

F8(214)/DoIT/Gen/13/ I/12280/2013Dated : 15.10.13

Circular

Security Audit Guidelines for web based contents hosted in RSDC

1.0 Purpose

The purpose of this policy to regulate the safe guarding of a hosted web based content / application by proactive method. The policy address the requirement of pre-hosting audits of applications and their subsequent hardening such that possible malicious penetration is minimized. The procedure for web hosting and security auditing will be as follows:

2.0 Policy

2.1 For new web based contents:

2.1.1 Request for hosting:

- a. The department after UAT and completion of hosting procedures would request the RSDC with the filled Web Hosting form duly signed and sealed by Head of the Department.

2.1.2 Staging Environment:

- b. All new web based contents would be hosted in the staging environment as per the “Hosting Procedures of RSDC”.
- c. The web based contents should be audited by a cert-in empanelled firm as per GIGW guidelines. The audit carried out shall highlight the vulnerabilities observed.
- d. The vulnerabilities shall be identified and communicated in predefine structured format to the respective nodal officer of the department.
- e. Once vulnerabilities are informed to the nodal officer, he/she shall get them removed/patched from the respective development agency as per audit recommendation and again get it submitted for security audit. This shall be iteratively performed till the contents are cleared as “safe for hosting”. Once vulnerabilities are removed, a ‘Safe to Host’ certificate is issued by auditing agency.
- f. In case vulnerabilities are not removed and the security audit certificate is not submitted within a reasonable period of time, the web based contents shall be removed from staging environment.

2.1.3 Production environment:

- g. Any web site / web based contents / application to be hosted in RSDC shall require mandatory approval of Director / Commissioner, IT&C.
- h. “Safe to Host” certificate is mandatory for all web based content hosted in Rajasthan State Data Centre.

GOVERNMENT OF RAJASTHAN

Department of Information Technology & Communication

- i. On receipt of "Safe to Host" certificate, the web based content shall be moved to Production environment.
- j. In some cases, low or medium risk vulnerabilities may move to the Production environment, on the recommendation of the auditing agency.

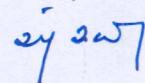
2.2 For existing web based contents:

- k. All web based contents hosted in the Production environment of the RSDC shall be security audited regularly as follows:
 1. **Yearly Audit:** All web-based contents hosted in RSDC shall be audited every year.
 2. **Bi-annual Audit:** All web based applications with payment gateway and critical transactions or undergoing frequent changes shall undergo bi-annual security audit.
 3. If at any instance a web site or web application is found to be vulnerable or having malicious contents, it may be decided to restrict web access to the same.

3.0 Responsibilities

All designers / developers / development agencies and site owners responsible for web based contents / site / application development shall take necessary action as per this policy. It shall be the responsibility of the RSDC Team to ensure adherence to this policy.

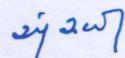
The policy shall come into force immediately from the date of issue of this circular. The web sites / web based application which have not obtained "safe to host" certificate are required to obtain the same by 15 November, 2013. After this date, web access to web sites / web based applications not adhering to above policy or not having "safe to host certificate" shall be restricted.



(Sanjay Malhotra
Secretary IT&C

Copy for information and necessary action to:

1. Additional Chief Secretary to H.E., the Governor of Rajasthan
2. Principal Secretary to Chief Minister, Rajasthan
3. P.S. to Chief Secretary, Government of Rajasthan
4. All Additional Chief Secretaries, Government of Rajasthan
5. All Principal Secretaries, Government of Rajasthan
6. All Secretaries, Government of Rajasthan
7. All Head of Departments, Government of Rajasthan
8. All District Collectors, Government of Rajasthan
9. Guard file



Secretary IT&C