

Application/Website hosting and VPN/VM Request Form (To be filled by Department)

Requesting Department Name		Request Date & Time	
Address			
Requester's Name		Requester's Email - ID	
Requester's Contact No		Project Name	
Office Contact No.			
Application/Website details:			
Application Name			
Destination IP Address		Source IP Address	
Application Port no		Tcp/udp	Requirement of Public IP (Yes/No)
Application usage by internet user			Internet services in Server (Yes/No)
Required duration for internet in server			
Business Justification for Internet Requirement in Server			
Intranet (Yes/No)			
Access Required to URL's			
OS of application (Version)	Windows Server 2012 Tick () Red hat Linux 7 Tick () CentOS Linux Tick ()	DBMS/RDBMS (Name and Version)	
Server Configuration Details	RAM Storage CPU	Remarks	
Type of Web Server		Web Server (Version)	

Note - 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.

Any other third party software used for development of the application	1
2	3
4	5
Proposed URL for application	
Name of the agency/person who developed the application/website	
Contact details of the department	
Email ID of the developer	
Usage of the application/Website	
Nature of website/application (Static/Dynamic)	
Initial size(in MB) of the database to be installed on staging server	
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)	1. Access through the PC installed at SDC
	2. VPN Provided by SDC (Only from GBBN Network)
	3. Required ports for VPN Users
	4. Server IP Address from VPN
Static IP Details of the Desktop/Laptop from where VPN will be accessed	
In case of option 1, the undertaking is as follows:	
<input checked="" type="checkbox"/> The authorized person of the application developer/vendor shall visit NOC of SDC and shall accesses the application/website through a PC Installed byDCO	
In case of option 2, the undertaking is as follows:	

Note - 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.

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 password.
- By not doing so the account may be compromised by hackers and the hacker can misuse the same account. GSDC is neither responsible nor accountable for any such misuse of the compromised VPN account and the data of the application/website.
- The VPN account shall be used only to accessing authorized servers/ resources as per the access given by the DCO.
- Any security threats due to remote/VPN access or any changes in the website & services/application, user or user department will be responsible and user or user department will re-audit the website & services/application at every year. This is also to state that the user or user department is having the remote access of the website/application and relevant services, hence DCO may be exempted from SLA compliance for the respective servers.
- 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 uploaded to the servers through VPN connection. GSDC is not responsible for the contents that are being accessed / upload by the user.

Details of the security audit conducted by CERT-IN empaneled.	
---	--

Enclosed (Yes/No)	
-------------------	--

Purpose of hosting the application on staging server (Tick/describe wherever required)
--

1. To conduct security audit	
------------------------------	--

2. To test its functionality on the staging server and later deploy on production server	
--	--

3. Any other	
--------------	--

Requester's Signature		Date	
-----------------------	--	------	--

HOD Name and Signature		Date	
------------------------	--	------	--

Seal of the Department/Organization:

Note - 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.

Application/Website hosting and VPN Request Form (To be filled by ITG and DCO)

Approval by DCO Project Manager

Status of approval (Yes/No)			
Name of the approving person		Designation	
Date		Signature	

Approval by Info Tech Corporation Goa Ltd.

Status of approval (Yes/No)			
Name of the approving person		Designation	
Date		Signature	

Office of DCO

Call ID			
Assigned to (Name of the person)			
Designation		Date	
Public IP mapped (If required)			
Application URL (for testing)			
Application URL in production server			
Staging server test name			
IP Address			
Production Server host name			
IP Address			
Date of migrating the application to production			
Date of completion of the assignment			
Name of the person			
Date		Signature	
Status (Open/Closed)			
Remarks by DCO			
Details of the permissions given by DCO			
Item	IP Address	Ports	Remarks
Name of the person giving the access			
Signature		Date	
Intimation to the user (Yes/No)		Date of intimation	

Note - 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.

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 reaudit 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.

Details of Servers/Web/App for which VPN Service/Access will be required

Server Name & IP:

Name of the Website/Application:

Justification:

.....
.....

Duration For VPN Access: (for maximum 180 days)

From: DateTime.....

To: DateTime.....

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 - 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.