**Government of Gujarat**
**Science & Technology Department,**
**Circular No.: DTC/10/2012/2909/IT**
**Sachivalaya, Gandhinagar**
**Date:** 27 FEB 2013

**Read:**

1. This Department circular no. DTC/132009/2131/(269)/IT dated 01.03.2012 regarding information Guidelines for different content of Gujarat State Data Center
2. This Department Circular of even number dated 25.07.2012 regarding ISO 20000 and ISO 27001 Procedures & Processes to be adopted by all the users of the Gujarat State Data Center (GSDC)
3. GIL letter no. GIL/SDC/593-29/2012/SW/776885 dated 22.12.2012 regarding request to consider and decide about Infrastructure and Application hosting guidelines for SDC

**Preamble:**

This Department vide circular no. DTC/132009/2131/(269)/IT dated 01.03.2012 read at 1 above has issued an information Guidelines for different content of Gujarat State Data Center. Also this Department vide circular of even number dated 25.07.2012 have issued a ISO 20000 and ISO 27001 Procedures & Processes to be adopted by all the users of the Gujarat State Data Center (GSDC)

2. The Implementing Agency (i.e. GIL) for Gujarat State Data Center Project vide letter no. GIL/SDC/593-29/2012/SW/776885 dated 22.12.2012 read at 3 above have informed that DeitY, Government of India has prepared and sent the draft policy on Infrastructure and application hosting guideline for SDC. The same policy/ guideline document has been referred by DCO (i.e. M/s Wipro Infotech) and made necessary changes. Further GIL has received an email from Project Manager, Composite Team dated 18.12.2012 with final hosting policy/ guidelines which is being hosted at SDC.

**Circular:**

After careful consideration of the views and facts mentioned in the preamble Government of Gujarat has decided to implement the guidelines regarding Infrastructure and Application hosting is Gujarat State Data Center enclosed herewith.

2. This guideline is to be abided, complied and followed by all the users of Gujarat State Data Center. Also, all the users of GSDC have to ensure compliance with the IT Act 2000 and IT Amendment Act 2008. The violation of any part of this guideline will be dealt with the legal regulations as laid out by the Government of India in the IT Act 2000 and as per IT Amendment Act 2008.

3. State Composite team is responsible for implementation of this guidelines regarding Infrastructure and Application hosting is Gujarat State Data Center. Any breach of the said guidelines is observed, the Project Manager, Composite Team has to bring to the notice of State Implementing Agency GIL with the recommendation of action to be taken. The State

implementing agency (i.e GIL) is responsible for taking action for the above breaches on the recommendation of Composite team including rectification of the error, and due penalties if any as per the SLA /Contract Agreement. A fortnightly report is to be sent to the DST by GIL (Implementing Agency) & Composite Team on the action taken.

***By order and in the name of the Governor of Gujarat,***

**(Mukesh Ved)**
**Joint Secretary (IT)**
**Science & Technology Department**

**To,**

- The Secretary to the Hon'ble Governor, Raj Bhavan, Gandhinagar.
- The Principal Secretary to the Hon'ble Chief Minister, Government of Gujarat.
- Deputy Secretary to Hon'ble Chief Secretary, Government of Gujarat
- All Secretaries Department, Sachivalaya, Gandhinagar.
- The Chairman & Managing Director, Gujarat Informatics Ltd., Gandhinagar.
- The Secretary, Gujarat Vigilance Commission, Gandhinagar.
- The Secretary, Gujarat Public Service Commission, Ahmedabad.
- The Secretary, Gujarat Legislature Secretariat, Gandhinagar.
- The Registrar, Gujarat High Court, Ahmedabad.
- The Secretary, Gujarat Civil Services Tribunal, Gandhinagar.
- All Heads of Department.
- All Collectors.
- All D.D.Os.
- The Accountant General, (A&E), Gujarat, Post Box No.220, Rajkot.
- The Accountant General (A&E), Gujarat, Ahmedabad branch, Ahmedabad.
- The Accountant General (Audit)-1, Gujarat, M.S.Building, Ahmedabad.
- The Director of Accounts & Treasuries, Gandhinagar.
- All Treasury Officer.
- Ali Pay & Accounts Officers, Ahmedabad/Gandhinagar.
- Resident Audit Officer, Ahmedabad/Gandhinagar.
- TPA for GSDC (i.e. M/s Ernst & Young Pvt. Ltd.), Gujarat State Data Center Project
- DCO for GSDC (i.e M/s Wipro Infotech), Gujarat State Data Center Project
- M/s (n)Code Solution, (O & M Physical Infrastructure), Gujarat State Data Center Project
- Select file, S & T Department.

