System Security Plan

<Agency's Name>
<Application/System name>

<Date Submitted>

CONFIDENTIAL

For Official Use Only - Portions of this information may be exempt from disclosure under the Colorado Open Records Act. Colorado Revised Statute 24-72-204(2)(a)(VIII)(A).

Contents

PLEASE ADJUSY THE TABLE OF CONTENT NUMBERING AS NEEDED

System Record of Changes

Modifications made to this plan, since the last printing, should be documented here for audit and process management purposes

Date	Item	Description	Author	Version

System Security Plan

Introduction

The purpose of a System Security Plan (SSP) is

- To document the security requirements of the system and describe the controls in place or planned to meet all applicable State Cyber Security Policies requirements and ultimately reduces the risk introduced by the system/application.
- To delineate responsibilities and expected behavior of all individuals who access the system.
- To establish and document the security controls, and form the basis for the authorization of individuals to perform security related activities in the system, supplemented by the Risk Assessment Report (RAR) and the Plan Of Actions and Milestones (POAM).

The objectives of this SSP are

- To improve protection of information system resources.
- To document the protection of the system security.
- To respond to Internal and External system security Audits.
- To demonstrate documented compliance to state and federal mandates.

This is a living document subject to annual review and regular updates as needed.

System Identification

Put system/application name(s) known by the program, IT, and end users.

Example: **LegalFiles – case management system for the Office of Administrative Courts**

Security Team Roles and Responsibilities

Business System Owner

The Business System Owner has sufficient knowledge of the system to be able to provide additional information or points of contact regarding the security plan and the system, as needed. They are the decision making authority as to budgetary and operation function of the system or solution.

Name:		**Address:**	
Title:		**Phone**	
Agency:		**E-mail**	

System Data Owner

The Data Owner is the designated individual who is ultimately responsible for the Confidentiality, Integrity and Availability (CIA) of the data owned by the System Owner. This individual typically determines how data is accessed, who the data is accessed by, its *distribution and security. This individual has a clear understanding of all state, national, federal or international laws and regulations governing the security and access of the data.*

Name:		**Address:**	
Title:		**Phone**	
Agency:		**E-mail**	

Agency IT Director

The Agency IT Director is the designated OIT representative responsible for the general management of the IT system or solution utilized by a system owner or agency. This individual is the decision making authority over budgetary requirements, project design, disaster recovery and ongoing maintenance and support of the system or solution for the system owner or agency.

Name:		**Address:**	
Title:		**Phone**	
Agency:		**E-mail**	

Chief Information Security Officer

The Chief Information Security Officer (CISO) or delagate is ultimately responsible for the security of the system and has assigned responsibility to ensure that the application has adequate security and is knowledgeable of the management, operational, and technical controls used to protect the system.

Name:		**Address:**	
Title:		**Phone**	
Agency:		**E-mail**	

System Subject Matter Expert / Administrator

The Subject Matter Expert (SME) is the individual responsible for the overall business management and administration of the system. This individual is involved in all operational discussions for the system to include user access control, documentation, applications, data, design and disaster recovery requirements for the system and is the primary business contact for all security events affecting the system.

Name:		**Address:**	
Title:		**Phone**	
Agency:		**E-mail**	

Authorizing Security Official

The Colorado Chief Information Security Officer (CISO) or delegate after review of each System Security Plan (SSP) is the individual responsible for sponsoring and approving the operation or denying operation of state computing systems and solutions for the state of Colorado.

Name:	Jonathan Trull/Delegate	**Address:**	601 W. 18th Ave., Denver, CO
Title:	State of Colorado CISO	**Phone**	303-764-7994
Agency:	OIT	**E-mail**	Jonathan.Trull@state.co.us

General System Design Description

System Environment – Architecture/Diagram

Infrastructure Diagram

Technical Specifications

System Attributes	Description
Architecture & Operating Environment	
Software	
Physical Environment	
Interfaces	

Compliance Requirements

There are several standards/acts/regulations that apply to the IT systems depending on type of data that is hosted within the application. For example HIPPA, FISMA, PCI, SSA etc. List, below any such standards/acts/regulation that the IT systems needs to adhere to.

Existing and Planned Security Controls:

Security Requirement	Existing Controls	Planned Controls
1. Identify unique requirements for protecting the application or system and system information in the case of disaster recovery operations.		
2. Describe the application or system's user authentication requirements.		
3. Describe the application or system's system integrity requirements.		
4. For electronic commerce systems involving financial transactions, describe how you are ensuring that the parties in a transaction cannot deny that the transaction took place.		
5. Describe the application or system access controls and their rules for all levels of the system and/or application.		
6. Describe the audit trails that will be captured and the details included in the audit trail for tracking administrative actions that impact access or change to critical data.		
7. Security Control selection (*how did we select the controls)*		
8. Physical barriers around the area where the system resides		
9. Workstation security		
10. Backup Frequency		
11. Backup Plan		
12. Disaster Recovery Plan		
13. System Review		
14. Policy Waiver		

Security Requirement	Existing Controls	Planned Controls
15. Describe the process to define user access rights based on the individual's need to view and manipulate data within the application or system.		
16. Describe procedures for requesting, establishing, issuing, and closing user accounts in the system or application. These procedures must include the process for reviewing and confirming access rights on a specified schedule.		
17. Describe the procedures for identifying and reporting security violations.		
18. Vulnerability/Penetration testing documents available?		
19. Interface Security (*transmission security, access control)*		
20. Vendor Access		
21. User Access		
22. Server patch installs/upgrades		
23. Application patch installs/upgrades		
24. Change Management		
25. System Admin Procedures and Responsibilities		
26. Server Access Control		

For all Web Based Application, the following OWASP TOP 10 must be addressed:

https://www.owasp.org/index.php/Top_10_2013-Top_10

Vulnerability	Description	Mitigation Status
A1-Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.	
A2-Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.	
A3-Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.	
A4-Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.	
A5-Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date.	
A6-Sensitive Data Exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax ids, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser	
A7-Missing Function Level Access Control	Virtually all web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access unauthorized functionality.	

A8-Cross-Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests the vulnerable application thinks are legitimate requests from the victim.	
A9-Using Components with Known Vulnerabilities	Vulnerable components, such as libraries, frameworks, and other software modules almost always run with full privilege. So, if exploited, they can cause serious data loss or server takeover. Applications using these vulnerable components may undermine their defenses and enable a range of possible attacks and impacts.	
A10-Unvalidated Redirects and forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.	