PhoneTel Executive Recognition System Testing

# **Test Plan**



Table of Contents

Overview 4

Project Objectives 4

System Description 4

Plan Objectives 4

References 4

Outstanding Issues, Assumptions, Risks and Contingencies 4

Test Scope 5

Features to be Tested 5

Features Not to be Tested 5

Test Methodologies 6

Testing Approach 6

Test Data 6

Test Documents 6

Requirements Validation 6

Control Procedures 6

Test Phases 7

Definition 7

Participants 7

Sources of Data 7

Entrance and Exit Criteria 7

Requirements 7

Work Products 7

Test Completion Acceptance 7

Test Environment 8

Hardware 8

Software 8

Location 8

Staffing and Training 8

Schedule 9

Approvals and Distribution 10

Appendix 11

References 11

Glossary 11

***Document Revision History***

|  |  |  |
| --- | --- | --- |
| **Version Number** | **Date** | **Description** |
| **1.0** | 6/3/2013 | Initial Document version |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Overview

## Project Objectives

1. This project seeks to test the functionality of the Phonetel system in adverse conditions and various circumstances. Testing will occur on various platforms as well as unfavourably scenarios to test for robustness, accessibility, information integrity and security. Compliance testing will also occur to ensure permission segmentation by staff role.

## System Description

Phonetel provides an e-learning portal that seeks to identify potential future executives within an organisation. The major component systems are an e-learning login portal, an e-learning system (that has several components such as javascript games and databases for information storage) and a website for hosting the various components.

## Plan Objectives

The objectives of the plan are to test of all of the scenarios within the various different user cases

* Student logs into e-learning portal to undertake training :
  + Test items and their version
    - * Internet browsers site functionality test: IE v6-10, Chrome v20+, Firefox v12+, Opera v10+, Safari 4+, Dolphin – Current version.
      * Secure login testing (https), security protocols
      * Testing for a compatible browser (and browser add-in components eg Javascript) and case action if there is no browser present or browser is incompatible with site
      * Password resetting facility and verification of student ID
      * Testing of post condition notification systems under both success and fail scenarios.
* Administrator use of Executive Staff Recognition training module
  + - * Login security and security protocol testing.
      * Login and ID verification – proper identification of role
      * Functionality of Administrative tools
      * Proper compliance audit of administrative permission sets by role – correct level of access
* Manager use of Executive Staff Recognition training module
  + - * Login security and security protocol testing.
      * Login and ID verification – proper identification of role
      * Functionality of Administrative tools
      * Proper compliance audit of administrative permission sets by role – correct level of access

## References

## Outstanding Issues, Assumptions, Risks and Contingencies

1. Risk: Availability of a wide range of actors at the required levels of access (Students, Administrators and Managers)

Contingency: One actor to be fully versed and assumes all roles in testing.

1. Assumption: Portal is functional and actor has sufficient time and resources to complete their functions with sufficient access rights
2. Risk: Infrastructure failure at the time of the test

Contingency: Test to be rescheduled

1. Risk : Lack of expertise on hand to fix issues that arise

Contingency: Core technical staff to be present and rostered. All remaining technical staff to be on call.

1. Risk: Business As Usual (BAU) disruption

Contingency: Test to be scheduled out of business hours.

1. Assumptions: A testing kiosk of PCs and handheld hardware(tablets) that can support the full range of testing scenarios.

# Test Scope

## Features to be Tested

* Functionality of the Phonetel e-learning tool for students, executives and manager.
* The secure login system for employees to undertake training
* The secure login system for administrators/managers to view employee results
* The functionality of the memory game for the purpose of training staff
* Testing the current workstation setup for the Phontel Sydney training office
* Capcity of the website hosting for the e-learning portal
* Aesthetics of the site as specified by Section 6 of the specification reference document.

## Features Not to be Tested

## - Any other staff training system

## - Any other Phontel system - Physical hardware setup (assumed)

## - Provision of web hosting (assumed)

## Test Methodologies

## Testing Approach

Students:

Testing requirements: Internet browsers site functionality test: IE v6-10, Chrome v20+, Firefox v12+, Opera v10+, Safari 4+, Dolphin – Current version. Testing is to be conducted offsite by independent contractors with the results to be logged to a central system for immediate verification.