# GSDC Web Hosting Server/ Application Security User Guidelines v 4.0

## General Web Server Security Guidelines to be followed

1. Operating System configuration should be in accordance with approved InfoSec guidelines.

2. Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

3 . Services and applications that will not be used must be disabled where practical. Close all unused services and ports in the servers.

For eg: Unused FTP, File sharing ..etc In case FTP is required, Use SFTP instead of FTP.

4 . Uninstall all unwanted applications like FTP, SMTP, NNTP .etc. in the servers

5. Change Default SNMP string from public to a strong private string relating to the server so that it will be difficult to identity by an external party or hacker.

For eg: Public to Gujgnrsnmp_hyp01

6. All the Servers should sync time with common NTP Server and this should be configured and running in all servers.

7. Telnet session which transfer password in plain text should be disabled in all servers and only secure remote access like SSH or related tools should be used.

8. All the Microsoft critical patches/ security related patches to be applied on Servers.

9. Al the Web application related updates/patches should be tested by the department side in their test environment and based on the outcome of the patch on test setup.Then the updated application has be tested for application security auditing or OWASP top 10 based Web security auditing .Based on th audit results, necessary precautions/ patches to be taken before applying them to production .

10. Departmental users has to be follow the below steps before applying patch in their respective applications.

a. Prepare a test environment which is exact replica of production environment

b. The concerned patch applying team has to prepare a detailed plan of action with rollback plan also. The rollback plan is required in cases where the patch is deployed and application functionality gets affected.

c. The web application owner should check the plan of action and approve them to carry on the patch in the test environment first.

d. Apply the requested patch and check the application functionality along with OS functionality. Perform Web application security auditing on the new /modified and fix any gaps found in the audit.

e. Please make sure that application is working perfectly fine after applying the patch.

f. Please do a regression testing of all modules which are interconnected to the application module where patch is applied.

g. The application/Data owner should check that the patches are applied and application is running properly after the patch activity.

h. On successful completion of patch in the test environment, this can be deployed in the production.

i. The application / data owner should get a updated plan of action , in case there is any changes required as per patch in test environment.

j. The application owner should approve the new POA .

k. Based on the same, a Change request has to be raised for the patch upation by patch applying team to application owner.

l. On approval, the changes can be done in production and testing also to be completed.

m. In case the patch is not applied properly, based on the rollback plan, the changes has to be reverted.

n. This process has to be strictly followed on all Critical Web production servers running in GSDC.

## Web Application Security Controls

1. Verify the use of limited permission on shares especially of sensitive datafiles.

2. verify that vendor accounts are evaluated

3. Determine whether default settings and accounts have been changed or removed, if necessary.

4. Verify that there is a limited number of administrators

5. Verify the use of password policies in server .

6. Follow the CIS benchmark policies and make sure that the operating system and web server is compliant to security standards.

## Web Server Administration - INCIDENT MANAGEMENT AND RESPONSE

**Countermeasures and Actions to be taken prior to website security threats/attacks:**

1. Identify critical Web sites and services and their priority. Develop Business Continuity Plan.

2. Deploy appropriate Intrusion/DDoS Prevention System capable of detecting and mitigating DDoS attacks.

3. Ensure that Intrusion/DDoS Prevention System contain signatures to detect the attacks launched from common DDoS tools.

4. Maintain list of contacts of ISPs, vendors of network and security devices and contact them as appropriate

5. Understand your current environment, and have a baseline of the daily volume, type, and performance of network traffic.

6. Implement Egress and Ingress filtering at router level.

7. Implement a bogon block list at the network boundary.

8. Review the traffic patterns and logs of perimeter devices to detect anomalies in traffic, network level floods (TCP, UDP, SYN, etc) and application floods (HTTP GET)

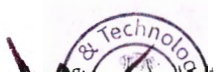
9. Maintain and regularly examine logs of webservers to detect malformed requests/traffic.

10. In case your SLA with ISP includes DDoS mitigation services instruct your staff about the requirements to be sent to ISP.

