Contract No. 75N93019C00001

Immune Epitope Database and Analysis Resource Program

# Operational and Disaster Recovery Plan

Generated January 2019

La Jolla Institute for Immunology
9420 Athena Circle
La Jolla, CA 92037

Submitted
January 14, 2019

Program/Site Contacts

Sheridan Martini Project Manager
858-752-6647
smartini@lji.org

Michael Scarpelli IT Senior Director
858-752-6534
mscarpel@lji.org

## Purpose

This Operational and Disaster Recovery Plan (ORP/DRP) is intended to describe how the La Jolla Institute for Immunology (LJI) will ensure the protection and integrity of the Immune Epitope Database (IEDB) application.

This document defines the systems and methods LJI has put into place to protect against potential failures that could affect the uptime and availability of the IEDB, including power outages, internet circuit outages, and hardware or software failures.

## Scope

The scope of the controls and practices described apply to all systems (hardware and software) related to the functioning of the IEDB.

## Roles and Responsibilities

Senior Director, Information Technology - responsible for the overall management, planning, procurement, and implementation of IT technologies and processes.

Senior Systems Administrator - responsible for the technical implementation and monitoring of IT systems.

External servers monitor all independent IEDB resources to verify that they are reachable. The external service attempts to load IEDB webpages and verifies that all content is accessible. Contact from the monitoring servers will occur every 120 seconds, 24 hours a day, 365 days a year.

The majority of operational outages can be mitigated by redundancies in place at LJI. Failure of our primary internet circuit will result in immediate failover to a secondary circuit, provided by a separate ISP. Power failures are mitigated by uninterruptible power supplies and LJI's diesel power generator. IEDB servers are hosted in a VMWare environment on a 5-node cluster, ensuring that server hardware failure is highly unlikely to affect the IEDB's service, and computing resources are allocated dynamically to ensure that the IEDB always has the resources necessary to perform optimally.

In the event of a failure that renders an IEDB-critical resource unreachable, however, the monitoring service will automatically alert the Sysadmin and Senior Director of the connection failure (the system is capable of e-mail and SMS notifications) and initiate DNS failover to the IEDB's replication site located at the San Diego Supercomputer Center (SDCC) on the University of California, San Diego (UCSD) campus. This failover is immediate.

The replication site represents an exact mirror of production IEDB servers at the time of failure. Non-production servers will be current from the night before the failure. This distinction is to ensure that replication of production systems are able to take advantage of the maximum bandwidth to reduce replication latency.

Once failover to the replication site has been verified as functional, the sysadmin will troubleshoot the server/application at the primary site.

Once the issue has been repaired, the failover will be reverted and service restored to the primary site. This step is performed manually, to ensure the primary site is ready to once again be the main target for visitors. The issue will be documented and reported to relevant IEDB Personnel.

For issues that cannot be detected in an automated fashion or do not represent critical failures, IEDB Personnel will monitor for service performance. If a problem is detected, the responsible party for that server/application is notified. If the IEDB Personnel responsible is unable to resolve the issue quickly, the sysadmin will be notified, and the steps outlined above will be followed to bring the issue to resolution.

For problems where the replication site failover cannot be employed, missing or damaged application data will be restored first from on-site near-line virtual machine backups. In an absolute worst-case scenario where both primary and secondary sites are offline, IEDB hardware will be physically relocated to a data center that can provide the necessary services to bring the IEDB back online.