|  |  |
| --- | --- |
| **DEP Logo** | **Department of Environmental Protection** |
| ***STD-09061812.2.0*** | ***Page 1 of 8*** |
| **Portal Standard** | |

# Purpose

This document specifies the Florida Department of Environmental Protection’s (DEP) Portal Standard. The purpose of this standard is to ensure that DEP application development follows the specifications for integrating with the DEP Portal page, DEP Portlets and Oracle Internet Directory (OID) Security.

# Scope

This standard applies to all application development at DEP.

# Standard

Developers shall comply with the DEP Portal Specification in the Appendix to this standard. This specification provides requirements for securing DEP applications using Portal, Portlets and OID Security.

# Deviation from Use

Any deviation from this standard shall be documented in associated project and contract documentation. For contracts, deviation from standard shall be documented and approved by the DEP contract manager. For non-contract work, deviation from use shall be documented in the project plan/scope of work and approved by the project manager.

# Appendix

*Portal Specifications.*

**Approved by R. John Willmott, CIO \_\_\_\_\_\_\_\_\_4/1/10 \_\_\_\_\_\_\_\_\_**

**Approval Date**

# Appendix – Portal Specifications

# Overview

# Purpose

This document provides an overview of overview of the DEP Portal, its layout and the usage of Portlets on the Portal. This document also specifies how DEP will secure those Portlets and the requirements for using the Security features of the Portal and Oracle Identity Management suite of products.

# Requirements

Portlet Usage

All projects’ application entry point will be linked to via static URLs to be placed into the respective Portlet for the application. The placement of the link in a portlet will be based upon the scope of the project’s users and must be approved by OTIS staff prior to implementation. Only OTIS technical resources may make changes to the portlets, and all changes must be pre-approved.

Single Sign On

All applications will be secured behind the Single Sign On features of the Oracle Identity Management suite and all applications will use the supplied Authentication Filter found in the SVN repository as module securitymanager-n.n.n.jar (use most current version), and available via the OTIS technical Wiki found on the DEP Integration platform Portal.

Self Registration

All external users will self-register on the DEP Portal and maintain their own userids, passwords, and PINs through the Portal and the DEP Security Suite found under the Enterprise Tools “Security Management” portlet.

# Background

DEP has chosen the Oracle Portal environment as the sole environment for all new development work. The Oracle Identity Management suite is the tool of choice for all security in this framework.

# Portal

The Oracle Portal has been chosen as the core product suite and will feature pages for initial access with links to open (non-secured) applications – such as subscription services and mapping tools – and a page for secured application access. This is a sample of the proposed Public page for the Portal – the first page that all users will see when accessing DEP from outside the agency.



Figure 0‑1. Public Portal Page

# Portlets

The primary navigation into FDEP applications, components, and tools will be via links on grouped portlets. The portlets will be grouped into “Divisional Services”, “Enterprise Services”, and “Enterprise Tools” on the main page, as seen here:

