CIRCULAR

Department of Information Technology, Government of Goa has developed an online portal www.e-requestdoit.goa.gov.in, with an objective of carrying out registration of new website/request for carrying out website deployments in State Data Center electronically. Earlier the manual process followed was taking certain amount of time for hosting the application. Now the online application will eliminate the manual procedures while requesting for registration of new websites along with other website deployments thereby providing a single window via online mode.

All the Government Department/Corporations/ Autonomous Bodies/ Institutions etc. are requested to strictly submit their request for any website deployment at the State Data Centre through the above online portal. However in order to access the portal all the Government Department/Corporations/ Autonomous Bodies/ Institutions etc would have to initially fill the New User Login Request Form (enclosed to this circular) and submit it to this Department for further course of action. Manual submission of form is discontinued with immediate effect. Further, the Corporations/ Autonomous Bodies / Institutions etc. are also advised to refer the webserver security guidelines (second version) issued by this Department which are available on online portal at www.goa.gov.in.

This issues with approval of Government vide C.M U.O No. 10767/F dated 28th November, 2014.

Note: This circular is applicable to all the Departments/ Corporations/ Autonomous Bodies/ Institutions etc. Whose websites are presently hosted/running at the SDC of the department of IT or who may want to host in future.

(Nilesh B. Fal Dessai)
Director (IT)

To,

1. All Head of Departments/ Corporations/ Autonomous Bodies/ Institutions of Government of Goa.
2. Office Copy
3. State portal
4. Guard File

Phone Nos.: +91 (832) 2411505 / 2411509
Fax No.: +91 (832) 2411490
Dept of Information Technology
www.goa.gov.in
Application form for new users ONLY
This form is for getting user credentials from DoIT to access new web based online system to cater the requests of various Departments/corporations to host new website and daily website deployments on SDC web server.

The form should be completed and the scanned copy should be emailed to 'netdba1-dit.goa@nic.in'.

User Information

1) Name of the Department: ____________________________________________

2) Address: _________________________________________________________

3) Telephone Number (O)*: ___________________________________________

4) E-mail id: _______________________________________________________

Attach Department logo (if any) while forwarding the scanned copy via mail.

Security policy and declaration

☐ Username and Password is not transferrable and concerned department shall be soul owner of the username and password allocated to them. DoIT shall not be held

Department of Information Technology, Goa
responsible for any password sharing or any misinformation interpreted by using concern login credentials.

☐ The content uploaded shall be valid and department shall be fully responsible for the necessary content uploaded/updated/

☐ Information uploaded shall be inline and complied to the web server security guidelines issued by DoIT.

I hereby declare that above information is true to my best knowledge and I shall abide to security and policy mentioned as above.

Name and Signature of Competent Authority of the Department
With date and seal

[Table]

Name: ___________________________  Designation: ___________________________

Date: ___________________________  Signature: ___________________________

Stamp/ Seal:
WEBSERVER SECURITY AND WEBSITE DEPLOYMENT GUIDELINES
AT STATE DATA CENTRE

Version 2.0
Abbreviations

- DoIT/DOIT: Department of Information Technology, Goa
- GOI: Government of India
- GSDC/SDC: (Goa) State Data Center
- ICT: Information and Communication Technology
- DCO: Data Center Operator
- CISO: Chief Information Security Officer
- GBBN: Goa Broadband Network
- VPN: Virtual private network
Table of Contents

VISION & OBJECTIVES ............................................................................................................. 4

1. Introduction .......................................................................................................................... 5

2. Website Hosting .................................................................................................................... 5
   ☐ About the Service ............................................................................................................... 5
   ☐ Procedure for hosting new departmental website/application at SDC ............................. 6
   ☐ Procedure for updating content of the existing website at SDC ................................. 8
   ☐ Procedure for upgradation of website (technology) at SDC ........................................ 8
   ☐ Platforms available in SDC for hosting Websites is as follows .................................... 10

3. Roles & Responsibilities of Stakeholders ........................................................................ 11

4. Website Defacement/ Hacking ......................................................................................... 11
   ☐ Few tips to Prevent Hackers .............................................................................................. 12

5. How access will be given for data transmission? ............................................................ 14

6. Password Policy .................................................................................................................. 15

7. Checklist regarding Web Server Security Guidelines ...................................................... 16
VISION & OBJECTIVES

Vision

The Department of Information Technology (DoIT) has been created for evolving suitable IT program with the basic philosophy to realize the dream of taking the benefits of Information and Communication Technology (ICT) to the masses of Goa.

