[Based on NIST 800-34-rev_bia_Template]
Color Code: Gray text is the instructions for completing the document

[This document is a template for Disaster Recovery Planning. The results of this document will be used in the areas to work following a disaster, and feed into the steps in CiCOE Disaster Recovery Policy Template.]

IceCube Cyberinfrastructure

Security Categorization: Low

IceCube Neutrino Observatory

Information System Contingency Plan (ISCP)

Version 2

DRAFT

Disclaimer: This IceCube Information System Contingency Plan (ISCP) draft has not been finalized. This is a conceptual prototype ISCP and will undergo changes as systems are operationalized.

23-July-2019

Prepared by

Cyberinfrastructure Center of Excellence Pilot (CiCOE Pilot)
and IceCube teams
CONTACT INFORMATION

TABLE OF CONTENTS

Plan Approval

[Provide a statement in accordance with the project's contingency planning policy to affirm that the Business Impact Analysis is complete and has been tested sufficiently. The statement should also affirm that the designated authority is responsible for continued maintenance and testing of the ISCP. This statement should be approved and signed by the system designated authority. Space should be provided for the designated authority to sign, along with any other applicable approving signatures. Sample language is provided below.]

As the designated authority for *IceCube Cyberinfrastructure (CI)*, I hereby certify that the *Business Impact Analysis (BIA)* is complete, and that the information contained in this BIA provides an accurate representation of the application, its hardware, software, and telecommunication components. I further certify that this document identifies the criticality of the system as it relates to the mission of the National Science Foundation, and that the recovery strategies identified will provide the ability to recover the system functionality in the most expedient and cost-beneficial method in keeping with its level of criticality.

I further attest that this BIA for IceCube CI will be tested at least annually. This plan was last tested on ***{insert exercise date}***; the test, training, and exercise (TT&E) material associated with this test can be found ***{TT&E results appendix or location}***. This document will be modified as changes occur and will remain under version control, in accordance with *IceCube and NSF*'s contingency planning policy.

____ __________________________

{System Owner Name} Date
{System Owner Title}

1 - Overview

Information Systems are vital to the missions of NSF and IceCube. Therefore, it is critical that the cyberinfrastructure (CI) is able to operate effectively and without excessive interruption. This Business Impact Analysis (BIA) is developed as part of the contingency planning process for the IceCube Cyberinfrastructure (CI). It was prepared on **23-July-2019**.

The IceCube CI provides the computational framework for the information produced by the IceCube Neutrino Observatory, and as such it serves the entire Data Life Cycle from initial collection to final archiving and dissemination. Transport and distribution of information from the experimental site is challenging (satellite bandwidth to the South Pole is limited, and most of the data is saved on disk drives and flown out once a year). Some computation is done *in situ* at the pole to rapidly screen for interesting events supporting astronomy and astrophysics. Much more of the computation, and all of the public dissemination and long-term archiving, is done at other sites on three more continents.

[A short summary of this disaster recovery planning document goes here. Level of detail should be sharply limited. The intent is to provide an idea of the overall motivating forces and decision making thought process that have gone into it.]

The general structure of the disaster recovery plan follows from the identification of potential failures at each step in the Data Life Cycle. This analysis method results in a plan for contingency operations in response to each of the failures. In many cases, there are multiple possible ways forward. A "preferred" solution is presented first, followed by other options. Substantial outages can often create fluid situations, and having several options already surveyed may be of considerable use.

1.1 - Purpose of this Document

The purpose of this BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports, and using this information to characterize the impact on the process(es) if the systems were unavailable.

The BIA is composed of these four sections:

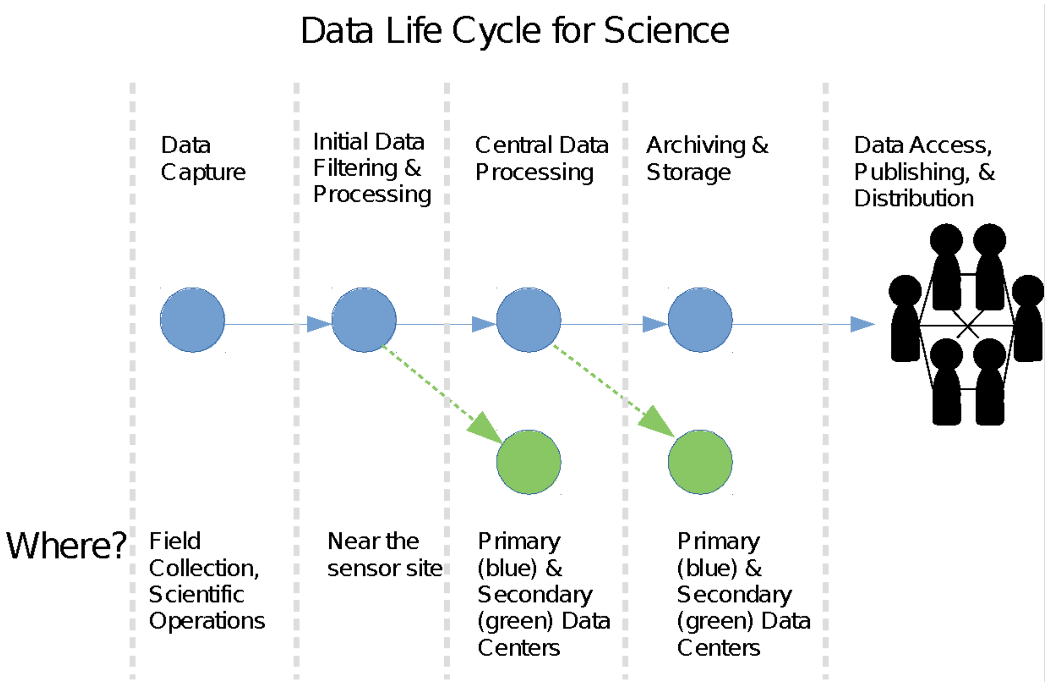
1. **Overview.** This section provides a top-level view of the cyberinfrastructure recovery needs of the organization and serves as summary and context for the remainder of the document.
2. **Mission, data life cycle, and recovery criticality.** Cyberinfrastructure to support the entire data life cycle of IceCube is identified and the impact of a system disruption to those systems is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum that an organization can tolerate while still maintaining the mission.
3. **Resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to restore the systems and processes supporting the data life cycle and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.
4. **Recovery priorities for system resources.** Based on the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and

