H-GAC Secure Application and System Development Guidelines

HOUSTON – GALVESTON AREA COUNCIL

Prepared by the Data Services Information Security Manager
Last update June 13, 2022

TABLE OF CONTENTS

INTRODUCTION

Customized applications and software solutions are needed for business processes and tasks where an out-of-the-box solution is not able to meet the needs. Because of the customizations where the solution is built from the ground up, we must ensure it is coded and developed in a stable and secure manner. In addition, we must provide a means to quickly resolve software bugs and mitigate security vulnerabilities discovered after implementation. Out-of-the-box applications will also need to meet minimum security standards

In addition to securely developing applications, a proper development life cycle is needed to ensure the application maintains its data integrity and availability as code changes, functionality changes, and platform changes are experienced throughout its life. It also ensures the data is properly archived or destroyed as the application is retired.

1. PURPOSE AND BENEFITS

This guide is to establish specific security practices and requirements for all applications and software developed for the agency. It also establishes guidelines for proper handling of data created, consumed, stored, and served. These security practices are well known industry standards and should be applicable to the implementation regardless of the platform used for development. This guide will also recommend the proper steps for managing the implementation, changes, and retirement of the application.

2. ROLES AND RESPONSIBILITIES

The Data Services Information Security Manager and Data Services Director are responsible for the development, outline, and update of this document. All agency staff and contractors solicited by the agency shall review this guide, understand, and implement security protocols defined in this guide as is applicable to their implementation. All policies and protocols created are to be presented to and approved by the Information Services Steering Committee and the Executive Director of H-GAC.

3. SCOPE

This policy encompasses all systems, automated and manual, for which the agency has administrative responsibility, including systems managed or hosted by contractors, consultants and third parties on behalf of the agency. It addresses all information and services, regardless of the form or format, which is created or used in support of business activities.

GUIDELINES

These guidelines define the minimum standards to be implemented on all applications developed and any associated data. Security measures and protocols may exceed these standards as deemed appropriate for the situation.

1. SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

Integrating security into each step of the development process is the most effective way to protect information and information systems. The multistep process includes the following:

- Initiation
- Acquisition/Development
- Implementation/Assessment
- Operations/Maintenance
- Sunset (Disposal)

These steps are defined by the National Institutes of Standards and Technology (NIST) and references various special publications by NIST. Please refer to the NIST document for additional information and details. It will be up to the system developer and system adopter to review the SDLC guidelines and develop a plan that best fits the business model while considering what the acceptable costs, risks, and threats to the program and stakeholders are. The System Development Life Cycle (SDLC) | NIST

While determining what are the appropriate SDLC processes and details, the following sections describe what should be considered critical elements of that SDLC process and should be incorporated.

2. APPLICATION AVAILABILITY AND INTEGRITY

All applications developed and implemented for the agency shall take all feasible measures to ensure the application is available for service and the operation and data remains intact. Implementation of the application shall address threats such as:

- Distributed Denial of Service (DDoS) attacks.
- Identity theft
- Unauthorized access
- Exploitation of vulnerabilities

3. DATA STORAGE AND TRANSMISSION

Information created, received, stored, or delivered must provide measures of protection to ensure the integrity of the data and that only the appropriate end user interacts with the system.

- Data at rest must be encrypted using industry standard encryption methods regardless of the data type or storage mechanism such as flat files stored on the local disk, SQL database, or proprietary storage mechanism.
- Data in transmission must be encrypted using industry standard encryption methods.

4. ROLE BASED ACCESS CONTROL

Access to information and services should be limited to authorized users as the business needs require and should be defined based on roles. Methods of access and authentication should leverage the agency's standard methods for access control where possible.

- Verify that the principle of least privilege exists – users should only be able to access functions, data files, URLs, controllers, services, and other resources, for which they possess specific authorization.
- Roles should be clearly defined within the application.

5. AUTHENTICATION AND CREDENTIAL MANAGEMENT

Applications should uniquely identify and authenticate users or processes acting on behalf of the users. Authentication methods for management accounts ideally should leverage Multi-Factor Authentication and Single Sign-On with an accredited Identity Management Provider (IdP). If the business stakeholders have performed a risk assessment and deem that local management of authentication and accounts is acceptable, then credentials can be stored locally but shall be encrypted at rest and stored in a secure manner.

6. ACCESS LOGS AND EVENTS

All access and configuration change events shall be logged and recorded for periodic review. Logs should be kept for a minimum of three (3) months and have a means of purging out logs in the event storage is unavailable or has been determined it is not needed anymore.

7. APPLICATION CODE AND DATA OWNERSHIP

All applications developed for the agency, whether managed and hosted by the agency or by another entity on behalf of the agency, shall be fully owned by the agency. At the completion of development, a copy of all development source code shall be delivered to the agency without any restrictions on modifications or use. All data created or recorded by the application shall be owned by the agency exclusively.

If exclusive ownership of the application code and data presents a conflict with the business requirements, the case(s) should be evaluated as part of the business risk assessment and be formally documented.

8. APPLICATION MAINTENANCE AND SUPPORT

Maintenance and support must be provided throughout the life of the application. In the event an operational bug or security vulnerability is discovered, it can be addressed and remediated quickly and properly. If maintenance of the application is no longer available, the application and data should be decommissioned and archived in accordance with the appropriate retention schedule.

9. CHANGE MANAGEMENT

Applications are constantly being developed to incorporate new features required by the ever-changing business, restore functionality due to changes to the platform or network architecture, or the deprecation of functionality. With each change there is a chance to introduce a new vulnerability. These vulnerabilities could include inadvertent exposure of unintended data, the application becomes unavailable to the end user, corruption to the data or code, and others. It is important to incorporate a proper testing procedure to the application each time a change is made. The application developer and owner will be required to incorporate a change management process that adequately tests the application to ensure the application remains available and its data intact.

10. RESOURCES AND BEST PRACTICES

Security best practices and technologies evolve over time. Standards specified today may become outdated as new technologies emerge or business requirements evolve. The developers and stakeholders should incorporate into their periodic review of the application the following resources for best practices and technologies. Developers should review these resources and ensure any of the applicable measures are incorporated.

- OWASP Cheat Sheet Series | OWASP Foundation
- Securing Web Application Technologies : [SWAT] Checklist | SANS Institute