Date: August 22, 2013  
To: Payroll Managers  
Human Resources Officers  
From: Evelyn Nazario  
Associate Vice Chancellor  
Human Resources Management & CO HR Services  
Subject: Disaster Recovery Testing

The purpose of this technical letter is to announce HR requirements to support Disaster Recovery Testing initiated by the SCO for agencies and campuses paid through the uniform state payroll system. HR Data Operations within systemwide Human Resources Management (HRM) has worked in collaboration with the SCO, to implement testing procedures which will allow campuses to maintain connection with the SCO in the event of a disaster that could potentially disrupt campus payroll-related operations.

General Overview
To preclude a potential disruption of business operations in the event of a disaster or disruption, and to minimize connection interruption between campuses and the SCO, systemwide HR is implementing systemwide mandatory Disaster Recovery Testing. These tests are necessary and will occur on an ongoing basis to ensure that in emergency situations, campuses will be able to maintain connections to the SCO.

Since the SCO serves as the California State University’s (CSU) pay agent, connections with the SCO are vital. The SCO is also the source the CSU utilizes for other payroll-related applications, which include data reporting, employee pay history information, and employee data retrieval. These business operations are critical to the CSU because without connection to the SCO, the CSU would be unable to complete employment history or data transactions in the uniform state payroll system, and most importantly, the SCO

Distribution:
CSU Presidents  
Vice Chancellor, Human Resources  
All Campus Vice Presidents
would be unable to issue payroll warrants to CSU employees. As a result, it is mandatory that all campuses participate in these testing procedures. HR Data Operations will be responsible for facilitating and overseeing these activities for CSU.

**Disaster Recovery Testing**

Disaster Recovery Testing consists of two phases:

**Phase One: Connectivity Testing**, requires campuses to log on to the Disaster Recovery System to confirm that they are able to successfully connect.

**Phase Two: Applications Testing**, whereby campuses follow provided scripts to run at their campuses.

**Phase One is scheduled for October 1-4, 2013 while Phase Two is scheduled for May 2014.** Campuses will work with HR Data Operations staff, who will facilitate testing with the campuses and resolve any issues that may arise.

**Campus Requirements**

**Establish Campus Test Coordinators**

In preparation for the Disaster Recovery Testing, campuses must select a test coordinator who will work with HR Data Operations to coordinate testing activities. A Business Process Guide has been provided in Attachment A. The campus test coordinator must have the following qualifications:

- Working knowledge of SCO payroll and employment database applications (e.g., CIRS, PIMS)
- Is a CIRS security coordinator, or
- Is a current security authorizer of SCO applications (form PSD125A)

Please contact Gene Howard, HR Data Operations, at ghoward@calstate.edu to indicate who your campus test coordinator will be by **September 10, 2013**. HR Data Operations will be in contact with campus coordinators with further information in preparation for the October 2013 Disaster Recovery Testing requirements.

Questions regarding this coded memo communication should be directed to systemwide Human Resources at (562) 951-4411. This document is available on the Human Resources Management’s Website at [http://www.calstate.edu/HRAdm/memos.shtml](http://www.calstate.edu/HRAdm/memos.shtml).

EN/It

Attachment
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>iii</td>
</tr>
<tr>
<td>Background on the Disaster Recovery Testing for SCO Applications Project</td>
<td>1</td>
</tr>
<tr>
<td>1. Purpose of the Project</td>
<td>1</td>
</tr>
<tr>
<td>2. Approved Recommendation to Conduct the Disaster Recovery Connectivity Testing</td>
<td>1</td>
</tr>
<tr>
<td>3. Project Stakeholders</td>
<td>2</td>
</tr>
<tr>
<td>4. Project Sponsors</td>
<td>2</td>
</tr>
<tr>
<td>5. Current Project Team Membership</td>
<td>2</td>
</tr>
<tr>
<td>Roles and Responsibilities</td>
<td>3</td>
</tr>
<tr>
<td>Overview of Required Steps with Forms</td>
<td>4</td>
</tr>
<tr>
<td>Process Prerequisites/Assumptions</td>
<td>5</td>
</tr>
<tr>
<td>Details of Required Steps for Disaster Recovery Connectivity Testing</td>
<td>6</td>
</tr>
<tr>
<td>1. Step 1: Complete Required Documentation</td>
<td>6</td>
</tr>
<tr>
<td>2. Step 2: Submit Firewall Access Form</td>
<td>6</td>
</tr>
<tr>
<td>3. Step 3: Set Up Shortcut on Testers' Machine</td>
<td>6</td>
</tr>
<tr>
<td>4. Step 4: Perform Connectivity Testing and Advise HR Data Operations</td>
<td>8</td>
</tr>
<tr>
<td>Proposed Order of Campuses for Disaster Recovery Connectivity Testing</td>
<td>9</td>
</tr>
<tr>
<td>Revision Control</td>
<td>10</td>
</tr>
</tbody>
</table>
Introduction

The Disaster Recovery Testing for SCO Applications Project Business Process Guide will provide an overview of the Disaster Recovery Testing for the State Controller’s Office (SCO) Applications Project and instructions on what is needed for the Disaster Recovery Testing at the campus level. Phase I will cover the initial phase of testing (connectivity testing) while Part II will cover applications testing.