resources.

[Completion of the Disaster Planning Document will be greatly facilitated by having adequate requirements and design documents available.]

1.2 – Planning Philosophy and Context

This BIA is structured to reflect the Data Life Cycle (DLC). DLC is a model for representing the flow of information and actionable knowledge through a sequence of processes. The progression of steps is not necessarily linear. The following illustration shows an example of the information flow for a (hypothetical) scientific facility. This diagram should be considered conceptual rather than schematic – any real-world installation has loops, skipped steps, and special cases with *ad hoc* processes.


Data Life Cycle for Science
Data Capture
Initial Data Filtering & Processing
Central Data Processing
Archiving & Storage
Data Access, Publishing, & Distribution
Where?
Field Collection, Scientific Operations
Near the sensor site
Primary (blue) & Secondary (green) Data Centers
Primary (blue) & Secondary (green) Data Centers

This framework provides guidance for designing the Disaster Recovery Plan. Each step in the Data Life Cycle corresponds to a major deliverable process in a scientific facility. Analyzing each of these processes and determining the criticality, resource requirements, and recovery priority of each step is the key to understanding where redundancy and/or contingency processes are needed.

Later sections in this document will look at the cyberinfrastructure assigned to each of the lifecycle stages and consider downstream impacts of possible failures. At each stage, there are several challenges to consider, especially for steps that have to be run close to the sensor array itself (which means those steps have to happen at the pole).

2 - Mission, Business Processes, and Recovery Criticality

[This section describes what the Large Facility does, the processes (CI) that it uses to perform those actions, and how important it is to be able to recover each of those processes. For instance, if a LF has been identified as a FIPS 199 “Moderate” CI project, preservation and recovery processes should be appropriate to that. This section will have many sublevels added in analysis, treating the Facility as a complex system of missions, goals, processes, and results.]

The mission of the IceCube Neutrino Observatory is to detect neutrinos, alert other observatories around the world when scientifically interesting events occur, postprocess the raw data, and archive the data from the observatory. These functions are necessary to advance physics, astronomy, and earth sciences. Possible failures and/or events leading to failures are discussed in this section, below. The following table lists the primary mission and functions of this facility and its CI.

Mission/Business Process	Description
Collect observational data for scientific inquiry	Operate an array of photodetectors buried in a cubic kilometer of ice at the south pole.
Ingest data from sensors for further use	Operate networks at the south pole, satellite and physical data transport to UW-Madison, and bulk internet transfer to DESY-ZN and to NERSC (National Energy Research Scientific Computing Center). Notification of neutrino events to worldwide observatories, both radio and optical.
Process data for QA, events, and production of private and public datasets	Operate clusters of computers to analyze data for interesting events, QA, and calibration. Data reduction for low bandwidth satellite link.
Archive data for future use	Operate a curated repository of collected and processed data redundantly copied across three institutions.
Disseminate data	Provide **alerts** for interesting astrophysical events, i.e. during L1 analysis, if an event of interest is detected, an alert is sent out immediately. Operate an access portal to support querying the collection and accessing the stored and/or computed results. Provide well documented access methods and ensure that access methods can be added into the far future as needed.

[Create sub-sections for each of the above points. Depending on the level of thoroughness, this can get involved]

2.1 Major System Components

This section highlights the major components that make up the IceCube Cyberinfrastructure. This disaster recovery plan views the total cyberinfrastructure in terms of large subsystems.

2.1.1 Collect observational data for scientific inquiry

Mission/Business Process	Description
IceCube DOM (Digital Optical Module) array	5160 DOMs under the ice, optical sensors on cables embedded into the ice
IceTop	300+ sensors at the surface of the ice

2.1.2 Ingest data from sensors for further use

Mission/Business Process	Description
Local sensor network	Power and communications from IceCube laboratory to the sensors down in the ice
IceCube Laboratory	~100 servers for detector readout. Unreliable power. Special cooling challenges
Local network to South Pole Station	Short-haul fiber network across the runway area connecting IceCube Laboratory to Amundsen-Scott Station
Data transmission to Northern Hemisphere	Satellite: 125 GB/day. JADE transmits the data via satellite. 3 TB/day of raw data saved on disk drives and flown out of the pole once a year

2.1.3 Process data for QA, events, and production of private and public datasets

Mission/Business Process	Description
Event detection and first-pass QA	In IceCube Laboratory at the pole – circa 500 cores
Processing for Public and Private data sets	Coordinated at UW-Madison. Distributed computing using HTCondor to many member institutions. Other CPU/GPU resources scavenged from XSEDE, DOE, OSG etc.

