be responded to until Monday 1:30pm.

2 Service Overview

The service will provide in this section a description of the service and its features or a reference to a customer-accessible controlled document containing such a description.

3 Responsibilities

The Customer, Users, and Providers are expected to abide by applicable Fermilab policies, including but not limited to:

- [Fermilab Policy on Computing](#)
- [Guidelines for Incidental Computer Usage](#)
- [Fermilab Human Rights Policy](#)
- [Fermilab Director's Policy Manual](#)

4 Computer Security Considerations

Computer Security incidents are to be reported through the mechanisms defined in the FCIRT Incident Response Procedure document on the [Computer Security Policies web page](#).

5 Service Support Procedure

5.1 Requesting CD Service Support

Access to all Computing Division IT services may be requested through the CD Service Desk, via the [Remedy tool](#), or by phone (630-840-2345). More information about requesting service can be found at the [Service Desk web portal](#).

5.2 Standard On-Hours Support

5.2.1 Hours

All Computing Division IT services shall maintain at least 8 x 5 On-Hours support.

5.2.2 Support Details

Critical incident response requires a phone call to the Service Desk (630-840-2345). Users cannot initiate critical incident response with the current Remedy tool interface.

The requestor or proxy should be available for consultation after reporting an incident or submitting a request, and will provide their preferred contact information in the service ticket or phone call to facilitate response by the Service Desk and the service support group involved. If the requestor or proxy is not available, then the assigned service provider may not be able to query important information or coordinate computer access in order to restore service or fulfill a request in a timely fashion. If a service provider is waiting to contact a requestor or proxy, the associated Remedy ticket is put into the “pending” state, and time spent in “pending” is not counted against Response or Resolution time targets.

5.3 Standard Off-Hours Support

5.3.1 Hours

While many Computing Division IT services will offer some form of Off-Hours support, not all do. Please see the appropriate service definition and service level agreement for details. Those services which do offer Off-Hours support shall offer enhanced support for critical incidents.

5.3.2 Support Details

Computer security incidents always qualify for Off-Hours critical incident response.

Off-Hours support is provided via phone (630-840-2345) for critical incidents only. Off-Hours paging of service experts currently requires this phone call approach to report an incident. Individual services may have a specific definition of what other incidents qualify for off-hours versus the next business day response.

5.4 Special Support Coverage

The service will provide in this section a description of the kinds of special support coverage that may be arranged, if any, and how this may be negotiated ahead of time.

5.5 Service Breach Procedures

The IT Service Level Management process determines how service breaches (failures to meet service level agreement goals or conditions) will be handled to prevent recurrence and mitigate the consequences. In general, this process involves offline interaction between the Service Level Manager and customer. If appropriate, individual services may provide a description of how specific service breaches are to be handled operationally.

6 Service Target Times and Priorities

6.1 Response Time

The response time target for incident tickets for CD services is eight (8) business hours or less. The response time target for service request tickets is sixteen (16) business hours or less. CD service providers will meet each of these targets for 90% of tickets assigned to them. Please see the appropriate service level agreement for details.

6.2 Resolution Time

There is no resolution time target across services due to the wide variety of incidents and requests being handled. Each service shall provide some guidance on the expected resolution time for the most frequent incidents and requests to help set user expectations. Please see the appropriate service level agreement for details.

6.3 Incident and Request Priorities

The **Priority** for incidents and requests is determined by a combination of the **Impact** and the **Urgency**. The **Impact** is driven by how many people are affected, and whether there is a serious business or financial loss at risk. The **Urgency** is driven by whether the user can do other tasks or use a work-around for a time, or whether a time-critical task is blocked. Users can only set the **Urgency** of a Remedy ticket directly. The **Impact** is determined by the service personnel from the ticket description field written by the user. **Urgency** and **Impact** then determine the **Priority** in the Remedy tool.

The priority assigned any ticket may be re-adjusted by service personnel after consultation with the user.

Adjusting the incident or request ticket priority is necessary to allow the complete context of an incident or request to be taken into account. A “laptop malfunctioning” may be considered at most medium priority without context, and this may be the initial priority setting. From the text description or after consulting with the user, the service personnel may learn that the “Division Financial Manager’s laptop malfunctioning during the budget season” or “scientific conference presenter’s laptop malfunctioning on the day before leaving to the conference” is a more complete statement of the incident which may be considered much higher priority than normal,

perhaps even critical priority. Until the complete picture is understood by both service personnel and the user, the priority cannot be set appropriately.