The brief objectives of the Department are as under:

1. To create world class IT Infrastructure and connectivity for e-Governance in the state of Goa.
2. To serve as the Enabler for Promotion of Information Technology Industry in Goa.
3. Promotion of E-Governance, E-education and streamlining of IT in Goa as a way of life.
4. Infrastructure Development and Capacity Building for promotion of IT.
5. Establishing Goa's USP as the Intelligent State through promotion of Information Technology in Trade, Commerce and Infotainment.
6. To conceptualize the concept of “Enabling and empowering the people,” for the spread of ICT to masses based on the e-Governance Roadmap prepared by this department.
1. Introduction

The Department of Information Technology (DoIT), Government of Goa has established a State Data Center (SDC) at Porvorim, with a vision to provide “Secure Infrastructure Services Centre for hosting and managing the e-Governance Applications of Government of Goa and its constituent Departments”.

Web Server Security Guidelines address the entire lifecycle of a website, web portal/application right from its conceptualization to design, development, maintenance and management. Apart from providing the information to every citizen usability, consistency and accessibility are taken into consideration while drafting the guidelines.

2. Website Hosting

◇ About the Service

As per the policy, all the Government departments are required to host their Websites/Portals/Applications at State Data Center.

The concerned departments may deploy their websites using existing infrastructure available at SDC in terms of servers, system software etc. In case of co-hosting services, where concerned department hosts their server and application in SDC, it may be noted that these servers are Owned and Managed by the respective departments only; DoIT is only providing infrastructure services i.e. Electric power, Cooling, Network infrastructure and Non IT support services.

To avoid any delay and cost on account of procurement of additional hardware/software, the departments are advised to develop their websites/applications/portal in a manner as per the website guidelines of this Department

In case departments are highlighted without having their own website; they can upload their requirements/data on www.goa.gov.in portal in concerned with their departments section.
The SDC provide the facility of staging infrastructure in order to facilitate the testing of the new websites as well as their enhanced or revised versions content prior to publishing on the internet / production web server.

Procedure for hosting new departmental website/application at SDC

1. For this purpose the departments would have to use the online portal to request for hosting of new departmental website at State Data Center. The portal can be accessed using http://www.e-requestdoit.goa.gov.in/

2. On accessing the portal, user is required to login by using appropriate credentials provided by DoIT after submitting the “New User Login Request” form. For new user registration, you may download the form available on login page of http://www.e-requestdoit.goa.gov.in/ and submit the same to DoIT or email the scanned copy to balaji.naik@nic.in in order to get user credentials (username & password).

3. The concerned department needs to ensure that the application code developed by the vendor is tested before registration of website.
4. Website registration form should duly be filled by login from the respective departmental account prior to hosting.

5. A clearance certificate (on letter head) indicating that the application is safe and secure to be hosted on staging server at SDC needs to be uploaded in .pdf or .jpg format along with the Website registration form.

6. Once the Website registration form is submitted, form will be reviewed by CISO & the status of the same will be indicated at the user’s side. If approved, DCO (in SDC) will plan and schedule the deployment date and time and will notify to the user in the portal itself.

7. Deployment of application on staging server will be done in SDC in presence of website vendor and DoIT personnel.

8. The website vendor will visit the State Data Center as per schedule along with the set of media to be used for deployment of websites on the staging server at SDC.

9. Provision of any additional IT Infrastructure (if required based on feedback of DCO), DoIT will not provide any additional infrastructure and the concerned department will borne the cost.