2.1.4 Archive data for future use

Mission/Business Process	Description
Long-term storage	Three copies – original at UW-Madison, also at DESY and at NERSC (National Energy Research Scientific Computing Center)
Data Management	Homegrown “JADE” for archive management

2.1.5 Disseminate data

Mission/Business Process	Description
Data product production	Private, full-featured data for members, reduced Level 2 data for Public
Event detection and Alerts	Alerts happen at the South Pole during Level 1 processing - alerting systems detect events and then an immediate alert is sent out using GCN (Gamma Ray Coordination Network - operated by NASA) or the Astronomical Telegrams along with initial estimate/small portion of PFRAW data sample via satellite link to UW; When a full PFFILT data set is available at UW later, a refinement of the first alert is sent. The purpose is to computes where neutrinos came from – if from space, notifies in seconds a global association of observatories (radio, optical, gravity waves) to study what is happening (supernovae, etc.).

2.2 - Outage Impacts and Estimated Downtime

[This section identifies and characterizes the types of impact categories that a system disruption is likely to create in addition to those identified by the FIPS 199 impact level, as well as the estimated downtime that the organization can tolerate for a given process. Impact categories should be created and values assigned to these categories in order to measure the level or type of impact a disruption may cause. An example of cost as an impact category is provided. Organizations could consider other categories like harm to individuals and ability to perform mission. The template should be revised to reflect what is appropriate for the organization.

Different kinds of disasters can cause greatly variable impacts. Highly resilient systems might stand up to major disasters without ill effects, but usually at substantial cost. Conversely, some inexpensive systems are, in fact, quite brittle. When designing CI, it is always necessary to think about the expected loss and the expected cost to recover. Expected loss is a function of the probability of a disaster multiplied by the cost of downtime. Designers must balance the expected cost to recover against the expected loss, bearing in mind that assigning dollar amounts to downtime is an imprecise action at the very best.]

2.2.1 – Outage Impacts

[Impact categories and values should be created in order to characterize levels of severity to the organization that would result for that particular impact category if the mission/business process could not be performed. These impact categories and values are samples and should be revised

to reflect what is appropriate for the organization.]

A significant part of disaster recovery planning is understanding the relative impact of various forms out outages. Not all outages hurt the overall mission of the project by the same amount – some are trivial and some are devastating. This section looks at the major elements of the Data Life Cycle, considers three categories of impacts, and assigns a severity level to each one.

Impact categories:

- **Mission Impact** = How severe is the risk to the overall mission of the facility? This includes scientific operations, safety and operation of the instrument, relationships with scientists, preservation of data, confidence in the accuracy and usefulness of results, and educational impacts.

- **Science Return** = How much value is being created for the specific purpose of science? Aspects of this include accuracy, timeliness, availability, and trustworthiness.

- **Cost** = What is the financial impact? Small amounts of downtime, or relatively minor damage to facilities, will typically be much less expensive to recover from than it would be for a more substantial event – the costs often rise dramatically out of proportion to the objective severity of the event.

- **Impact** = Finally, the overall impact for failure of a given Data Life Cycle stage is given – this is the maximum value for all of the impacts in that stage.

Impact values for assessing category impact:

- **Severe** = Major impact leading to catastrophe, permanent loss of data, loss of public and/or scientific confidence in data, or substantial recovery cost reflected in the overall NSF budget.
- **Moderate** = Substantial inconvenience or actual inability for the pulic or the scientific community to use data and CI facilities for a non-trivial period. Temporary loss of data, delays in accessing data resulting in scientific impacts (with workarounds).
- **Minimal** = Tolerable inconvenience for public and/or scientific users, no loss of data collection, and simple, low-cost recovery options.

The table below summarizes, in terms of the Data Life Cycle, the impact on each business process if IceCube's CI becomes unavailable, based on the following criteria:

Data Life Cycle Stage	Impact Category			
	Mission Impact	Science Return	Cost	Impact
Collect observational data for scientific inquiry	Severe	Severe	Severe	Severe
Ingest data from sensors for further use	Severe	Moderate	Moderate	Severe
Process Data for Multimessenger GCN Alerts	Severe	Severe	Moderate	Severe
Process data for QA, and production of private and public datasets	Moderate	Moderate	Minimal	Moderate
Archive data for future use	Severe	Severe	Severe	Severe
Disseminate data - Alerts	Severe	Severe	Minimal (short term)	Severe
Disseminate data – Level 2+ processed products	Moderate	Minimal	Minimal	Moderate

From the table above, we see rough divisions of how much total impact is expected if major scientific processes of IceCube are unable to continue. Not all impacts are equal, and even inside particular levels there are gradations. For example, ingesting data from a “total facility” standpoint carries a “severe” rating, but it’s important to note that the process has several steps. The ingestion from the DOMs to the IceCube Laboratory at the pole is extremely important and needs to be done without interruption. On the other hand, delay in shipping disk drives from the pole to UW-Madison has a minimal impact, at least until the delay becomes intolerably long. It should also be noted that some of these impact estimates may vary based on a particular analysis chain and how important that particular analysis is for the observatory and other entities depending on the results of the analysis.