1. The student is to login into the system securely using all browsers specified above. The ability of the browser to properly render the page and accept the website security protocols is to be examined and signed off.
2. Transporting the student to the correct profile information is also to be examined and signed off. The student is to attempt accessing unauthorised information. Access should be denied and any exception is to be immediately flagged.
3. The student is to attempt login to the site with an unsupported broswer. The message flagging the unsupported browsers asking the user to upgrade and the ability to login is denied is to be signed off. Redirection to a page of supported browser links is also to be signed off.
4. The student is to attempt login with and without required 3rd party browser addins such as Javascript. Signoff required on the sites ability to detect the addin requirement and redirect the user to install prior to login.
5. Testing of the training module and the e-learning game is to be carried out and signed off if successful. Error messages are to be logged.
6. The post condition success/fail student and administrator notification is to be signed off.

Administrators:

Testing requirements: Phonetel corporate approved browsers and version (Internet Explorer v7 or 8 and Firefox). Testing is to be conducted both onsite and offsite (with a corporate approved and verified piece of hardware) by in house staff with the results to be logged to a central system for immediate verification.

1. The Administrator is to login into the system securely using only the Phontel corporate approved browser and version (for administrative use, all other browsers are unapproved and out of scope). The ability of the browser to properly render the page and accept the website security protocols is to be examined and signed off.
2. The administrator is to attempt login to the site with an unsupported corporate browser. A message flagging the unsupported browsers and login being denied is to be signed off.
3. Transporting the administrator to the correct profile information is also to be examined and signed off. The administrator is to attempt accessing unauthorised information outside the scope and permission set of their role. Access should be denied and any exception is to be immediately flagged.
4. The functionality of the administration module with regards to the manipulation of employee and employee e-learning records as per the specification file is to be attempted and signed off. Anomalies are to be immediately flagged and referred to the SME.

Managers:

Testing requirements: Internet browsers site functionality test: IE v6-10, Chrome v20+, Firefox v12+, Opera v10+, Safari 4+, Dolphin – Current version. Testing is to be conducted offsite by independent contractors with the results to be logged to a central system for immediate verification.

1. The manager is to login into the system securely using all browsers specified above. The ability of the browser to properly render the page and accept the website security protocols is to be examined and signed off.
2. Transporting the manager to the correct profile information is also to be examined and signed off. The student is to attempt accessing unauthorised information. Access should be denied and any exception is to be immediately flagged.
3. The manager is to attempt login to the site with an unsupported broswer. The message flagging the unsupported browsers asking the user to upgrade and the ability to login is denied is to be signed off. Redirection to a page of supported browser links is also to be signed off.
4. The manager is to attempt login with and without required 3rd party browser addins such as Javascript. Signoff required on the sites ability to detect the addin requirement and redirect the user to install prior to login.
5. Testing of the training module and the viewing of employee e-learning records is to be carried out and signed off if successful. Error messages are to be logged.

## Test Documents

* Testing workflow documents : Student, Administrator and Manager versions. This document identifies step by step testing tasks with sign off for a successfully completed review.
* Fault Logging/Incident Management document. All unsuccessfully completed tasks, faults and testing issues must be immediately logged with the Test Lead. The project management team is to risk assess the fault, issue or unsuccessful task according to the risk matrix.
* Post test review document: This reviews the test process and examines what could have been improved and recommendations about the changes that need to be made.
* Problem Management and Change Management documents: To be produced in resolving problems that arise as logged in the Fault Logging/Incident Management document. If the changes required to resolve a problem are sufficient in scope and magnitude, then the Change Management process may be invoked and the Change Advisory Board may be convened.

## Requirements Validation

Project Report Writer Julie Wilks will generate the test workflow signoff documentation and map the output of testing to the testing workflow as specified in the System Specification document section 3.3 User Case Identification. Anomalies will be reconciled to the Fault Logging/Incident Management document. A full fault report will be generated and presented to the Project Lead for risk assessment.

## Control Procedures

Test workflow and signoff documentation is to be produced in Student, Administrator and Manager versions that document the User Cases in section 3.3 of the specification documentation. Major signoff points are to be highlighted and vigorous testing of these points and exceptions is to be conducted. A result for these scenarios (either positive or negative) MUST be recorded or the test will be deemed incomplete.

