LARGE SYNOPTIC SURVEY TELESCOPE

Large Synoptic Survey Telescope (LSST)

Disaster Recovery Plan

Iain Goodenow and Robert McKercher

LPM-101

Latest Revision Date: September 3, 2013

Change Record

Version	Date	Description	Owner name
1	7/22/2013	Initial release	Robert McKercher
1.2	8/8/2013	Teams consolidated; member names changed; Call Tree simplified and clarified	R. McKercher
1.3	9/3/2013	Added emergency contact list as appendix	R. McKercher
	10/4/2013	Placed under formal project-level change control via LCR-156	R. McKercher

Table of Contents

The LSST Disaster Recovery Plan

Summary

The LSST Disaster Recovery Plan (DRP) captures, in a single document, all of the information describing the LSST Project Office's (LSSTPO) ability to withstand a disaster and the processes that must be followed to achieve disaster recovery.

Definitions of Terms

Emergency Contact List (Document-14948)

Glossary of Abbreviations (Document-11921)

Glossary of Definitions (Document-14412)

The LSST Disaster Recovery Plan

1 Purpose

In the event of a disaster, the LSST Project Office's (LSSTPO) first priority is to prevent the loss of life. Before any secondary measures are undertaken, LSSTPO will ensure that all employees and any other individuals on the organization's premises are safe and secure.

After the safety of employees and other individuals has been secured, LSSTPO will enact the steps outlined in this Disaster Recovery Plan (DRP) to restore the organization's groups and departments to business-as-usual as quickly as possible. This includes:

- Preventing the loss of resources such as hardware, data, and physical IT assets
- Minimizing IT-related downtime
- Keeping the business running in the event of a disaster

The DRP also details how the plan is to be tested and the document maintained.

2 Scope

The LSST DRP takes into consideration all of the following:

- Network Infrastructure
- Servers Infrastructure
- Data Storage and Backup Systems
- Data Output Devices
- End-user Computers
- Organizational Software Systems
- Database Systems
- IT Documentation

This DRP does not apply to non-IT related disasters.

3 Definition of a Disaster

A disaster can be caused by man or nature and results in LSSTPO IT Services being unable to perform all or some of their regular roles and responsibilities for a period of time. LSST defines disasters as the following.

- One or more vital systems are non-functional
- Building unavailable for an extended period of time but all systems are functional within it
- Building is available but all systems are non-functional
- Building unavailable and all systems are non-functional

The following events can result in a disaster, requiring this Disaster Recovery document to be activated

- Fire
- Power Outage
- Theft
- Terrorist Attack
- Natural Disaster (e.g. Earthquake)

4 Disaster Recovery Teams & Responsibilities

In the event of a disaster, different groups will be required to assist IT Services in their effort to restore normal functionality to LSST employees. The different groups and their responsibilities are as follows:

- Disaster Recovery Lead(s)
- Facilities Team
- Network Team
- Server Team
- Applications Team
- Operations Team
- Senior Management Team
- Communications Team

The lists of roles and responsibilities in this section have been created by LSST and reflect the likely tasks that Disaster Recovery Team members will be responsible for performing. In some disaster situations, Disaster Recovery Team members will be called upon to perform tasks not described in this section.

4.1 Disaster Recovery Lead(s)

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role will be to guide the disaster recovery process. All other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs at LSST, regardless of their department and existing managers.

4.1.1 Role and Responsibilities

- Make the determination that a disaster has occurred and trigger the DRP and related processes.
- Initiate the DR Call Tree
- Be the single point of contact for and oversee all of the DR Teams.
- Determine the magnitude and class of the disaster
- Determine what systems and processes have been affected by the disaster
- Determine what first steps need to be taken by the disaster recovery teams

- Ensure that all decisions made abide by the DRP and policies set by LSST
- Organize and chair regular meetings of the DR Team leads throughout the disaster.
- Present the state of the disaster to the Management Team and the decisions that need to be made.
- Organize, supervise and manage all DRP tests and author all DRP updates.
- Notify the relevant parties once the disaster is over and normal business functionality has been restored.
- Create a detailed report of all the steps undertaken in the disaster recovery process.