2.2.2 - Estimated Downtime

The priorities of the major stages in the Data Life Cycle determine, in the wake of a disaster, how much downtime can be tolerated (both typically and *in extremis*) and how much of a gap in data collection and processing can be tolerated. These parameters are:

1) **Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing

recovery procedures, including their scope and content.

2) **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

3) **Recovery Point Objective (RPO**). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

The table below identifies the MTD, RTO, and RPO (as applicable) for the Data Life Cycle stages for IceCube's CI.

[Values for MTDs and RPOs are expected to be specific time frames.]

Data Lifecycle Stage	**MTD**	**RTO**	**RPO**
Collect sensor data for scientific inquiry – operation of the actual sensors	1 hour	1 hour	N/A
Ingest data from sensors for further use	Optical DOMs to IC Lab: 2 days; IC Lab to South Pole Lab: 6 months	1 day from DOM; 1 month from lab to station	1 day
Process data for QA, events, and production of private and public datasets	Events: 1 hour; All others: 1 month	Events: 30 minutes; Others: 4 days	Equal to recovery time
Archive sensor data for future use	6 months w/ no loss	1 hour	1 day
Disseminate data - alerts	6 hours	3 hours	None
Dissemination – Level 2+	1 year	1 month	1 day

Collecting observational data is the most important process performed by IceCube; data collection is the purpose of the instrument and the entire program. Actual physical operation of the sensors is needed to keep them from freezing and becoming permanently inoperative. Collecting the data is very expensive because of the scale of the array and the phenomenally challenging environment in which it is used. Downtime incurs the discounted Net Present Value of most of the project.

Ingesting data from sensors is a companion process to collecting the data, and is composed of networking (both locally at the pole and globally for forwarding both alerts and data, processed, via satellite, and raw via shipping disk drives by air). Failures of the local network, especially between the DOMs and the IceCube Laboratory, are critical in that they reduce or destroy the scientific value of the data collected. There is a six and a half day buffer built in to the DOMs, supporting a Recovery Point Objective of Zero Seconds provided the data flow back up the well within that period. It is important, also, to be able to notify observatories around the world when neutrino "events" are detected, indicating interesting astrophysical processes. This ingest relies on flows from the DOMs into the IC Laboratory (and resulting alerts flow out via the Iridium Satellite Network).

Processing data for QA, events, and production of completed products has two aspects. Again, event detection and reporting is very important. NSF's Astronomy efforts depend on rapid coordination between observatories, of different types, to simultaneously study astrophysical phenomena with many different kinds of instruments. The event processing and alert production processing is therefore very time sensitive. IceCube's other processing, the production of private and public datasets and derived products, lacks the time sensitive nature of event detection. This is not to say that the processing is unimportant, just that delays are much more tolerable. The tremendous majority of data is sent from the pole once a year in a physical shipment – the resulting processing is very bursty.

Archiving data is an essential function of any large facility, and IceCube is no exception. The data produced by the observatory is difficult and expensive to collect. Just like observational data from radio and optical telescopes, researchers will want to analyze the collected information for a long time to come. Archiving is not simply saving data, but rather a process that involves determining what to keep, preserving the information, and ensuring there are methods in place to locate right information again. While the safety and reliability of the archive is paramount, the requirement for availability is significantly more tolerant. As long as data has not been lost irretrievably, researcher access to the collection can be down for substantial periods of time. Further simplifying the requirements, the overwhelming majority of the data from the observatory is shipped out from the pole once a year.

Disseminating data is often thought of as part of archiving, but in reality, is a separate function of its own. Dissemination also has two distinct components in terms of this facility: the production of alerts and the provision of level 2 and higher (more abstract) data. IceCube is critically affected by this duality because of the need to alert a worldwide network of observatories, quite quickly, after detection of a scientifically interesting event. Detecting a "flash" of neutrinos is the kind of event that needs to be communicated to the Gamma Ray Coordinating Network (GCN) of observatories worldwide. These observatories include LIGO (for detecting gravity waves) and also optical and radio telescopes. Multi-messenger astronomy is about observing interesting events with a wide range of sensing modalities. The alerts, carried via the Iridium satellite constellation, must arrive at the other observatory sites before it's too late for them to obtain useful data.

3. Resource Requirements

[Describe what kinds of resources are required to execute the mission and each stage of the Data Lifecycle, above.

Provide a general description of system architecture and functionality. Indicate the operating environment, physical location, general location of users, and partnerships with external organizations/systems. Include information regarding any other technical considerations that are important for recovery purposes, such as backup procedures. Provide a diagram of the architecture, including inputs and outputs and telecommunications connections.

Note: Information for this section should be available from the system's System Security Plan (SSP) and can be copied from the SSP, or reference the applicable section in the SSP and attach the latest version of the SSP to this contingency plan].

The following table identifies the resources that compose IceCube's Cyberinfrastructure including hardware, software, and other resources such as data files.

System Resource/Component	**Platform/OS/Version (as applicable)**	Description
Collect observational data for scientific inquiry	DOMs (custom)	Sensors buried in the ice. Also power, IceCube Laboratory Facilities, staff
Ingest data from sensors for further use	Data communication to DOMs, network to South Pole Station, rest of world	Communications from DOMs, network to South Pole station, satellite and sneakernet to rest of world. JADE software for archive and distribution worldwide.
Process data for QA and for computed results	Server clusters, other CPU/GPU resources, HTCondor compute middleware, data distribution software	Datacenters at IceCube Lab and South Pole Station with special challenges. Data centers at UW-Madison, DESY, and NERSC. Distributed computing on OSG, XSEDE, DOE resources.
Archive sensor data for future use	JADE	Long term archive and archive management
Disseminate data	Web servers, data access/distribution middleware	Public-facing Portal, other data distribution methods (xrootd, ceph etc.)