# Test Phases

### Unit testing

Unit testing, also known as component testing, refers to tests that verify the functionality of a specific section of code, usually at the function level. In an object-oriented environment, this is usually at the class level, and the minimal unit tests include the constructors and destructors.

***Definition***

Unit testing are tests that verify the functionality of a specific section of code.

***Participants***

Unit tests will be carried out by Student, Administrator and Management Actors.

***Sources Of Data***

Student and Management Data can be example data that covers multiple scenarios. This data can be manufactured to suit purpose or it can be a duplicate of live student and management data so that the original data can maintain integrity.

***Entrance And Exit Criteria***

These are documented in the User Case Scenarios in section 3.3 of the Specification Documentation.

## Requirements

The requirements are Actors for all 3 scenarios (Student, Administrator and Management), technical staff on standby for all critical systems, the availability of all project leads and consulting staff.

## Work Products

The output of the testing should generate completed signoff documents for all User Cases as well as a Fault Logging/ Incident Management documentation.

## Test Completion Acceptance

Test completion should only occur when all major signoff points on the User Case Scenarios have recorded a result of either pass or fail. A failure to record a successful outcome should result in a Fault Logging/ Incident Management document entry. A failure to record any result against a required User Case signoff point should deem the test incomplete and should not be signed off as complete.

# Test Environment

## Hardware

User and Management testing should be conducted on a variety of adhoc machines which reflect the potential scope of hardware that may be used by potential PhoneTel clients. Administrator testing should be conducted on in house approved hardware only.

## Software

Internet Web Browsers that are to be used by the various actor groups are described in the Testing Approach section of this document.

## Location

The tests are to be conducted in a variety of locations that reflect the likely real life environments of the Student, Administrator and Management groups. Administrator testing is to be carried out in the PhoneTel Offices and on corporate approved remote working laptops used by the Administrators from a remote location.

## Staffing and Training

Availability of PhoneTel Administrators and Student and Management Actors are required.

The level of knowledge required by Student and Management Actors is the level equivalent to client training given to all PhoneTel clients (preferably provided by current PhoneTel training courses or documentation). Any over training or provision of information that would not normally be given to a PhoneTel client will compromise the integrity of the test.

# Schedule

Testing is to be conducted outside of business hours. The preference is for an available Friday evening or Saturday morning (subject to availability in the Change Management calendar and not conflicting with crucial corporate deadlines). This will allow for sufficient time to recover from any form of system failure in time for Business As Usual activities to resume on Monday.

# Approvals and Distribution

Identify the required approvers of the test plan and results as well as to whom the test plan document(s) is distributed.

Approvers

Assessor -

Phontel key stakeholder: Dianne King – Training manager

Cortrain key stakeholder: Dr John Spencer – Managing director, Cortrain

Distributiion List

PhoneTel Executive Board

PhoneTel Change Advisory Board

Required Student, Manager and Administrator Actors

Report writer:

# Appendix

## Test Data (appendix)

Test data will be a subset of live data that will be duplicated in order to provide the best rendition of live scenarios. A diverse set of PhoneTel client data should be used. A FULL DATA BACKUP is to occur before the test in the event that data is corrupted and restoration is required back to a current Business As Usual level. A mock set of invalid data and incomplete records should also be created by the Administrative team to enable for the testing of exceptions.

## References

*Source: SystemSpecfication\_Phonetel.doc By Julie Wilks*

*“Phonetel e-learning portal: Recognise Executive Staff E\_Learning Module Phase 4 – System Specification”*

## Glossary

SME - Subject Matter Expert.

Incident Management - The process of identifying faults in order to analyse and rectify them. An Incident Management system is the system where faults are logged so that they may be tracked until resolution.

Problem Management - The process that is invoked when an incident poses a sufficient risk (operational, reputational or revenue) to the organisation and required investigation in order to rectify the issue.

Change Management - The process of invoking organisational change of a system in order to rectify a problem. Change Management is a co-ordinated activity that ensures that multiple system changes occur in such a manner that minimizes organisational risk.

Change Advisory Board (CAB) – The group of stakeholders within an organisation that approve system changes and the change timetable.