4.1.2 Contact Information

Name	Role/Title	Work Phone #	Mobile/Home Phone #
Victor Krabbendam	Primary Disaster Lead	520-626-2496	520-429-1980
Iain Goodenow	Secondary Disaster Lead	520-318-8385	520-401-0362

4.2 Information Technology Systems Team

The Information Technology Systems Team will be responsible for all issues related to the Network, Server(s), and Applications. They will be primarily responsible for providing baseline network and server functionality and ensuring and validating appropriate application performance

The IT Team will be responsible for

a) Assessing damage specific to any network infrastructure and for provisioning data and voice network connectivity including WAN, LAN, and any telephony connections internally within the enterprise as well as telephony and data connections with the outside world.

b) Providing the physical server infrastructure required for the enterprise to run its IT operations and applications in the event of and during a disaster.

c) Ensuring that all enterprise applications operate as required to meet business objectives in the event of and during a disaster.

4.2.1 Network Roles and Responsibilities

- In the event of a disaster that does not require migration to standby facilities, the team will determine which network services are not functioning at the primary facility.
- If multiple network services are impacted, the team will prioritize the recovery of services in the manner and order that has the least business impact.
- If network services are provided by third parties, the team will communicate and co-ordinate with these third parties to ensure recovery of connectivity.
- In the event of a disaster that does require migration to standby facilities the team will ensure

that all network services are brought online at the secondary facility.

- Once critical systems have been provided with connectivity, employees will be provided with connectivity in the following order:
    - All members of the DR Teams
    - All Chief level and Executive Staff
    - All IT employees
    - All remaining employees
- Install and implement any tools, hardware, software and systems required in the primary and/or standby facility.
- Summarize any and all costs and provide a report to the Disaster Recovery Lead summarizing their activities during the disaster.

4.2.2 Server Roles and Responsibilities

- The team will determine which servers are not functioning.
- If multiple servers are impacted, the team will prioritize the recovery of servers in the manner and order that has the least business impact. Recovery will include the following tasks:
    - Assess the damage to any servers
    - Restart and refresh servers if necessary
- Install and implement any tools, hardware, and systems required in the primary facility.
- Summarize any and all costs and provide a report to the Disaster Recovery Lead summarizing their activities during the disaster.

4.2.3 Applications Roles and Responsibilities

- In the event of a disaster, the team will determine which applications are not functioning at the primary facility.
- If multiple applications are impacted, the team will prioritize the recovery of applications in the manner and order that has the least business impact. Recovery will include the following tasks:
    - Assess the impact to application processes
    - Restart applications as required
    - Patch, recode or rewrite applications as required
- Install and implement any tools, software and patches required in the primary facility.
- Summarize any and all costs and provide a report to the Disaster Recovery Lead summarizing their activities during the disaster.

4.2.4 Contact Information

Name	Role/Title	Work Phone #	Mobile/Home Phone #
Iain Goodenow	Systems Administrator	520-318-8385	520-401-0362
Steve Grandi	NOAO CIS Manager	520-318-8228	
George Angeli	Systems Engineering Mgr	520-318-8413	520-975-9732

4.3 Facilities and Operations Team

The Facilities and Operations Team will be responsible for all issues related to the physical facilities that house IT systems, including the tools employees need to perform their roles as quickly and efficiently as possible. They will be responsible for assessing the damage to and overseeing the repairs to the primary location in the event of the primary location's destruction or damage. They also will need to provision all LSST employees in an alternate facility and those working from home with the tools that their specific role requires.

4.3.1 Role & Responsibilities

- Assess or participate in the assessment of any physical damage to the primary facility.
- Ensure that measures are taken to prevent further damage to the primary facility.
- Work with insurance company in the event of damage, destruction or losses to any assets owned by LSST.
- Ensure that appropriate resources are provisioned to rebuild or repair the main facilities in the event that they are destroyed or damaged.
- Summarize any and all costs and provide a report to the Disaster Recovery Lead summarizing their activities during the disaster.
- Maintain lists of all essential supplies that will be required in the event of a disaster.
- Ensure that these supplies are provisioned appropriately in the event of a disaster.
- Ensure sufficient spare computers and laptops are on hand so that work is not significantly disrupted in a disaster.
- Ensure that spare computers and laptops have the required software and patches.
- Ensure sufficient computer and laptop related supplies such as cables, wireless cards, laptop locks, mice, printers and docking stations are on hand so that work is not significantly disrupted in a disaster.
- Ensure that all employees that require access to a computer/laptop and other related supplies are provisioned in an appropriate timeframe.
- If insufficient computers/laptops or related supplies are not available the team will prioritize distribution in the manner and order that has the least business impact.

- Maintain a log of where all of the supplies and equipment were used.
- Summarize any and all costs and provide a report to the Disaster Recovery Lead summarizing their activities during the disaster.

