1. Application Security Auditing - Procedure

CERT-K provides application security audit service for government agencies based on CERT-K engagement policy. Security auditing process flow is as follows:

1. As per Government Order# G.O.(Ms) No 43/2015/ITD dt 01/10/2015, any e-Governance application of a Government organization has to be security audited before launching it. It is strongly recommended to host the application at either if the State Data Centres SDC1 or SDC2.
2. Department has to submit request to hosting the web application/website in SDC-1 / SDC-2. The application form can be downloaded from KSITM website under Downloads>Application Forms link.
3. SDC provisions server resources in a Staging environment where the department has to host the application.
4. Once the application is set up on the staging server, the department needs to get the application security audited by a CERT-In empanelled agency or CERT-K.
5. CERT-K provides security audit service at no cost; however, due to increased demand, the department has to plan at least 2 months exclusively for Security audit, i.e., if department has a tentative date for launching the application, the application should be made available to CERT-K for auditing at least 2 months earlier.
6. To request CERT-K for audit, the department may send request to ***cert.ksitm@kerala.gov.in*** with the technical design details of the application and details of the application hosted in the staging environment. The application given for testing has to be the final version.
7. CERT-K then tests the application to find out vulnerabilities in the application. Phase 1 report is submitted to the department.
8. The department needs to get the security defects fixed and needs to re-submit the application for testing. CERT-K repeats the testing, provides phase 2 report and continues the cycle until all defects are cleared.
9. Once all defects are cleared, Safe to Host certificate is provided to the department as well as the hosting agency. The application can then be moved to Production servers to make it accessible to public.
10. Security audit is not a one time process. The application has to be re-audited at least once in every two years or when there is a change in the functionality. If there is a change, it needs to be communicated to SDC and CERT-K to check if a re-audit is required.

The following best practices may be followed from an application security perspective:

1. Department and the technical team who develops applications should be aware of the application security procedures to be followed.
2. Department needs to formally communicate to the development team during Requirements phase itself that security of the application is a primary requirement.
3. The technical team needs to conider Security during the design stage of the application itself. Architecture and design documents need to be created by the development team and delivered to the department. It is required by CERT-K as well for security auditing for reference.
4. Programmers need to follow coding standards during coding. Open source code analyzers such as Sonar needs to be used by the development team to improve the quality of source code and to minimize security defects.
5. The development team may by itself perform an internal security vulnerability testing based on 'OWASP Top 10' vulnerabilitiess using open source tools so that there are few defects during external security testing.
6. Department needs to include application ,security maintenance as one of the requirements of the Annual Maintenance Contract with the development vendor. Responsibility should be fixed as to who will install pathches/ upgrade of the development platforms such as Runtime environment (PHP, Java etc), Operating System, WebServer periodically. System Administrator has to be entrusted for the above.

2. Incident Management

CERT-K's Incident Response Service provides the capability to address and respond to security incidents that may impact IT assets of a Government organization. On the occurrence of a security incident, the concerned Department needs to intimate CERT-K. The procedures involved in Incident reponse/Handling of a web application are as follows:

1. If a web application/website belonging to Kerala Government which is hosted in data centre/other hosting agency gets defaced, the details of the incident needs to be intimated among the stakeholders – owner department, SDC/ hosting agency and CERT-K. CERT-K instructs State Data Centre or the hosting agency to pull down the website from public access in order to prevent further potential damage to other systems.
2. CERT-K collects details about the application and does a preliminary analysis of the incident. CERT-K provides minimum security steps to be taken by the department to remediate and mitigate risks to restore systems back online.
3. The hosting agency needs to provide restricted access to CERT-K to verify the steps implemented.

4. Once the department implements security steps recommended by CERT-K, CERT-K verifies the same and instructs if the application can be made Live again.
5. CERT-K further collects logs of affecetd systems for detailed incident analysis from State Data Centre/ hosting agency.
6. CERT-K team will analyse the incident to find out the root cause. A detailed incident analysis report will be prepared and sent to the department. The report will contains how the attack has happened, attack methodologies, Log traces of the attack and security recommendations to followed etc. A copy of the Incident report is also shared with CERT-In.
7. CERT-K further instructs the department to get a full fledged application security audit done by any CERT-In empanelled agency within a definite timeline.

3. Crisis Management Plan

CERT-In under Ministry of Electronics and Information Technology Government of India has mandated that a Crisis Management Plan be prepared by every State and Organization internally. CERT-K will coordinate with departments in creating Crisis Management Plan for the state.