**Monitoring Web Servers to mitigate the risk level:**

1. Monitor the logs and Identify any type of attack such as flooding of particular types of packets/requests (TCP SYN, ICMP, HTTP GET etc) by examining logs of network and security devices such as Router / IPS / IDS / Firewall or DDoS attack Prevention Solutions

2. Identify the attack sources.



3. Block the attack sources at Router/Packet filtering device/DDoS prevention solutions

4. Disable the non essential ports/services

5. Preserve all logs indicating type of attack and attack sources.

6. In case of high volume of DDoS, consult your ISP to block attack sources and apply appropriate rate limiting strategies

7. Allocate traffic to unaffected available network paths, if possible, to continue the services

8. Consult your Business Continuity Plan for appropriate actions in case critical services are affected

**Web Application Security - PROVE COMPLIANCE AND PROTECT CONTINUOSLY**

1) Web Server logs should be analysed continuously to ensure that it is safe from any attacks and no unauthorized access is happening on stes.

2) Departments has to conduct Periodic web application security audit of the websites and implement necessary security recommendations to be implemented to strengthen web application security.

## Secure Coding Practices for Web site development by Departments

1. Define security requirements. Identify and document security requirements early in the development life cycle and make sure that subsequent development artifacts are evaluated for compliance with those requirements. When security requirements are not defined, the security of the resulting system cannot be effectively evaluated.

2. Model threats. Use threat modeling to anticipate the threats to which the software will be subjected. Threat modeling involves identifying key assets, decomposing the application, identifying and categorizing the threats to each asset or component, rating the threats based on a risk ranking, and then developing threat mitigation strategies that are implemented in designs, code, and test cases

3. Validate input. Validate input from all untrusted data sources. Proper input validation can eliminate the vast majority of software vulnerabilities. Be

suspicious of most external data sources, including command line arguments, network interfaces, environmental variables, and user controlled files .

4. Heed compiler warnings. Compile code using the highest warning level available for your compiler and eliminate warnings by modifying the code . Use static and dynamic analysis tools to detect and eliminate additional security flaws.

5. Architect and design for security policies. Create a software architecture and design your software to implement and enforce security policies. For example, if your system requires different privileges at different times, consider dividing the system into distinct intercommunicating subsystems, each with an appropriate privilege set.

6. Keep it simple. Keep the design as simple and small as possible . Complex designs increase the likelihood that errors will be made in their implementation, configuration, and use. Additionally, the effort required to achieve an appropriate level of assurance increases dramatically as security mechanisms become more complex.

7. Default deny. Base access decisions on permission rather than exclusion. This means that, by default, access is denied and the protection scheme identifies conditions under which access is permitted .

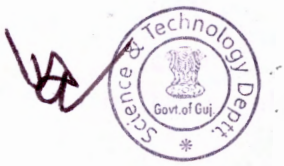
8. Adhere to the principle of least privilege. Every process should execute with the the least set of privileges necessary to complete the job. Any elevated permission should be held for a minimum time. This approach reduces the opportunities an attacker has to execute arbitrary code with elevated privileges .

9. Sanitize data sent to other systems. Sanitize all data passed to complex subsystems such as command shells, relational databases, and commercial off-the-shelf (COTS) components. Attackers may be able to invoke unused functionality in these components through the use of SQL, command, or other injection attacks. This is not necessarily an input validation problem because the complex subsystem being invoked does not understand the context in which the call is made. Because the calling process understands the context, it is responsible for sanitizing the data before invoking the subsystem.

10. Practice defense in depth. Manage risk with multiple defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense can prevent a security flaw from becoming an exploitable vulnerability and/or limit the consequences of a successful exploit. For example, combining secure programming techniques with secure runtime environments should reduce the likelihood that vulnerabilities remaining in the code at deployment time can be exploited in the operational environment .

11. Use effective quality assurance techniques. Good quality assurance techniques can be effective in identifying and eliminating vulnerabilities. Fuzz testing, penetration testing, and source code audits should all be incorporated as part of an effective quality assurance program. Independent security reviews can lead to more secure systems. External Third party auditor black box testing and website auditing bring an independent perspective; for example, in identifying and correcting invalid assumptions .

12. Adopt a secure coding standard. Develop and/or apply a secure coding standard for your target development language and platform.