10. Once the application is successfully hosted on staging server, the same needs to be security audited, without which the website will not be migrated onto production environment. During this period a temporary domain name will be given for hosting the website for the period of one month before which the necessary website audit needs to be completed and vulnerabilities (if any) needs to be identified and cleared. If for any reason, the audit activity is not completed within the stipulated time period the domain name will be withdrawn and the respective website will be discarded.

11. On completion of audit and clearance of vulnerabilities if any, scanned copy of audit certificate along with the report of the cleared vulnerabilities needs to submitted to DoIT or mail to CISO on netdbal-dit@nic.in (once received DOIT shall upload the same in the portal). Website will be hosted in the production environment of SDC as per the domain name indicated by

DEPARTMENT OF INFORMATION TECHNOLOGY | Version 2.0
the concerned Department in their application form in presence of website vendor and DoIT personnel.

- **Procedure for updating content of the existing website at SDC**

  This procedure indicates the steps that need to be followed for updating contents of existing website at SDC.

  a) Concerned department needs to request for an appointment in order to schedule the deployment process by logging into the online portal [http://www.e-requestdoit.goa.gov.in/](http://www.e-requestdoit.goa.gov.in/) regarding updation of contents.

  b) This request will be handled by DCO (in SDC) to carry out the deployment process.

  c) DCO (in SDC) will plan and schedule the deployment date and time and will notify to the user in the portal itself.

  d) The website vendor will visit DoIT as per the schedule indicated in the portal along with the set of media to be used for updating the contents of the website.

  e) The website vendor needs to upload their changes/data on the FTP of DoIT server before deployment at SDC. Further, deployment of the same will be carried out in presence of website vendor and DoIT official.

  f) During the deployment process, SDC team won’t be responsible for any CSS/Design or coding/database issues taking place during the deployment.

  g) Deployment process will be carried out in the presence of website vendor and DoIT officials.

- **Procedure for up-gradation of website (technology) at SDC**

  The procedure that DoIT, Goa follows for up-gradation of website (technology) at SDC from various departments of Government of Goa.

  a) The concerned website vendor needs to ensure that website hosted support the latest trends/technologies in market. Whenever such new
upgrades/technology is available, the same needs to be tested on staging server at SDC, before moving it on production.

b) DoIT will upgrade and maintain the latest technologies available in market of its web servers available in SDC. Installation of latest technology will be carried out only after passing stability and security checks on staging server, then production line.

c) DoIT shall have full right to upgrade any web server component/web services related web server software to keep web server updated to latest technological trends. Prior notice of 8 days shall be given to vendors/departments for minor changes and 15 days in case of major changes on the web server.

d) Clearance certificate is then submitted to DoIT officials indicating that the website is safe and secure to upgrade on production server at SDC.

e) Up-gradation process is carried out on production server by SDC in presence of website vendor and DoIT officials.

f) Website vendors / concerned department are totally responsible for upgradation of their concerned website.

g) Any financial implication pertaining to up-gradation of website will be borne by the concerned department.

h) If any major up-gradation of technology needs to be upgraded in the concerned website, the vendors should discuss the same with the DOIT officials.

Note:
For hosting any new websites at SDC, the concerned department needs to develop their website as per the websites development guidelines of DoIT which may be referred on https://www.goa.gov.in/pdf/Empanelment%20for%20Website%20Development%20and%20Maintenance-%20Circular.pdf
 Platforms available in SDC for hosting Websites is as follows

**A. Linux Webserver (Staging) & (Production)**

**Software Installed**
- **Operating System**: Red Hat Enterprise Linux 6 Update 5 (64 Bit)
- **Postgresql**: 8.4.18-1 (64Bit)
- **MySql**: 5.6.15
- **PHP**: 5.5.7-1
- **PhpMyAdmin**: 3.5.8.2-1
- **Apache Server**: 2.2.15
- **ISPCConfig**: 3.0.5

**B. Windows Webserver (Staging) & (Production)**

**Software Installed**
- **Operating System**: Windows 2012 Server Standard Edition (64 Bit)
- **IIS**: 8.0 (64 Bit)
- **SQL Server**: 2008 R2
- **MySQL**: 5.6.15
- **PHP**: 5.3.28
- **PhpMyAdmin**: 4.1.0
- **Dot Net Frameworks**: 2.0, 3.5, 4.0, 4.5

- Default Application Pool set to use .Net framework 2.0 & allow 32-Bit Application
3. Roles & Responsibilities of Stakeholders

A. Role of DoIT

➢ To ensure the connectivity of the State Data Center with the State Government Departments through GBBN.
➢ To provide hosting space in State Data Center.
➢ Management of web server.
➢ Monitoring system integrity, protection levels, and security-related events.
➢ Securing the web servers at the Network, Operating System, and Database level.