4.3.2 Contact Information

Name	Role/Title	Work Phone #	Mobile/Home Phone #
Daniel Calabrese	Business Manager	520-626-1262	520-471-0598
Victor Krabbendam	Project Manager	520-626-2496	520-429-1980

4.4 Communications Team

The Communications Team will be responsible for all communication during a disaster. Specifically, they will communicate with LSST's employees, clients, vendors and suppliers, banks, and even the media if required.

4.4.1 Role & Responsibilities

- Communicate the occurrence of a disaster and the impact of that disaster to LSST employees, partners, clients and vendors.
- Communicate the occurrence of a disaster and the impact of that disaster to media contacts, as required.
- Summarize any and all costs and provide a report to the Disaster Recovery Lead summarizing their activities during the disaster.

4.4.2 Contact Information

	Role/Title	Work Phone #	Mobile/Home Phone #
Steven Kahn	Director	520-621-0194	650-283-9109
Victor Krabbendam	Project Manager	520-626-2496	520-420-1980
Daniel Calabrese	Business Manager	520-626-1262	520-471-0598
Suzanne Jacoby	Communications Officer	520-626-1195	520-490-6683

4.5 Disaster Recovery Call Tree

In a disaster recovery or business continuity emergency, time is of the essence so LSST will make use of a Call Tree to ensure that appropriate individuals are contacted in a timely manner.

- The Disaster Recovery Team Lead calls all other Team Leads (Blue cells).

- Team Leads call all team members (Green cells).
- In the event a team lead is unavailable, the DR Lead assumes responsibility for subsequent calls until a team member is contacted. The first team member to be contacted assumes subsequent calls to all other team members.
- Each team lead will keep a hard copy of the LSST employees phone list offsite in the event that the online Contacts Database is inaccessible.

Contact	Office Number	Mobile Number
Disaster Recovery Lead Victor Krabbendam	520-626-2496	520-429-1980
IT Lead (also Secondary Disaster Recovery Lead) Iain Goodenow	520-318-8385	520-401-0362
Team Member Steve Grandi	520-318-8228	520-429-1980
Team Member George Angeli	520-318-8385	520-975-9732
Facilities and Operations Team Lead Daniel Calabrese	520-626-1262	520-471-0598
Communications Team Lead Steven Kahn	520-621-0194	650-283-9109
Team Member Victor Krabbendam	520-626-2496	520-429-1980
Team Member Daniel Calabrese	520-626-1262	520-471-0598
Team Member Suzanne Jacoby	520-626-1195	520-490-6683

5 Data and Backups

This section explains where all of the organization's data resides as well as where it is backed up to. Use this information to locate and restore data in the event of a disaster.

5.1 Data in Order of Criticality

	Data	When Backed Up	Backup Location
1	Active Directory Services and Data Files	Weeknights	Local server with copy of Friday backup copied to external HD and to tape. Tape

			is stored off-site (Iain's home)
2	Active Directory Services and Applications	Weeknights	Local server with copy of Friday backup copied to external HD and to tape. Tape is stored off-site (Iain's home)
3	Databases and Websites	Weeknights	Local server with copy of Friday backup copied to external HD and to tape. Tape is stored off-site (Iain's home)
4	Terminal Services and Databases	Weeknights	Local server with copy of Friday backup copied to external HD and to tape. Tape is stored off-site (Iain's home)

6 Dealing with a Disaster

If a disaster occurs, the first priority is to ensure that all employees are safe and accounted for. After this, steps must be taken to mitigate any further damage to the facility and to reduce the impact of the disaster to the organization.

Regardless of the category that the disaster falls into, dealing with a disaster can be broken down into the following steps.

1) Disaster identification and declaration.
2) DRP activation.
3) Assessment of current and prevention of further damage.
4) Backup facility activation.
5) Restoring IT functionality.
6) Repair and rebuild primary facility.

6.1 Disaster Identification and Declaration

Since it is almost impossible to predict when and how a disaster might occur, LSST must be prepared to find out about disasters from a variety of possible avenues. These can include

- First hand observation;
- System Alarms and Network Monitors;
- Environmental and Security Alarms in the Primary Facility;
- Security staff;
- Facilities staff;
- End users;
- 3rd Party Vendors; and
- Media reports.

Once the Disaster Recovery Lead has determined that a disaster had occurred, s/he must officially

declare that the company is in an official state of disaster. It is during this phase that the Disaster Recovery Lead must ensure that anyone who was in the primary facility at the time of the disaster has been accounted for and evacuated to safety according to the company's Evacuation Policy.