3.1 Collection of observational data

Data collection is done with the DOMs themselves (for our purposes, ~5200 embedded computers with custom communications). Control and power are handled by systems inside the IceCube laboratory.

3.2 Ingest of sensor data

Sensor data ingest consists of several stages. At the pole, there is a data network from the DOMs to the servers in the IceCube Laboratory. The Lab has 100 servers for reading data from the DOM sensors and an additional cluster with an aggregate of about 500 cores for data processing/filtering. The data leaves the laboratory and goes about a mile to the South Pole Station via an optical fiber installation. From there, the data goes over two paths – summarized data is sent via satellite to the Antarctic Project center and full, raw data is saved on disk drives and transported once a year to the Northern Hemisphere via an airplane, a ship, and a train. The data arrives at the University of Wisconsin's facility in Madison, WI., and from there copies of that are sent on to DESY in Germany and to NERSC.

3.3 Process data for QA and for computed results

Processing of the observational data begins at the pole on the ~500 core installation in the Laboratory itself. This first pass applies calibration, does the first pass of directional reconstruction, and produces a summarized form. This is where time-sensitive detection of interesting events begins, i.e. the alerts. Further processing occurs at UW-Madison and at member institutions, and also occurs on OSG, XSEDE resources and DOE facilities. Computation is coordinated and scheduled using HTCondor + PyGlideIn middleware. Approximately 10,000 cores of aggregate power are available along with about 400 GPUs. Some of the processing code (photon propagation using ray tracing in the Monte Carlo production, and also direction and energy reconstruction) gets very useful speedups from having GPUs available.

3.4 Archive sensor data for future use

The IceCube archive stores raw data as well as computed products. The archive is located at UW, DESY and at NERSC. In addition to copies of data at UW, Level 1 data (PFFILT) and Level 2 data are archived at DESY and the raw data (PFRAW) is sent to NERSC. The NERSC site has further backups, as the data is written to tapes at that site.

3.5 Disseminate data

Data dissemination again occurs in two forms – rapid sharing of event detections/alerts and the more deliberately paced sharing of computed products via the portal. Alerts use GCN and satellite link. Computed products are available to member institutions once they're available and to the general public after they are used in publication. This availability schedule makes dissemination a relatively low-resource task. More data dissemination approaches are being considered, including use of xrootd, ceph etc.

4. Recovery Priorities

Based upon the results from the previous activities, system resources can more clearly be linked to the critical steps in the Data Life Cycle. Priority levels can be established for sequencing recovery activities and resources. Not all recovery items are equally important – it might, for instance, be acceptable for some life cycle stages to be down for significant periods (data dissemination, for instance), while other processes (perhaps data collection) must be continuously available.

4.1 Recovery Prioritization

[Discuss the drivers and reasoning behind the recovery priorities, and the actual priorities that result from that analysis.]

Data collection and ingest are the most critical processes in IceCube's CI. The collection of the data is very expensive and lost observing time is impossible to replace. Archiving is a close second in terms of priority: once data is collected (at great expense) it is valuable and stays valuable for a very long time – probably measured in decades. The processing and dissemination steps are less important. If processing fails, there is time to restart that in an orderly, efficient, and relatively low cost way. The case with dissemination is similar. The exception to those two, as mentioned previously, is event detection for astronomy.

4.2 Recovery Time Objectives

The table below lists the order of recovery priority for IceCube resources. The table also identifies the expected time for recovering the resource following a "worst case" (complete rebuild/repair or replacement) disruption. All of these assume that the physical plant of the facility is basically intact and that the failure is confined to the CI. Given the remoteness of the detector itself, physical repair would be very challenging and highly dependent on the seasons: work during arctic winter is, practically speaking, not possible.

*[**Recovery Time Objective (RTO)** - RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, Data Lifecycle stages, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.]*

Priority	System Resource/Component	Recovery Time Objective
1	Collect environmental data for scientific inquiry	1 hour
4	Ingest data from sensors for further use	Optical DOMs to IC Lab: 1 day; IC Lab to South Pole Lab: 2 months
5	Process data for QA and for intermediate results	Events: 30 minutes Others: 4 days

3	Archive sensor data for future use	1 hour
6	Disseminate data – Level 2+	1 month
2	Disseminate Alerts	3 hours

5. Contingency Strategies

Any organization must consider the wide range of possible ways to mitigate the effects of a disaster, considering events ranging from minor to catastrophic. Analysis of these options results in the largest portion of the completed disaster recovery plan – the plan being at its essence a report on the best available options for the systems affected.

The following sections consider, in broad terms, the problems of copying and saving the organization's information, locating and preparing to use replacement resources, and making the saved information available through the replacement means. Additionally, cost-benefit analysis of the options is outlined, as is a discussion of the likely availability of staff to execute the necessary steps.