B. Role of Website Vendors / Concerned Department

➢ Website vendors / concerned department are totally responsible for the entire web-site/application management starting from coding/database till deployment of the concerned web-site.
➢ DoIT has its FTP server and whenever any deployment/updates need to be carried out, the concerned vendor needs to upload their changes/data on the FTP server of DoIT.
➢ If any major changes/improvements need to be done in the concerned website the vendors should discuss the same with the DOIT officials.
➢ Concerned vendor should take their website backup on regular time intervals from SDC team.
➢ Update website and its content regularly according to the upgrades of web server component/environment.
➢ Website vendors / concerned department are responsible for upgradation/maintenance of their concerned website.
➢ Any financial implication pertaining to upgradation or updation of website, will be borne by the concerned department,
➢ Vendors will be responsible for security at application level.

4. Website Defacement/ Hacking

Website defacement is an attack on a website that changes the visual appearance of the site or a webpage. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own. However, if despite the security measures in place, such an eventuality occurs, and if the website has been defaced, the site will be immediately blocked by the SDC. Concerned website development vendor must be available in SDC during such crisis and efforts should be made to restore the original site in the shortest
possible time. The complete details of the website development vendor must be submitted in the DoIT.
Regular back-ups of the website data must be taken by the website vendor to enable a fast recovery and uninterrupted availability of the information in view of any data corruption.

The Vulnerabilities which are largely exploited for the defacements and which needs to be taken care in the web application by the concerned vendor/department:

- Microsoft SharePoint Page Content Vulnerability (CVE-2014-2816)
- Cross-site scripting (XSS) vulnerabilities in Microsoft SharePoint Server (CVE-2013-3180, CVE-2013-3179)
- Security Bypass and file upload Vulnerability in Joomla! (CVE-2013-5576)
- SQL injection vulnerability in the JExtensions JF Poll component before 1.1 for Joomla! (CVE-2013-5101)
- SQL injection Vulnerability in Joomla! (CVE-2013-3056)
- Multiple CSRF vulnerabilities in XCloner Wordpress plugin (CVE-2014-2579)
- File Upload vulnerability in the Tribulant Slideshow Gallery plugin for Wordpress (CVE-2014-5460)
- CSRF vulnerability in the MailPoet newspapers for Wordpress (CVE-2014-3907)
- Remote code execution vulnerability in the File gallery Plugin for Wordpress (CVE-2014-2558)
- Information disclosure vulnerability in the secure pages module for Drupal (CVE-2013-4595)
- Security Bypass vulnerability in Drupal (CVE-2013-4379)

- Few tips to Prevent Hackers
  a) Use Strong Passwords
  Longer passwords are more secure; the number of possible combinations grows exponentially with every extra character added. Hackers employ a technique called “dictionary attack” where they repeatedly try username and password combinations by running through hundreds of common words, phrases, numbers and combination them till they get lucky. It’s important to use random strings like “j@m13s(l)" instead of perhaps “jamie123"
b) Update Security Patches

Website vendor along with the system administrator should check that all the latest security patches for various aspects of the service are properly installed. Word Press and Joomla are the most popular Content Management Systems. Updates and patches are regularly released, so we need to keep an eye out for all plug-ins/core files.

c) Don’t use Generic Usernames

Using common words for usernames such as “admin”, “administrator” or “Site Owner” can cause many implications because it makes the job of the hacker’s a lot easier.

d) Make sure files are using the correct CHMOD Permissions

CHMOD file permissions assign a specific value to every file/folder on the server, which allows different levels of access.