While employees are being brought to safety, the Disaster Recovery Lead will instruct the Communications Team to begin contacting the authorities, if necessary, and all employees not at the impacted facility that a disaster has occurred.

6.2 DRP Activation

Once the Disaster Recovery Lead has formally declared that a disaster has occurred s/he will initiate the activation of the DRP by triggering the Disaster Recovery Call Tree. The following information will be provided in the calls that the Disaster Recovery Lead makes and should be relayed during subsequent calls.

- That a disaster has occurred.
- The nature of the disaster (if known).
- The initial estimation of the magnitude, impact and expected duration of the disaster (if known).
- Actions that have been taken to this point.
- Actions that are to be taken prior to the meeting of Disaster Recovery Team Leads.
- Scheduled meeting place and time for the meeting of Disaster Recovery Team Leads.
- Any other pertinent information.

If the primary Disaster Recovery Lead is unavailable to trigger the Disaster Recovery Call Tree, the responsibility shall fall to the secondary Disaster Recovery Lead.

6.3 Assessment of Current and Prevention of Further Damage

Before any employees from LSST can enter the primary facility after a disaster, appropriate authorities must first ensure that the premises are safe to enter.

The first team that will be allowed to examine the primary facilities once it has been deemed safe to do so will be the Facilities Team. Once the Facilities Team has completed an examination of the building and submitted its report to the Disaster Recovery Lead, the Disaster Senior Management, Networks, Servers, and Operations Teams will be allowed to examine the building. These teams will be required to create an initial report on the damage and provide this to the Disaster Recovery Lead within 24 hours of examining the facilities.

During each team's review of their relevant areas, they must assess any areas where further damage can be prevented and take the necessary means to protect LSST assets. Costs for necessary repairs or preventative measures to protect the facilities must first be approved by the Disaster Recovery Team Lead.

6.4 Backup Facility Activation

LSST systems will need to be restored to a backup facility when the Disaster Recovery Lead determines that the nature of the disaster is such that the primary facility is no longer sufficiently functional or

operational to sustain normal business operations.

6.5 Restoring IT Functionality

Refer to Section 7 of this document.

6.6 Repair & Rebuild Primary Facility

Primary Facilities must be returned to an operable condition before the organization can return to operations. The tasks required to achieve operable condition will be variable depending on the magnitude and severity of the damage. Specific tasks will be determined and assigned only after the damage to Primary Facilities has been assessed.

7 Restoring IT Functionality

Should a disaster actually occur and LSST need to exercise this plan, this section will be referred to frequently as it contains information that describes the manner in which LSST's information systems will be recovered.

7.1 Current System Architecture

All LSSTPO services are hosted in Tucson. Some services used primarily for subsystem work are hosted or provided by LSSTC institutional members.

7.2 IT Systems

PDC	Domain Controller	Win2003	E-mail and Backup Software for servers
SDC	Domain Controller	Win2003	Terminal Server: Enterprise Architect, Primavera, other miscellaneous
Webserver01	Domain Controller	Win2003	Hosting Windows related websites: DocuShare, Primavera ASPX
SQLsServer01	Member Server	Win2003	Several MS-SQL databases: Primavera; Enterprise Architect
LSSTWeb	Server	CentOS 6	Primary web server, VM Host
Trac	VM-Server		DM services: Trac, GIT, Subversion
ListServ	Server	Fedora 10	Mailman list server
LSST-PDM	Server	Win2003	Telescope and Site ePDM server

8 Plan Maintenance & Testing

While efforts will be made initially to construct this DRP in as complete and accurate a manner as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the organization will change. As a result of these two factors, this plan will need to be tested on a periodic basis to discover errors and omissions and will need to be maintained to address them.

8.1 Maintenance

The DRP will be updated quarterly and any time a major system update or upgrade is performed. The Disaster Recovery Lead will be responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the organization in order to complete this task.

Maintenance of the plan will include (but is not limited to) the following

1. Ensuring that call trees are up to date;
2. Ensuring that all team lists are up to date;
3. Reviewing the plan to ensure that all of the instructions are still relevant to the organization;
4. Making any major changes and revisions in the plan to reflect organizational shifts, changes and goals;
5. Ensuring that the plan meets requirements specified in new laws; and
6. Other organizational specific maintenance goals.

During the Maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any member of a Disaster Recovery Team no longer works with the company, it is the responsibility of the Disaster Recovery Lead to appoint a new team member.

8.2 Testing

LSST is committed to ensuring that this DRP is functional. The DRP will be tested every year in order to ensure that it is still effective. Testing the plan will be carried out as follows.

