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

Requesting User Department's Name		Date of Request	
Full Address			
Project Name		Office contact no.	
Requester's Name		Requester's Contact No.	
Requester's Email ID (Nodal Officer's official Email ID only)			
Name of the agency/person who developed the Application/Website		Contact details of the developer	
		Email ID of the developer	
Application/Website Name			
Application/Website URL			
Request for	VPN ☐	VM Server ☐	
Port no required for access the Application/Website	RDP (3389) ☐ SSH (22) ☐ Any Other _____	TCP ☐ UDP ☐	Requirement of Public IP: Yes ☐ No ☐
DBMS/RDBMS (Name & Version)	1. 2.	Reqd. Operating System (Version):	1. Windows Server 2012 ☐ 2. Red Hat Linux 7 ☐ 3. CentOS Linux ☐
Server Configuration Details	RAM (in GB)	Type of Web Server	
	Storage (in GB)		
	CPU (in Nos.)	Web Server (Version)	
Any other third-party software used for development of the Application/Freeware		1.	
		2.	
		3.	
Proposed URL for Application/Website			
Nature of Application/Website		Static ☐ Dynamic ☐	
Static IP Details of Desktop/Laptop from where VPN will be accessed			

P.T.O.

Note: - This form needs to be submitted to ITG/CISO for approval, direct submission to DCO will not be considered.

Purpose of hosting the application/website on staging server	To conduct security audit	Yes ☐ No ☐
	To test its functionality on the staging server and later deploy on production server	Yes ☐ No ☐
Time Period for hosting the application/Website on Staging Server (if less than 60 days, please specify)	60 days (Max.)	
Application/Website use by end user is on Intranet (Tick the required option)	1. Access through PC installed at SDC	
	2. VPN provided by SDC	
	3. Server IP Address for VPN access	

Duration for VPN Access: (for maximum 60 days)

From	To
Date:	Date:
Time:	Time:

Letter of Undertaking

The authorized person (Nodal Officer) of User department shall access the application/website/server etc. through the VPN account provided to them by the DCO on the following terms and condition:

1. The VPN account will be allowed only to access to the authorized persons (Nodal Officer) of user department approved by competent authority.
2. GOA SDC/ DCO/ SDA is neither responsible nor accountable for any kind of misuse of VPN account or data/information of the application/ website.
3. License based Anti-virus must be installed/updated on remote clients and servers to prevent the spread of any malware/virus if either end is infected.
4. Internet access will be restricted in client VPN system.
5. User or user department will be responsible for 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/application/database/servers.
6. Split VPN should be avoided if the policy permits; i.e., users with remote access privileges must ensure that their organization-provided or personal device, which is remotely connected to the company's network, shall not be simultaneously connected to another network.
7. Users should also be sure not to violate any of the organization's policies, not to perform any activities that are illegal, and not to use the access for outside business interests while accessing the business network remotely.
8. User shall be responsible for the safety of VPN account & login credentials, by not doing so the account may be compromised by hackers and the hacker can misuse the same account. GOA SDC/DCO/SDA is not responsible for the contents that are being accessed/transferred by the user/user department.
9. Any unauthorized software should not be installed in the system from where VPN service will be used.
10. GOA SDC/DCO will only facilitate VPN over intranet. Under any circumstances VPN access to any Database will not be facilitated.
11. GOA SDC/DCO will not be responsible for any contents that are being accessed /uploaded to/from servers by the user/user department.
12. User shall not indulge in any unauthorized activity or attempt to gain unauthorized access to other servers or resources in SDC.
13. If User requires root/admin password/privilege, internet access & unauthorized/vulnerable port access in the servers then user has to give 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/violations.
14. Any User's request should be raised by respective user department through nodal officer's official mail id or letter only. If not yet nominated, then the same should be nominated by the concerned user department.

P.T.O.

Note: - This form needs to be submitted to ITG/CISO for approval, direct submission to DCO will not be considered.

15. GOA SDC/DCO will not be responsible for SLA compliance of specific servers permitted under VPN account.
16. If needed, User department are requested to submit their VPN requirement form at a maximum period of 60 days only.
17. Any VPN account will be disabled/deactivated/removed in case of inactivity for more than 20 days without any intimation to user/ user department.
18. GOA SDC/DCO will only provide intranet access for User department/vendor for the specified duration of time on request with proper justification/ approval.
19. The User department needs to take undertaking from the developer/developing agency of the website/application that they will be responsible for 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/application/ database/servers and forward the same to ITG/ DCO/DoIT.
20. 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.

We have gone through all the terms and conditions mentioned above in Letter of Undertaking and confirm that User Department/ Developer/Developing Agency/Vendor shall be liable and responsible for any violations of terms and conditions mentioned above.

Details of Developer/Developing Agency/Vendor			
Name of the Developer/Developing Agency/Vendor			
Designation		Date	
Seal & Signature of Authorized Signatory (Developer/Developing Agency/Vendor)			

Details of the security audit conducted by CERT-IN empaneled. Enclosed (Yes/No)		
Requester's Signature		Date:
HOD/Nodal Officer's Name & Signature		Date:
Seal of the Department/Organisation		

Approval of CISO, Info Tech Corporation Goa Ltd.			
Status of approval (Yes/No)		Date	
Name of the approving person			
Designation		Signature	
Seal of CISO/IT-Manager ITG			

Approval by DCO Project Manager			
Status of approval (Yes/No)			
Name of the approving person		Designation	
Date		Signature	

P.T.O.

Note: - This form needs to be submitted to ITG/CISO for approval, direct submission to DCO will not be considered.

Important Notes:

- ✓ 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.
- ✓ As per GOA SDC password policy, password will expire within 45 days. In case of any issue, kindly raise a request to GOA SDC Helpdesk from concern department's nodal officer's official email ID only.
- ✓ 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 60 days only.
- ✓ Once the website/application is security audited and shifted from 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/website from the production server, which cannot be restorable.
- ✓ In case the space provides on the staging sever at any time 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.
- ✓ VPN/VM request should come through concern department's nodal officer only as per DoIT circular.
- ✓ VPN/VM request form should be duly filled with all the necessary details with approvals.
- ✓ Incomplete/insufficient VPN/VM request form will not be considered.
- ✓ Please share the VPN credentials with concern department officials only & advise them to maintain the confidentiality.
- ✓ Please DO NOT reply on any mail which contains any kind of sensitive/confidential information.
- ✓ In case of difficulty in filling form, may contact to GOA SDC Helpdesk (0832-2226855) for any assistance.

For office use of DCO only			
Call ID			
Assigned to (Name of the person)			
Designation		Date	
Public IP mapped (If required)			
Application URL			
Server 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: - This form needs to be submitted to ITG/CISO for approval, direct submission to DCO will not be considered.