CHMOD Permission range from 000 (No access) to 777 (Full access), Website vendor and System administrator must decide which files get what permissions.

e) Unsolicited Installation of Scripts

It can be dangerous to install third-party scripts and programs on the live website.

Steps to be followed in case of any defacement/hacking in future:

First, Even though the site is hacked, vendors need to come personally in DoIT and take backup of concerned website, and should start with the cleaning process.

Second, If any of the hacked areas include defaces or other visible clues (or even in our face writings), then concerned vendors should take screen shots of the same.

Third, vendors should provide necessary information along with the screenshots to DoIT officials.

Fourth, once the site is backed up and running clean, the vendors need to take the review whether an additional security can be put up for the concerned website.
5. **How access will be given for data transmission?**

For CMS based websites, administrator rights will be restricted from public access which can be accessed by domain administrators and will be given ONLY through Virtual Private Network (VPN). DoIT will provide VPN access to the concerned department as and when required ON REQUEST for updation of websites. This will allow concerned department to establish secure connections and thus can access and update their concerned website. However, DoIT may also opt for intranet access to respective folder wherein the website vendor/department shall be provided credentials for respective websites for folder for updation of content via intranet through concerned department and may not go ahead with VPN access. Final Decision of access shall be taken by DoIT.

✓ **Virtual private network**

Virtual Private Network (VPN) establishes a "secure tunnel" on the network and makes use of the Internet's infrastructure to move secure data to and from the organization network.

For security, VPN provides strong encryption, enables authenticated access to the Network from external and untrusted environments.
✓ Password Policy

a) Password Policy: Overview
passwords are an important aspect of computer security. A poorly chosen
password may result in unauthorized access and/or exploitation of
resources. All users from the department, including vendors with access
to system, are responsible for taking the appropriate steps, as outlined
below, to select and secure their passwords.

b) Password Policy: Purpose
The purpose of this policy is to establish a standard for creation of strong
passwords, the protection of those passwords, and the frequency of
change.

c) Password Policy: Scope
The scope of this policy includes all personnel who are responsible to
access any system that resides at any department’s facility, has access to
the network, or stores any non-public information.

d) Password Policy: Policy

✓ General
➤ All system-level passwords (e.g., root, enable, Windows
Administrator, application administration accounts, etc.)
must be changed on at least a quarterly basis.
➤ All user-level passwords (e.g., email, web, desktop computer,
web server etc.) must be changed at least every two months.
➤ User accounts that have system-level privileges granted
through group memberships or programs such as "sudo"
must have a unique password from all other accounts held
by that user.
➤ All user-level and system-level passwords must conform to
the guidelines described below.
e) **Password Policy: Guidelines**

- **Password Protection Standards**
  - Always use different passwords for each account from other outside access.
  - Do not share any passwords with anyone, including people who are working within the organization and on the same project.
  - All passwords are to be treated as sensitive, confidential information.
  - Passwords should never be written down or stored on-line without encryption.
  - Do not reveal a password in email, chat, or other electronic communication.
  - Do not speak about a password in front of others.
  - Always decline the use of the "Remember Password" feature of applications.

10. **Checklist regarding Web Server Security Guidelines**

<table>
<thead>
<tr>
<th>Hosting center(Websites/portals/web applications)</th>
<th>DoIT</th>
<th>Website Vendors</th>
<th>Concerned Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment process done by</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Server Login access</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>Testing on Staging server/Production Server</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Request Approval is given by</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Ready infrastructure for hosting the web application/website is provided by</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>To ensure the connectivity through GBBN</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Maintenance of a web server/systems in a secure manner/ Monitoring System</td>
<td>✓</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Concerned web-site management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Database/Coding changes</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Up gradation/maintenance of their concerned website</td>
<td>×</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Website backup on regular time intervals</td>
<td>✓</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Task</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Configuring additional security controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patching and updating the host OS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Identification of vulnerabilities &amp; resolving audit queries</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>File permission modes</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>Up gradation of new technology</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Deployment of web application packages</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>VPN access/Remote access</td>
<td>✓</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Financial implication pertaining to upgradation or updation of website</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
END