

Application/Website hosting and VPN Request Form (To be filled by Department)					
Requesting Department Name			Date of Request	__/__/20__	
Project Name					
Address					
Office contact no.					
Requester's Name			Requester's Email - ID		
Requester's Contact No					
Application Name					
Port no required for access the application		Tcp and udp	Yes <input type="checkbox"/> No <input type="checkbox"/>	Requirement of Public IP	Yes <input type="checkbox"/> No <input type="checkbox"/>
Application usage by internet user	Yes <input type="checkbox"/> No <input type="checkbox"/>				
Intranet	Yes <input type="checkbox"/> No <input type="checkbox"/>				
DBMS/RDBMS specify	1. 2. 3.				
Server Configuration Details	RAM	GB	Initial size of the database to be installed on staging server	____MB	
	Storage	GB			
	No. of CPU	Nos			
Type of Web Server			Web Server (Version)		
Any other third party software used for development of the application/freeware			1		
			2		
			3		
			4		
			5		
Proposed URL for application					
Name of the agency/person who developed the application/website					
Contact details of the developer			Email ID of the developer		
Nature of website/application (Static/Dynamic)	Yes <input type="checkbox"/> No <input type="checkbox"/>				
Time period for hosting the application/website on staging server(days/weeks)	60 Days Only				
Application usage by end user is on Intranet (Tick the required option)	Access through the PC installed at SDC			Yes <input type="checkbox"/> No <input type="checkbox"/>	
	VPN Provided by SDC (Only from GBBN Network)			Yes <input type="checkbox"/> No <input type="checkbox"/>	
Static IP Details of the Desktop/Laptop from where	IP :				

VPN will be accessed		
Purpose of hosting the application on staging server (Tick/describe wherever required)		
To conduct security audit	Yes <input type="checkbox"/>	No <input type="checkbox"/>
To test its functionality on the staging server and later deploy on production server	Yes <input type="checkbox"/>	No <input type="checkbox"/>
HOD Name and Signature Seal of the Department/Organization:	Date	

---

Note – Once the website/application is shifted from the staging server to production server the department should apply SSL certification to the website/application within 8 days failing which the DCO shall be free to remove the application from the production server.

In case VPN connection is required, department has to sign the letter of undertaking and submit the same.

**Letter Of Undertaking**

The authorized person of the application developer/vendor shall access the application/website through the VPN account provided to them by the DCO on the following terms and condition:

- The user shall be responsible for the safety of VPN account.
- GOA SDC/DCO/SDA is neither responsible nor accountable for any kind of misuse of VPN account or data of the application/website.
- The VPN account will be used only to access the authorized servers/ resources as per the access given by the DCO.
- Any security threats (Like Virus Attack, Denial of Service Attack, Intrusion, Data Theft, data loss and Hacking etc.) due to Remote/Ports access or any changes in the website & Services/application/server, user or user department will be solely responsible and user or user department will re-audit the website & services/application as per standards. This is also to state that the user or user department is having the remote access of the website/application/server and relevant services, hence DCO should be exempted from SLA compliance for the respective servers.
- Any security audit certificate will be valid till no additional changes in the dynamic content carried out or one year from the date of issue whichever is earlier.
- User shall not indulge in any unauthorized activity or attempt to gain unauthorized access to other servers or resources in SDC.
- The user should ensure that the system used for the VPN service shall be free from virus and should have only authorized software.
- User shall be responsible for the contents / data transfer to the servers through VPN connection. GOA SDC/DCO/SDA is not responsible for the contents that are being accessed / transferred by the user.
- If User requires root/admin password/privilege, internet access & unauthorized/vulnerable port access in the servers then user has to give the proper justification for the same and GOA SDC/DCO/SDA will not be held responsible/accountable for the said server or any kind of security incidents.
- If the website/application is security audited in any other environment apart from Goa State Data Center, then the responsibility of any security threats/incident, cyber-attack & cyber terrorism like Virus Attack, Denial of Service Attack, Intrusion, Data Theft, data loss, Hacking etc. would be of the concerned user department. In such scenario, GOA SDC/DCO/SDA will not be held responsible/accountable for any kind of security incidents and should be exempted from SLA breach or non-compliance.
- After hosting the website/application in production environment at Goa SDC, the respective department will re-audit the website/application within 30 days. In case, if the website/application is not security re-audited within the mentioned timelines, then same will be removed from the Goa SDC production environment.

We have gone through all the terms and conditions mentioned above and confirm that we shall be liable and responsible for any violations of terms and conditions mentioned above.

---

Duration For VPN Access: ( for maximum 180 days)

From: Date.....Time.....

To: Date .....Time.....

HOD/Nodal Officer Signature & Seal of the Department/Organization:

Name of the HOD/Nodal Officer .....

Name of the Department .....

Contact Number: .....

Date: .....

Note –This document is subject to review in accordance with the best IT practices followed in the industry and in order to comply with this, user departments/vendors are requested to submit their requirements at a period of maximum six months only.

---

Note – Once the website/application is shifted from the staging server to production server the department should apply SSL certification to the website/application within 8 days failing which the DCO shall be free to remove the application from the production server.

After completion of maximum staging duration i.e. 60 days, DCO will remove the website/application from Goa State Data Center Staging Environment which cannot be restorable.

Also in case the space provide on the staging sever at any times for hosting the website / application is not utilized within 15 days from the date of creation of URL or VM, the same shall be deleted after 15 days.