During the connectivity testing (Phase 1) of the Disaster Recovery process, each campus will log on to the SCO Disaster Recovery System to confirm that they are able to successfully connect. This connectivity testing is only done once in the overall course of Disaster Recovery Testing. The user will not need to run any additional applications or perform any Campus Information Retrieval System (CIRS) functions. This test is to confirm that their network and software is configured correctly.

After the initial connectivity testing is completed, campuses will conduct annual application testing in May or October in order to maintain their preparedness in case of an incident that disrupts connections at the Office of Technology Services Gold Camp data center (OTech).

The intent of this document is to provide CSU campuses with the established requirements and steps needed to successfully start Phase 1 of the Disaster Recovery Testing.
Background on the Disaster Recovery Testing for SCO Applications Project

Purpose of the Project
The purpose of this project is to test all SCO applications in the event of a disaster that renders all or part of the equipment and data located at OTech inoperable.

Twice a year, OTech conducts a disaster recovery test at the OTech Vacaville CA test site. All SCO data, programs, and applications (e.g., CIRS, PIMS, HIST, KEYMASTER, PIP, MPC, IDLLS, VIEW and HEAL) are replicated at the Vacaville backup site. Campuses should test to determine whether all critical SCO applications work at the Vacaville site in the same way they do at the OTech Gold Camp data center. If issues arise, OTech, the SCO and HR Data Operations will fix the process so campuses will be prepared and capable of accessing the backup site in the event of a disaster.

Currently if a disaster occurs, it will take six months to find a site and construct a new data center. By participating in the Disaster Recovery Testing, campuses will be assured that they will be able to access all SCO applications within one day.

Approved Recommendation to Conduct the Disaster Recovery Connectivity Testing
After careful consideration of the consequences in the event of a disaster that results in the disruption of network activities, the Project Team concluded that the testing project was necessary in preparing campuses in the event of such an occurrence. Therefore, the Project Team recommended that the CSU proceed in dividing the Disaster Recovery Testing into two phases: a connectivity testing followed by an applications testing. The Long Beach Campus and the Chancellor’s Office Human Resource groups have served as pilots to test and establish a Disaster Recovery model. The proposed testing model is being made available to all campuses. Participation in the two phases of the Disaster Recovery Testing is mandatory for all campuses.
Project Stakeholders

The following entities provided the Disaster Recovery Project Team with critical perspective and recommendations when creating the Disaster Recovery Testing project requirements:

- OTech:
  - Provided testing schedule dates
  - Provided list of Campus IP addresses used by the SCO to allow access to the Disaster Recovery network

- SCO Information Systems Division (ISD):
  - Two months prior to the DR test, SCO will provide HR Data Operations with documentation concerning the dates, goals and objectives, and other documents that are primarily for the SCO
  - One month prior to testing SCO will provide an email confirming the dates, and include the SCO’s staff coordinator listing

- Human Resources Management Data Operations, Chancellor’s Office:
  - Provided initial campus feedback and documented project requirements

Project Sponsors

- Systemwide Human Resources

Current Project Team Membership

- OTech
- State Controller’s Office: ISD
- Human Resources Management, Chancellor’s Office: HR Data Operations
- Long Beach: Payroll Department, HR Tech Support Services
- Testing Pilot subjects: Collaborative Management System (CMS), Human Resources Management, Chancellor’s Office; Payroll, Long Beach campus
Roles and Responsibilities

Several roles are involved in the successful completion of the campus Disaster Recovery Connectivity Testing for SCO Applications. The respective roles and typical responsibilities of all parties involved are noted below:

OTech/California Office of Technology
- Supplies IP addresses and port numbers for campuses. Also manages the Disaster recovery site.

Chancellor’s Office
- **HR Data Operations:** Oversees the project. Works with testers and campus desktop support. Acts as liaison for OTech and SCO staff in coordinating and overseeing project activities. Also maintains the Campus Disaster Recovery Testers form for each campus.

CSU Campuses
Campuses will need to identify a **Test Coordinator** who will oversee the work for the campus. This representative will be responsible for interactions and communications with the Disaster Recovery Project Team. This individual will also be responsible for conducting the connectivity testing at campuses. Below are the typical responsibilities for each area typically involved at the campus level:

- **Payroll:** Identifies campus system users with access to SCO applications, e.g., CIRS, PIMS, HIST, KEYMASTER, PIP, MPC, VIEW and HEAL. Determines if the campus will test printing and File Transfer Protocol (FTP).