5.1 Backup and Recovery

[Several alternative approaches should be considered when developing and comparing strategies, including cost, maximum downtimes, security, recovery priorities, and integration with larger, organization-level contingency plans. The following table is an example that can assist in identifying the linkage of FIPS 199 impact level for the availability security objective, recovery priority, backup, and recovery strategy.

FIPS 199 Availability Impact Level	***Information System Target Priority and Recovery***	***Backup / Recovery Strategy***
Low	*Low priority - any outage with little impact, damage, or disruption to the organization.*	*Backup: Tape backup* *Strategy: Relocate or Cold site*
Moderate	*Important or moderate priority – any system that, if disrupted, would cause a moderate problem to the organization and possibly other networks or systems.*	*Backup: Optical backup, WAN/VLAN replication* *Strategy: Cold or Warm site*
High	*Mission-critical or high priority – the damage or disruption to these systems would cause the most impact on the organization, mission, and other networks and systems.*	*Backup: Mirrored systems and disc replication* *Strategy: Hot site*

]

Backup and recovery methods and strategies are a means to restore system operations quickly and effectively following a service disruption. The methods and strategies should address disruption impacts and allowable downtimes identified in the BIA and should be integrated into the system architecture during the Development/Acquisition phase of the SDLC. Multiple backup and recovery options are considered in this section. The recommended approach for the project is to save multiple copies of the IceCube data at multiple sites.

5.2 Backup Methods and Offsite Storage

[It is good business practice to store backed-up data offsite. High speed networking has revolutionized both backups and high-availability storage systems, especially between an organization's multiple sites or between a group of cooperating entities. Conventional, commercial data storage facilities still thrive, though, and are specially designed to archive media and protect data from threatening elements. If using offsite storage, data is backed up at the organization's facility and then labeled, packed, and transported to the storage facility. If the data is required for recovery or testing purposes, the organization contacts the storage facility requesting specific data to be transported to the organization or to an alternate facility. Commercial storage facilities often offer media transportation and response and recovery services. When selecting an offsite storage facility and vendor, the following criteria should be considered:

- *Geographic area: distance from the organization and the probability of the storage site being affected by the same disaster as the organization's primary site;*
- *Accessibility: length of time necessary to retrieve the data from storage and the storage facility's operating hours;*
- *Security: security capabilities of the shipping method, storage facility, and personnel; all must meet the data's security requirements;*
- *Environment: structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls); and*
- *Cost: cost of shipping, operational fees, and disaster response/recovery services.*

]

System data should be backed up regularly. This section defines the minimum frequency and scope of backups (e.g., daily or weekly, incremental or full) based on data criticality and the frequency that new information is introduced. The location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite is discussed here. The specific methods chosen for conducting backups are based on system and data availability and integrity requirements.

The raw data from the IceCube array is buffered in the IceCube laboratory itself before being sent approximately a mile to the south pole station. This first line of defense will store a day's worth of data and give some time to recover in the event of a network failure across the ice. From the station, data is sent via satellite and by shipping disks once a year to UW-Madison. UW-Madison stores their data and houses their computation in an environment that spans more than one building on their campus, providing some redundancy. Additionally, copies of the data are sent to

DESY (in Germany) and to the Department of Energy's NERSC lab. Both the DESY and NERSC copies are further backed up to tape. In total, there are a minimum of five copies of the IceCube data (spanning Level 1 and Level 2) stored at three sites.

5.3 Alternate Sites

[Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. Thus, for all FIPS 199 moderate- or high-impact systems, the plan should include a strategy to recover and perform system operations at an alternate facility for an extended period. Organizations may consider FIPS 199 low-impact systems for alternate site processing, but that is an organizational decision and not required. In general, three types of alternate sites are available:

- *Dedicated site owned or operated by the organization;*
- *Reciprocal agreement or memorandum of agreement with an internal or external entity; and*
- *Commercially leased facility.*

Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three alternate site types commonly categorized in terms of their operational readiness are cold sites, warm sites, or hot sites. Other variations or combinations of these can be found, but generally all variations retain similar core features found in one of these three site types. Progressing from basic to advanced, the sites are described below.

- *Cold Sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.*
- *Warm Sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.*
- *Hot Sites are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.*

As discussed above, these three alternate site types are the most common. There are also variations, and hybrid mixtures of features from any one of the three. Each organization should evaluate its core requirements in order to establish the most effective solution. Two examples of variations to the site types are:

- *Mobile Sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements.*
- *Mirrored Sites are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.*

Site	***Cost***	***Hardware Equipment***	***Telecommunications***	***Setup Time***	***Location***

Cold Site	*Low*	*None*	*None*	*Long*	*Fixed*
Warm Site	*Medium*	*Partial*	*Partial/Full*	*Medium*	*Fixed*
Hot Site	*Medium/High*	*Full*	*Full*	*Short*	*Fixed*

Alternate sites may be owned and operated by the organization (internal recovery), or commercial sites may be available under contract. If contracting for the site with a commercial vendor, adequate testing time, work space, security requirements, hardware requirements, telecommunications requirements, support services, and recovery days (how long the organization can occupy the space during the recovery period) must be negotiated and clearly stated in the contract. Customers should be aware that multiple organizations may contract with a vendor for the same alternate site; as a result, the site may be unable to accommodate all of the customers if a disaster affects enough of those customers simultaneously. The vendor's policy on how this situation should be addressed and how priority status is determined should be negotiated.]