1) **Walkthroughs**- Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the DRP project manager to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities.

2) **Simulations**- A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. However, validated checklists can provide a reasonable level of assurance for many of these scenarios. An analysis of the output of the previous tests is carefully done before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.

3) **Parallel Testing**- A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as the prior business day's transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the primary site for the current business date should agree with those reports produced at the contingency processing site.

Any gaps in the DRP that are discovered during the testing phase will be addressed by the Disaster Recovery Lead.

8.3 Call Tree Testing

Call Trees are a major part of the DRP and testing is required yearly in order to ensure that it is functional. Tests will be performed as follows.

1) Disaster Recovery Lead initiates call tree and gives a code word to the first round of employees called.
2) The code word is passed from one caller to the next.
3) The next work day all Disaster Recovery Team members are asked for the code word.
4) Any issues with the call tree, contact information, etc. will then be addressed accordingly.

Appendix A: Emergency Contact List

Location		Name	Home Phone	Cell Phone	Spouse's Cell	Other
Tucson	Emily	Acosta		520-907-6253		
	Robyn	Allsman	520-297-6514	520-248-5221	520-256-5609	
	John	Andrew	520-298-0636	520-907-7806		
	George	Angeli		520-975-9732		
	Tim	Axelrod		520-780-2054		
	Jeff	Barr		520-307-4423		
	Melissa	Bowersock	520-297-7454	520-275-8723		
	Daniel	Calabrese		520-471-0598		
	Srini	Chandrasekharan	520-495-0453	520-360-6778	520-425-4110	
	Chuck	Claver	520-690-5857	520-603-4884		
	Joe	DeVries		520-349-2662		
	Iain	Goodenow		520-401-0362		
	Chuck	Gessner				520-318-8211
	Bill	Gressler	520-742-8938	520-225-9471	520-440-6257	315-823-3106
	Ed	Hileman		520-577-6115	520-237-7809	520-514-9681
	Suzanne	Jacoby	520-794-1624	520-490-6683	520-904-4135	
	Mario	Juric		617-744-9003		385-98-9018301
	Steve	Kahn		650-283-9109		
	Jeff	Kantor		520-979-9941	520-981-2019	520-979-9949
	Victor	Krabbendam	520-229-8863	520-420-1980		
	Ming	Liang	520-790-6885	n/a		

	Rob	McKercher	520-886-4028	520-870-7612	520-390-3578	
	Dave	Mills	520-822-5221	520-954-4818		520-954-8366
	Doug	Neill		520-256-0170		
	Mark	Newhouse	520-885-2393	520-360-8724		
	Sandra	Ortiz		520-977-5741		
	Steve	Ridgway	520-577-2118	520-248-4408		
	Abi	Saha	520-742-5305	520-834-5237		
	Bill	Schoening				
	Jacques	Sebag	520-299-1373	520-780-0910		
	Brian	Selvy	520-219-2452	818-634-0771	818-519-6544	
	Oliver	Wiecha		520-343-5744		
	Sidney	Wolff	520-577-2291	520-990-7068		
AURA	Bill	Smith				202-483-2101
	Dionne	Makila				202-483-2101
Chile	Francisco	Delgado		56-51-94451647		
	Enrique	Figueroa		56-9-8270660		56-51-205-225
	Ron					56-51-205-238
	German	Schumacher	56-51-292-099	56-9-94411100		
	Mike	Warner	56-51-210-341	56-98-468-7837		520-247-1167
Harvard	Chris	Stubbs		978-460-1672		617-495-2866
IPAC	Schuyler	Van Dyk		626-200-1802		626-395-1881
NCSA	Mike	Freemon				217-244-7503
Princeton	Robert	Lupton		609-233-2011		609-258-3811
	Michael	Strauss				609-258-3808
SLAC	Jacek	Becla				650-926-8664
	Gregory	Dubois-Felsmann				650-926-4207
	Nadine	Kurita		408-833-9050		650-926-2340
	Kian-Tat	Lim				650-926-2902
	David	MacFarlane				650-926-3406
	Regina	Matter				650-926-3783
UC Davis	Tony	Tyson		530-400-0406		530-752-3830
UCSC	Steve	Ritz		831-332-7764		831-459-3018
Univ. of Washington	Andy	Connolly		412-983-5329		206-543-9541
	Zeljko	Ivezic	206-361-6381	206-403-6132		206-543-9375
	Lynne	Jones		206-795-4755		206-543-9487