- **Desktop Support:** Creates shortcut for the PassPort application to go to the Disaster Recovery Site.
## Overview of Required Steps with Forms

Below is a list of required steps for the campus Disaster Recovery Connectivity Testing along with the responsible parties:

<table>
<thead>
<tr>
<th>Action</th>
<th>Responsible Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Complete required forms and submit to HR Data Operations:</strong></td>
<td>Campus Test Coordinators</td>
</tr>
<tr>
<td>- List of Testers, Desktop Support and Application Users will test.</td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Campus Disaster Recovery Testers Forr" /></td>
<td></td>
</tr>
<tr>
<td>2. <strong>Submit Firewall Access Form</strong> to SCO.</td>
<td>HR Data Operations</td>
</tr>
<tr>
<td><img src="image" alt="SY3DR_1_Vacaville_Firewall_Request.xlsx" /></td>
<td></td>
</tr>
<tr>
<td>3. <strong>Setup shortcut for PassPort</strong> to point to the logon screen for Disaster Recovery.</td>
<td>Campus – IT Services</td>
</tr>
<tr>
<td><img src="image" alt="Creating a Shortcut to the Disaster recovery" /></td>
<td></td>
</tr>
<tr>
<td>4. <strong>Campuses conduct the Connectivity Testing and advise</strong> HR Data Operations of setup completion activities.</td>
<td>Campus</td>
</tr>
<tr>
<td><img src="image" alt="Campus disaster" /></td>
<td></td>
</tr>
<tr>
<td>5. <strong>HR Data Operations informs SCO staff of testing completion and results.</strong></td>
<td>HR Data Operations</td>
</tr>
<tr>
<td><img src="image" alt="Campus disaster" /></td>
<td></td>
</tr>
</tbody>
</table>
## Process Prerequisites/Assumptions

<table>
<thead>
<tr>
<th>Prerequisite/Assumption</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNA/IP Project has been completed at testing campus</td>
<td>Campus has been migrated from SNA to IP in the Disaster Recovery testing process.</td>
</tr>
</tbody>
</table>
Details of Required Steps for Disaster Recovery Connectivity Testing

**Step 1: Complete Required Documentation**

*This step is to be performed by each campus. Campus action required.*

To initiate the Disaster Recovery connectivity testing on the campus, the following listed documentation will need to be **completed and submitted to HRM via Email to jwakayama@calstate.edu.**

- **Campus Disaster Recover Testers Form:** Identify a minimum of two (2) testers per campus, along with a list of applications campuses will test is required.

**Step 2: Submit Firewall Access Form**

*This step is to be performed by HR Data Operations. Campus action required if OTech is unable to provide the list of Campus IP addresses.*

The firewall access form is necessary for the SCO to set up security protocols that will allow the campus to access the Disaster Recovery system. It is assumed that OTech will be able to provide this information. However, if they are unable to, then this information is required from each campus.

**Step 3: Set Up Shortcut on Testers’ Machine**

*This step is to be performed by campus IT services. Campus action is required.*

Follow the instructions below to create a PassPort (emulation software) shortcut to the Disaster Recovery System. Assuming the campus set the connection up in advance of the connectivity test date, the tester will view a black screen for entry.

**Note:** If the campus is not using PassPort, then the settings described below should be configurable in the terminal emulator software used at the campus. The configuration examples provided below relate to the PassPort software.

1) Launch the Passport application
2) From the main menu select ‘File’ then ‘New’. This will start the New Session Wizard:

   ![New Session Wizard](image)

   It should default to **TN3270** and **Display Session**, if it does not make those selections now.

   Click ‘Next’.
3) Enter in the host name as ‘sy5dr.state.ca.gov’, and port 23. The other selections should be set up by default as shown below, if not then make any appropriate changes to the set up so that it matches the screen below.

4) No changes are necessary in this next screen.

5) Confirm that the settings are correct.
Select ‘Finish’.

This will launch PassPort and the application will try to connect to the Disaster Recovery system. However, the system will not be active for connection until the test date, so the tester should see a blank screen.

6) From the main screen Select ‘File’, then ‘Save As’. Save the session file to on the user desktop and name it ‘Disaster Recovery System’. It would be advisable to move the desktop icon away from the normal PassPort icon to prevent accidental use of the Disaster Recovery system.

Step 4: Perform Connectivity Testing and Advise HR Data Operations

This step is to be performed by each campus in coordination with HR Data Operations.

On the specified date of the disaster recovery test, testers will see if they are able to log on to each SCO application. Follow the instructions below to perform the connectivity testing.

1) Run the PassPort Disaster Recovery short cut that will connect to the Disaster Recovery system.
2) Log on to the system as normal.
   a. If testers are able to successfully log on, they will need to logon to each application that has been marked on the Disaster Recovery Tester form, i.e. CIRS, PIMS, HIST, KEYM, PIP, MPC, VIEW, HEAL, etc. Testers will not need to test any further than logging on and off of the system. Upon completion email the HR data Operations team; jwakayama@calstate.edu and ghoward@calstate.edu notifying them that the login to the SCO system was successful. Specify systems successfully accessed
   b. If testers were unable to logon to the system, or any of the applications, the designated campus test coordinator should contact the CIRS Hotline at 916-323-5694 and notify HR Data Operations of the issues encountered.
Proposed Order of Campuses for Disaster Recovery Connectivity Testing

1. Long Beach – Initial pilot – May 15-17, 2013
2. Chancellor’s Office – Initial pilot – May 15-17, 2013
3. All other campuses – October 2013. The exact date will be provided by OTech in September 2013.