Events more serious than a minor emergency will frequently call for changing the location where operations occur. Heavy damage to the physical plant where data and computation resides will necessitate shifting the location where this occurs. At a modest scale this might involve switching to backup servers in a different building, and in times of calamity the entire information processing enterprise may need to be relocated thousands of miles away.

Selection of alternative sites is based on the FIPS impact level, acceptable downtime, and recovery point objectives of the systems. Some of these factors are mutually exclusive. For instance, an alternative site should be very far away to mitigate the risks of large scale storms. On the other hand, moving the site further away hurts the performance of many kinds of data replication strategies and also increases operating costs. An analysis of the tradeoffs is considered here, and ultimately results in selecting data and compute replication as the Alternate Site strategy.

IceCube's CI is distributed across several sites, offering redundancy and a high degree of resilience in the final stages of the data life cycle. Initial data gathering at the sensor is, of course, impossible to duplicate. The sensor array is too expensive to replicate and, in any case, there's only one south pole. The same can be said for the reliance on the existing south pole station. Once data has left the pole and arrived in the northern hemisphere is when the recovery options start to multiply.

The distribution of data between UW-Madison and DESY is, in effect, a hot-hot scenario for either of them to use in recovery operations. The relationship between UW-Madison and NERSC needs to be evaluated from a DR standpoint.

5.4 Equipment Replacement

[If the information system is damaged or destroyed or the primary site is unavailable, necessary hardware and software will need to be activated or procured quickly and (potentially) delivered to the alternate location. Three basic strategies exist in NIST 800-34 to prepare for equipment replacement:

1) Vendor agreements, whereby the supplier will make replacement hardware available quickly

2) warehoused equipment inventory (keeping spare hardware offsite until it is needed), and

3) compatible hardware from cooperating agencies or entities, where another NSF-funded Large Facility, for instance, might have unaffected hardware sufficiently similar to take over some or all of the load.

A fourth hardware option that must be considered is rental of cloud computing capacity. Vendors such as Microsoft, Amazon, Google or others can provision hardware within minutes and will rent that capacity by the minute. There are difficulties, to be sure, in moving data back and forth to a cloud provider, but if a cloud provider has already been selected to hold "cold" backups of essential data then using their facilities for contingency hardware might be a very attractive option.]

Replacement of failed equipment poses an interesting challenge at the south pole. Shipment is by air and is only an option for six months out of the year – the so-called Antarctic Summer isn't much of a summer (at -40 degrees) but winter is a lot worse. The strategy at the pole is to have enough spare equipment and parts on hand to keep the observatory running through various adverse events. Replacement of gear in Wisconsin or in Germany is a much simpler matter. Given the time-sensitive nature of the astrophysical alerts, sufficient spares should be kept on hand to swap out failed equipment if it cannot be quickly recovered. The slower-paced activities can be served by normal vendor relationships.

5.5 Cost Considerations

[The ISCP Coordinator should ensure that the strategy chosen can be implemented effectively with available personnel and financial resources. The cost of each type of alternate site, equipment replacement, and storage option under consideration should be weighed against budget limitations. The coordinator should determine known contingency planning expenses, such as alternate site contract fees, and those that are less obvious, such as the cost of implementing an agency-wide contingency awareness program and contractor support. The budget must be sufficient to encompass software, hardware, travel and shipping, testing, plan training programs, awareness programs, labor hours, other contracted services, and any other applicable resources (e.g., desks, telephones, fax machines, pens, and paper). The organization should perform a cost-benefit analysis to identify the optimum contingency strategy. The table below provides a template for evaluating cost considerations.]

Contingency Resources	Strategies	Vendor Costs	Hardware Costs	Software Costs	Travel/Shipping Costs	Labor/Contractor Costs	Testing Costs	Supply Costs
Alternate Site	Cold Site	Low	V.Low	V.Low	High	High	High	Low
	Warm Site	Med.	High	High	Med	High	High	Low
	Hot Site	High	V.High	High	Low	Med	V.High	Low
Offsite Storage	Commercial	Low	N/A	N/A	N/A	Med.	Med.	N/A

	Internal	High	High	Low	N/A	Low	Med.	Med.
Equipment Replacement	SLA				V.Low	Med	N/A	N/A
	Storage				V.Low	Med	N/A	N/A
	Existing Use				V.Low	Med	Low	N/A

Disaster Management plans are only useful to the extent that they are practical. It is important to identify the costs associated with the various recovery options and weigh those against each other. There are quite commonly cases where some cyberinfrastructure processes must be recovered quickly, even at substantial cost while other functions can be restored slowly but in an inexpensive manner without terrible consequences. Making an informed decision about these tradeoffs, before a disaster strikes, is essential.

IceCube's data resiliency stems from having multiple copies of the information replicated at three sites. In light of that, the cost of recovery is strongly influenced by site capacity. If, for instance, DESY is able to handle the (external) load that UW-Madison normally does, then they can serve as a hot recovery site until Madison comes back online. Processing capacity, however, would be noticeably impacted. Use of workload management makes it easier to use other resources, in extremis, for recovery. In principle, the recovery workload could be sent to any computing resources that have adequate network connectivity. Cloud computing vendors would, perhaps, be a reasonable strategy under this scenario. Cloud vendors offer relatively low-cost computing and typically charge rather steep prices for outgoing network bandwidth. The IceCube scenario, in which a lot of data would be transferred into a cloud and computed on before a small summary of the data is emitted, is a good candidate for this kind of recovery option.

