B.7.4 Data Security

Rajya Sabha website is hosted at NIC data Centre and is being developed and managed by a team of Engineers of NIC. NIC has taken every precaution to secure information on Rajya Sabha website.

The Rajya Sabha website is placed in protected zone with implementation of firewalls and IDS (Intrusion Detection System) and high availability solution. All the static contents of the website are stored in the NIC Data Centre at CGO Complex. However, the Dynamic contents (data base applications) are stored in the servers installed in Parliament House Complex. The IPS (intrusion prevention System) and IDS (Intrusion Detection System) are in place in the Parliament network.

Before the launch of the Rajya Sabha website, NIC has done the simulated penetration testing. Also penetration testing has been done after the launch of the website.

Application Security Audit: A large number of web enabled applications are in use in the Rajya Sabha website for displaying the information dynamically as per the users' requests. All the applications have been security audited for the known application level vulnerabilities and all the application security vulnerabilities have been addressed before the launch of the website.

Server Audit: The Applications and database servers hosting the Rajya Sabha applications and Databases have been security audited. The hardening of the server has been done as per the guidelines given by the NIC Cyber security division. The access to the server is restricted both physically and through the network as far as possible. The Logs are being maintained for authorized physical access to Rajya Sabha servers. The servers have been placed behind the Application firewall in order to make them hidden to the outside public.

All the development work is done on separate development environment and well tested on staging server before updating it on the production server. The Rajya Sabha website contents on the NIC Data centre servers are uploaded using secured SSH and VPN through a single point.

The contents are first checked on the development server before publishing on the production server. All contents of the web pages are checked for intentional or unintentional malicious content before final upload of the same on the web server.

Audit and Log of all activities referring to the operating system, access to the system and access to applications are maintained and archived. All rejected accesses and services are logged and listed in exception reports for further scrutiny.

All newly released system software patches, bug fixes and upgrades are deployed regularly and reviewed. The Antivirus has been deployed on the servers and is updated online.

Servers' passwords at NIC data center are changed at the interval of one month and are shared by two officers of NIC only. Servers at Parliament Complex are under direct control of TD (NIC) and Server Administrator and passwords are given to only authorized persons of NIC.