Application Owner Roles and Responsibilities (R&R)

V 1.0

1. Introduction

This document establishes standards for the roles and responsibilities of the application owner of web based applications, not hosted or managed by Chapman University IS&T department.

2. Purpose

The objective of this standard is to establish guidelines for adding, maintaining, disabling, and deleting user access to the University's data maintained on web-based applications not hosted or managed by Chapman University IS&T department

3. Definitions:

3.1 Application Owner:

Chapman University employee that is the business owner of the application and is responsible for the business delivery, functioning and services of the application. The application owner is also the custodian of the data in the application.

3.2 Role:

A role defines a set of users that share the same informational needs, based on their need-to-know. This is commonly known as Role Based Security.

3.3 User:

The end-user of the application. A user can be assigned to an account role

4. Security principles

4.1 Need to know

Users should be granted access only to data that they need to know or work with.

4.2 Least privilege

User should have the least level of access permissions so that the user has access only to the data that they are required to see and work with.

5. Application owner - primary responsibilities:

5.1 Account Management

- Owner of application account provisioning and de-provisioning

    - The application owner will provision or add a new user to the application using the principles of least privilege and need to know
    - The application owner will de-provision or remove access to an existing user to the application as soon as possible (within one business day or earlier)
- Owner of application role management assignments and changes (updating existing users)
    - The application owner will set up the roles and the corresponding entitlements within each role in the application. E.g. Admin role or data entry role
    - The application owner will assign and modify users to roles in the application based on need to know and least privilege. The application owner will assign users to roles e.g. Newly joined manager assigned to admin role. If the current user has moved to a different job function, then the application owner should modify user's role assignment in the application accordingly

5.2 Manage Application portal security settings

The application owner will set application portal security settings.

These include but are not limited to:

- Number of login attempts and lockout policies
- Process for changing and resetting passwords
- Requirements for security questions

5.3 Password policy

Most applications rely heavily on the user password as the primary means to protect access to the application (and related Chapman data). The Application owner will set password policy corresponding to requirements for the University active directory password system. These policies currently are available with the information security office

5.4 Response

- Application owner will notify their management as well as the office of information security of any breach of University data or account misuse

5.5 Review and Audit

- Periodic review (quarterly) of accounts status and roles ((once per quarter recommended but at least once per six months)

    - The application owner will periodically review the roles, roles assignments and user's access within the application
    - Document the periodic review, if not already available through the application.

6. Document owner

Review and updates of this standard is the responsibility of the Chief Information Security Officer.

7. Reference

Information Security Policy– Access Control