General Guidelines for Secure Application and Infrastructure

S.No.	Action Item(s)
1	All your web-applications should be security Audited initially (for Web-application/mobile apps) • In every two years • Or whenever new module/page is added or modified or functionality is changed
2	In all web-applications/mobile-apps incorporate security requirements at the design and development phases.
3	Ensure that web-applications are deployed on hardened servers/infrastructures.
4	All components on server should be hardened and latest stable (non-vulnerable) version should be upgraded.
5	All server environment/infrastructure should be configured for least privileged access, at all layers. [Servers, files/folders, network devices etc. should not be accessible to all. It should be accessible to authorized persons/services only with very minimal required privileges only]
6	Effectively monitor system for any changes or intrusion. [Effective monitoring of servers/network devices etc. is necessary for timely detection of any intrusion or suspicious attempts. This helps in prevention of attacks by stepping-up security infrastructure at all/required layers.]
7	Configure system logs on server [e.g. :Web-Access logs, Application Logs, Security Logs etc.]
8	Incorporate proper security advisories across all layers of infrastructure and servers.
9	Ensure proper backups of system/server/devices content/logs on a segregated server (preferable on disconnected server or storage devices)
10	Whenever any suspicious/intrusion incident is detected : • Block the site for public access • Report incident to Incident handling agency • DO NOT CHANGE ARTIFACTS