5.6 Roles and Responsibilities

[Having selected and implemented the backup and system recovery strategies, the ISCP Coordinator must designate appropriate teams to implement the strategy. Each team should be trained and ready to respond in the event of a disruptive situation requiring plan activation. Recovery personnel should be assigned to one of several specific teams that will respond to the event, recover capabilities, and return the system to normal operations. To do so, recovery team members need to clearly understand the team's recovery effort goal, individual procedures the team will execute, and how interdependencies between recovery teams may affect overall strategies.

The types of teams required are based on the information system affected and could be tailored according to FIPS 199 impact levels to reflect specific differences in requirements and backup procedures. The size of each team, team titles, and hierarchy designs depend on the organization. In addition to a single authoritative role for overall decision-making responsibility, including plan activation, a capable strategy will require some or all of the following groups:

- *Management team (including the ISCP Coordinator)*
- *Outage assessment team*
- *Operating system administration team*

- *Server recovery team (e.g., client server, Web server)*
- *Local Area Network/Wide Area Network (LAN/WAN) recovery team*
- *Database recovery team*
- *Network operations recovery team*
- *Application recovery team(s)*
- *Telecommunications team*
- *Test team*
- *Transportation and relocation team*
- *Media relations team*
- *Legal affairs team*
- *Physical/personnel security team*
- *Procurement team (equipment and supplies)*

Personnel should be chosen to staff these teams based on their skills and knowledge. Ideally, teams are staffed with personnel responsible for the same or similar functions under normal conditions. For example, server recovery team members should include the server administrators. Team members must understand not only the contingency plan purpose, but also the procedures necessary for executing the recovery strategy. Teams should be sufficient in size to remain viable if some members are unavailable to respond or alternate team members may be designated. Similarly, team members should be familiar with the goals and procedures of other teams to facilitate cross-team coordination. The ISCP Coordinator should also consider that a disruption could render some personnel unavailable to respond. In this situation, executing the plan may be possible only by using personnel from another geographic area of the organization or by hiring contractors or vendors. Such personnel may be coordinated and trained as an alternate team.

Each team is led by a team leader who directs overall team operations, acts as the team's representative to management, and liaises with other team leaders. The team leader disseminates information to team members and approves any decisions that must be made within the team. Team leaders should have a designated alternate to act as the leader if the primary leader is unavailable.

For most systems, a management team is necessary for providing overall guidance following a major system disruption or emergency. The team is responsible for activating the contingency plan and supervising the execution of contingency operations. The management team also facilitates communications among other teams and supervises information system contingency plan tests and exercises. Some or all of the management team may lead specialized recovery teams. A senior management official, such as the CIO, has the ultimate authority to activate the plan and to make decisions regarding spending levels, acceptable risk, and interagency coordination. The senior management official typically leads the management team.]

IceCube's CI can very naturally be compartmentalized into operations that have to be done at the pole and operations that are done anywhere else in the world. Staffing for recovery operations at the pole is limited to the staff on hand at the pole. Typically, there are two people at the IceCube Laboratory. Additional staff at the south pole station might be available to help, though there's a high likelihood that a disaster at the laboratory would be shared by the station, so additional people may be hard to come by.

Operations in North America and in Europe, on the other hand, are well understood and very simple by comparison. Both UW-Madison and DESY operate their CI from computing centers already accustomed to providing production support for scientific users. Much if not all recovery activity will be needed for both IceCube's CI and the other scientific workflows at the centers. Similar assumptions hold for other computing locations for IceCube. No additional recovery staff needs are anticipated.

5.7 Plan Testing, Training, and Exercises (TT&E)

[An ISCP should be maintained in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities within the plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in the environment specified in the ISCP. In addition, as indicated in Step 4 (Assess Security Controls) of the RMF, the effectiveness of the information system controls should be assessed by using the procedures documented in NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems. NIST SP 800-84, Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities, provides guidelines on designing, developing, conducting, and evaluating test, training, and exercise (TT&E) events so that organizations can improve their ability to prepare for, respond to, manage, and recover from adverse events. While the majority of TT&E activities occur during the Operations/Maintenance phase, initial TT&E events should be conducted during the Implementation/Assessment phase of the SDLC to validate ISCP recovery procedures.

Organizations should conduct TT&E events periodically, following organizational or system changes, or the issuance of new TT&E guidance, or as otherwise needed. Execution of TT&E events assists organizations in determining the plan's effectiveness, and that all personnel know what their roles are in the conduct of each information system plan. TT&E event schedules are often dictated in part by organizational requirements. For example, NIST SP 800-53 includes a control (CP-4) for federal organizations to conduct exercises or tests for their systems' contingency plans around an organization-defined frequency. Section 3.5.4 provides guidance on the type of TT&E identified for each FIPS 199 impact level.

For each TT&E activity conducted, results are documented in an after-action report, and Lessons Learned corrective actions are captured for updating information in the ISCP. NIST SP 800-84 provides detailed information on how to plan and conduct TT&E activities for information systems.]

IceCube CI's Disaster Recovery plan should be tested periodically – once upon completion, then annually thereafter. It isn't necessary or desirable to cause an actual outage to do a test. Testing that the ability for data ingestion to fail over to an alternative site is a key area (ensure that the JADE software infrastructure can do this). Also, ensure that the distributed computing and data distribution configuration allow many sites to host the configuration and the job queues.