CD Service Providers shall respond to an incident or request according to the following priority table:

Impact \ Urgency	Extensive Service is out for Enterprise	Significant Service is out for many users or degraded for Enterprise	Moderate Service is out for 1 user or degraded for many	Localized Service is degraded for 1 user
Critical <i>Based on event</i>	Priority - Critical Respond – 1 H Resolve – 5 H	Priority - High Respond – 4 H Resolve – 35 H (1.5 D)	Priority - Medium Respond – 8 H Resolve – 97 H (4 D)	Priority - Medium Respond – 8 H Resolve – 97 H (4 D)
High <i>Required</i>	Priority - High Respond – 4 H Resolve – 35 H (1.5 D)	Priority - High Respond – 4 H Resolve – 35 H (1.5 D)	Priority - Medium Respond – 8 H Resolve – 97 H (4 D)	Priority - Low Respond – 8 H Resolve – 172 H (7 D)
Medium <i>Important</i>	Priority - Medium Respond – 8 H Resolve – 97 H (4 D)	Priority - Medium Respond – 8 H Resolve – 97 H (4 D)	Priority - Medium Respond – 8 H Resolve – 97 H (4 D)	Priority - Low Respond – 8 H Resolve – 172 H (7 D)
Low <i>Desirable</i>	Priority - Medium Respond – 8 H Resolve – 97 H (4 D)	Priority - Low Respond – 8 H Resolve – 172 H (7 D)	Priority - Low Respond – 8 H Resolve – 172 H (7 D)	Priority - Low Respond – 8 H Resolve – 172 H (7 D)

Note that the “hours” specified in the table are driven by the On-Hours Support defined for the service in question. Incident ticket response within 16 hours for a service with 8 x 5 support means response within 2 business days. Response within 16 hours for a service with 24 x 7 support means response within 0.67 calendar days.

6.4 Critical Incident Handling

A critical incident is the highest priority incident, one in which a highly visible and important service depended upon by many users is no longer operable and there is no acceptable work-around. In addition to the faster response expectations listed in the priority/response table, critical incidents move to the front of the incident report queue and may be handled by a distinct Critical Incident Management process.

Critical incident response requires a phone call to the Service Desk (630-840-2345).

6.5 VIP Users

Services permit customers to designate a small number of their users, **VIP Users**, to have enhanced service due to their critical roles in the Fermilab organization. VIP users' incidents are labeled as such to allow them to be handled judiciously to insure the best possible response and resolution times for the incident priority setting and available resources. Examples of potential VIP users might be the Field Financial Officer for a division or the Director of the Laboratory. (Note that VIP status is technically associated with specific user names, not with roles.) Only a few VIP users may be defined and few changes made to the VIP user list per unit time due to the added administrative and support burden involved.

6.6 Default Escalation Path

Unless stated otherwise, for all CD services, escalation due to response time agreement breaches is hierarchic escalation, not functional escalation. This insures that response time-driven escalation is towards a single accountable role, the Computing Division Head, rather than possibly moving endlessly around an escalation loop from one service provider to another.

7 Customer Requests for Service Enhancement

The service will provide in this section a description of how customer requests for service enhancement are to be made. A description should cover more than just the initial service request submission, but also describe how requests for enhancement are managed, prioritized, and progress is communicated back to requestors over time.

8 Service Charging Policy

No changes are planned as of February 25, 2010 to the Computing Division policy on service charging.

9 Service Measures and Reporting

The service will provide in this section a description of the service measures and reporting that customers and providers may use to track service performance.

Appendix A – Known Issues

1. Response Time Definition (Section 1.2.4)
 - a. While this Response Time definition works in the tool, we need to consider the impact that our actual practices would have on it. "In progress" implies more than just acknowledgement. "Assigned" is too early to stop the response time clock IMHO because it does not provide any assurance that the support group

- assigned accepts responsibility for the ticket (correct assignment given available information).
- b. Whatever our decision on the exact definition of Response Time, we should check that the documented definition precisely matches the Remedy tool definition as configured to insure odd values later are trusted to be real rather than edge cases in the tool's response time definition.
 - c. Standard reports should be developed and linked (Section 10).
 - d. How does the response time definition apply in the case of automated ticketing from monitoring systems?
 - e. Proposed alternative definition: from t0 to time of last assignment. We might live with t0 to first assignment if that is easier to capture in the tool for now.
2. Business Hours Definition (Section 1.2.6)
 - a. Does this single uniform business hours definition work with services that are accustomed to varying personal work hours? Some services have a support process that accommodates this flexibility, but others may not.
 3. VIP User List management
 - a. VIP User List management procedures have not yet been documented. VIP User List change requests should arrive by ticket. The SLM and the Incident Manager should sign off on these requests. Separate issue: note that Remedy does not support service-by-service opt-in/opt-out. Either all services support the concept from the tools point of view or no services support it.
 4. Document repository location for:
 - a. SLAs are "formally" archived in CD DocDB. This tool however is limited in how it presents bundles of documents together, including historical snapshots that are distinct from the released version of controlled documents. We will also maintain an up-to-date copy in a clearly identified area in the SLM sharepoint area, which should be visible to all employees and users.
 - b. SLM Process Documents are handled the same way as SLAs.
 - c. How can we present the SLM/SLA information together with a link to Incident Management Process to help customers understand the holistic picture of Service-User interaction for incidents and requests.