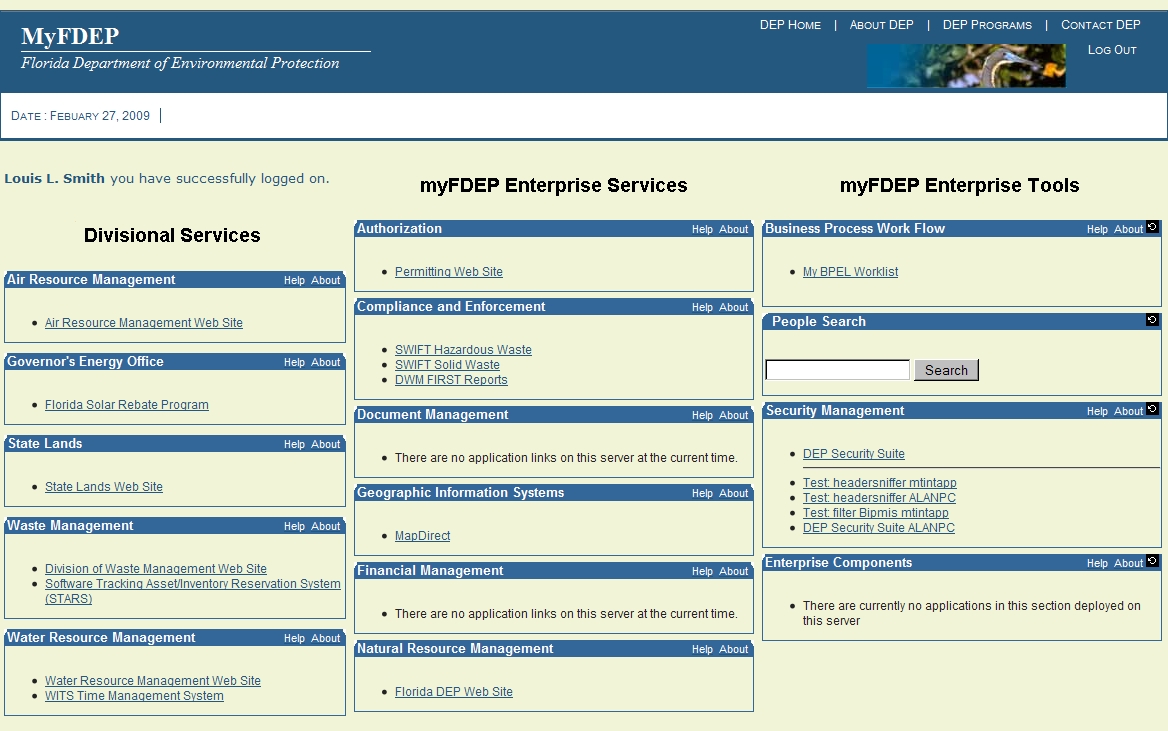


Figure 0‑2. Secure Access Portal Page

# Security

# SSO

The Oracle Single Sign On security framework has been chosen to implement all security for the new environment. The Portal features a self-registration aspect for the public and other external users of the systems to obtain log-in credentials, to reset lost passwords, and to interact with approved applications of the Agency.

# Portlet Security

In order to properly secure Portlets without a burdensome level of manual effort, a logical grouping has been proposed which will classify the Portlets into the three columns shown in Figure 2.2 above.

Divisional Services

The group for divisional services encompasses those applications that are primarily used only by the direct employees of that division.

Enterprise Services

The group for Enterprise Services encompasses those applications that cross-divisional boundaries or are aligned to the Integrated Management System (IMS) Core Areas.

Enterprise Tools

The group for Enterprise Tools encompasses those applications that are above the level of individual applications, or are components used by any application within the Agency. These include applications used by the development community (such as the DEP Technical Wiki) and Enterprise Tools such as Security Components which all registered users may need.

# Security Groups

Security groups have been established to further limit access to the Portlets. The following security groups have been established for the FDEP enterprise:

Divisional Services

The security groups for Divisional Services will be “DIV\_” and the Division Acronym.

|  |  |
| --- | --- |
| DIV\_ARM | Access granted to staff of the Division of Air Resource Management. |
| DIV\_SL | Access granted to staff of the Division of State Lands. |
| DIV\_WASTE | Access granted to staff of the Division of Waste Management. |
| DIV\_DWRM | Access granted to staff of the Division of Water Resource Management. |
| DIV\_DEAR | Access granted to staff of the Division of Environmental Assessment and Restoration. |
| DIV\_GEO | Open to the public, no security required. |

Enterprise Services

The security groups for Enterprise Services will be “SVC\_” and the short name of the functional area

|  |  |
| --- | --- |
| SVC\_AUTH | Links to access permitting and registration applications. |
| SVC\_COMP | Links to access compliance and enforcement applications. |
| SVC\_DOC | Links to access Oculus. |
| SVC\_FIN | Links to access financial management applications. |
| SVC\_GIS | Links to access GIS applications and tools. |
| SVC\_NATUR | Links to access Recs and Parks applications. |

Enterprise Tools

The security groups for Enterprise Tools will be “ENT\_” and the short name of the tool group

|  |  |
| --- | --- |
| ENT\_BPEL | Links to the Oracle SOA management consoles. |
| ENT\_COMP | Links to DEP components???? |
| ENT\_SEC | Links to DEP application security consoles. |
| ENT\_INFO | Links to DEP information consoles. |

# Application Level Security

# Authentication

All applications must utilize the Authenticate Filter as supplied by OTIS to secure their applications from direct URL addressing (such as users bookmarking a page). The filter will force a user who attempts direct access to supply their SSO credentials.

Additionally, the filter will automatically populate a User Information Object, which will be placed into the application’s session scope and is to be used to obtain the following information on the current user:

First Name, Last Name, Full Name, e-Mail, Secondary User ID

The usage of this object and the details of its fields are found in the ***JEE Security Framework Standard*** (FL Dept. of Environmental Protection, 2010).

# Authorization

Applications needing role based security must establish an Application Group as well as Application Role Security Groups. The Application Group and Application Role Security Groups will be established in Oracle Identity Manager (OIM).

Application Group Container

Applications needing role-based security must establish an Application Group named according to the Application context root. See the ***Java Application Naming Standard*** (FL Dept. of Environmental Protection, 2010) for guidance on naming the Application context root.

Role Security Groups

Role Security Group names must be descriptive values consisting of one to three words. The Application Group name should not be included in the group name since the groups fall under the Application Group in the OIM hierarchy.

Application Access to Role Security Groups

Applications must retrieve Role Security Groups using standard JAZN system calls.

# Bibliography

FL Dept. of Environmental Protection. (2010). *DEP JEE Security Framework Standard.* Tallahassee: FL DEP.

FL Dept. of Environmental Protection. (2010). *Java Application Naming Standard.* Tallahassee: FL DEP .

**Approved by R. John Willmott, CIO \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Approval Date**