## Secure Website management guidelines

1. Secure Coding practices for shared hosting websites: In shared hosting, multiple websites are hosted on the same physical server. Even if one website is completely secure, another insecure website hosted on the same server can help the hacker to compromise the secure website by attacking the insecure one. It is recommended to avoid shared hosting as much as possible, and in case shared hosting is the only available option, please make sure that hosted websites are checked for secure coding practices.

2. Harden your website's security: Hardening is the concept of securing a hosted environment that includes an operating system, web server, network and website, by removing the installation defaults. Kindly follow CIS benchmarks for the IIS 7.5 and Windows server 2008 for hardening the operating system and web server. Please take the following measures to add protection:

- Stop unwanted system services and remove unwanted programs.
- Configure the network firewall and intrusion prevention system (IPS) to protect your web server.
- Use the latest software versions and apply operating system patches to fix known security problems.
- Install an anti-virus program on the web server.
- Critical web applications can be protected by configuring web application firewall (WAF).

3. Back up content and log files to a secure location: Taking regular backup of your website's content is a good practice. However, back it up to a different location rather than storing backups within the website folder (webroot) itself. Doing this will make it available over the Internet, which actually makes life easier for malicious users than difficult! Similarly, logs offer sensitive information about your website and its underlying environment. So store the backup content and logs at a secure location. Search engines keep crawling every website over the Internet and display the indexed contents as search results. To protect files and folders from being crawled by the search engines, configure a robots.txt file in the webroot with rules to deny access to important directories by robots.

4. Encryption in storage and transit: Websites storing confidential data in a database or a file system should use strong encryption mechanism to store data. To protect the website data on transit, use SSL certificates to encrypt the communication channel between the visitor's Internet browser and the website.

Applying an SSL certificate to make the website work upon the HTTPS protocol doesn't provide any protection to the web application because HTTPS merely secures the communication channel so that an intruder can't read any data traveling between the visitor's Internet browser and the website. Similarly, the network firewall protects the server on which the website is hosted from external threats and doesn't provide any kind of security to the website.

5. Install host integrity checking software: Install host integrity checking software to track any unauthorized changes to the website contents. Such software sends an instant email notification on detecting any change in the website contents.

6. Do regular monitoring: Perform regular log monitoring to detect malicious activities and take informed decisions. Log monitoring and correlation tools can also be used to simplify the monitoring activity.

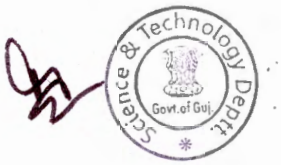
7. Secure the Webmaster's system: Webmasters should keep their systems updated with latest patches and antivirus software installed. Website management or modification from an insecure system can also lead to compromise of the website.

8. Use safe management methods: Follow safe methods to manage your website. For example, to protect the FTP username and password from being read during its transit over the Internet, use SFTP instead of FTP. Admin panel of website can be restricted to a particular IP address of the webmaster so that it is not available publicly. Also, change all management passwords on a regular basis.

9. Black box testing for dynamic websites by Third Party Auditor: For interactive websites having dynamic pages with input areas or database driven websites, it becomes important to get the website audited by experts. Specialized third party information security companies can be engaged to perform black box testing

against the website. Black box testing provides a detailed report on the vulnerabilities present in the web application along with the mitigation steps.

The above guidelines provide a broad framework of what we should do to secure the website. Remember that security is an on-going process and not a one-time activity, so webmasters and website owners need to continuously take proactive measures to keep their websites secure.



# Additional References

## Microsoft Windows 2008 Hardening Policy References

http://www1.ccny.cuny.edu/facultystaff/it/security/upload/CIS_Windows_Server_2008_Benchmark_v1-2-0.pdf

http://blog.tevora.com/enterprise-applications/10-steps-to-harden-windows-server-2008-2/

## Redhat Enterprise Linux / Centos Hardening Policy References

http://www.sans.org/score/checklists/linuxchecklist.pdf

http://www.nsa.gov/ia/_files/factsheets/rhel5-pamphlet-i731.pdf

http://people.redhat.com/sgrubb/files/hardening-rhel5.pdf

http://www.sysadminwiki.net/wiki/index.php?title=Red_Hat_Hardening_Guide

## IIS 7 Web Server Security Best Practices

http://learn.iis.net/page.aspx/88/configuring-security/

# Annexure I

## Responsibility Matrix for Application Hosting at the SDC

Each activity shall have the involvement of multiple stakeholders. However, ownership of the same would differ and the roles of participating stakeholders shall be different, as defined below:

A – Advice (Advisory / Monitoring Role)
The Advisory role for any entity is such where the primary responsibility to execute the activity lies with someone else, and the advising entity is required to provide inputs and advice, whenever referred to by the primary stakeholder
E – Execute (Primary ownership)
Any entity responsible for executing any activity shall be the primary stakeholder for the same, and it is the said entity's responsibility to liaison with other stakeholders for coordination and inputs / advice for the execution & successful closure of the activity.
C – Coordinate (Performing activities as directed / discussed)
The coordinating entity shall assist the primary stakeholder(s) (i.e., the activity executing entity) in successful execution of the tagged activity including performing various tasks for the completion as deemed required for the activity.

| S No. | Activity | Stakeholder | | | |
|---|---|---|---|---|---|
| | | User Department / Application Developer | DCO | State and Composite Team | NIC |
| 1 | Application Design, Development, Testing and Release | E | | | |
| 2 | Infrastructure finalization for Application | E | | A | |
| 3 | Finalization of Infrastructure requirements at SDC | E | C | E | |
| 4 | Application Hosting Testing in Staging Environment and Application Security Certification | E | C | C | |
| 5 | Application Migration to SDC Live Environment | E | C | C | |
| 6 | Application connectivity to SAN, and other common SDC Modules, and Web Connectivity (as | C | E | C | |

| S No. | Activity | Stakeholder | | | |
|---|---|---|---|---|---|
| | | User Department / Application Developer | DCO | State and Composite Team | NIC |
| | applicable) | | | | |
| 7 | Performance and Health Monitoring | C | E | A | |
| 8 | Error Reporting and Patch Management | E(Remote) | E (Helpdesk) | C | |
| 9 | Ensuring Power, cooling, available common SDC security,and Web & SWAN & SAN, connectivity, as applicable, to Application Servers | | E | | |
| 10 | Assessment of Application criticality for Disaster Recovery inclusion | E | C | E | |
| 11 | Application bringup at DR Site | E | | C | C |
| 12 | Application resumption at SDC Site | E | C | | |

# Annexure II

## Requirements for hosting applications/websites at the SDC

1. Users/Departments should fill up the respective **SAN & Service/ Server Co-location Form** as per their required purpose.
2. Any application/website must pass through Security Audit before getting hosted into GSDC.
3. CT will be responsible to validate the overall requirement as well as to verify findings from security audits conducted, make necessary recommendation to DST/GIL for approval.
4. Security Audit of any application/website hosted at GSDC has to be carried out at least once in 6 months and the cost for the same will be borne by the department owner.
5. Security Audit should be done by a Govt. Empanelled Agency (for the list of empanelled agencies visit (www.cert-in.org.in).Report of the same to be submitted to DST/GIL for verification and for track record.
6. Upon hosting application/website single point of contact from the department should be given specific server details like server name, IP, Port number, Rack number etc. for their record and transparency.
7. DST has the rights to reject any request for hosting/co-location/ Backup-Restore/installation/Upgradation/transfer or removal of equipment etc., on grounds of lack of feasibility or irregularities or non-compliance of GSDC ISO Policies & Regulations.
8. After above listed necessary actions the process forms should be submitted to DST/GIL for administrative approval followed by signing of SLA with GSDC.
9. After hosting is approved it will be mandatory to take approval from DST/GIL for any subsequent changes for additional services and "Change Management" form should be filled out by Department & approved by CT, DST/GIL.

# Gujarat State Data Centre

## SAN & Service/ Server Co-location Form

Date:

1. Name of the User / Department:

_____

_____

2. Name of the Project / Service:
(Enclose Description & Architecture on a separate sheet)

_____

_____

3. Category: Web [ ] Database [ ] Email [ ]

Server/Site Accessibility : GSWAN/Intranet [ ] Internet [ ]

Others if any specify._____

4. Server Specification (Not Applicable for Service Co-location)
   - Rack size of Server*:
   - Make & Model of Server:
   - Hardware configuration:

5. Software Environment
   - Operating System (with version):
   - Software & Tools:
   - In house developed applications:

| S. No. | Application | Operational since | Clustered / Non clustered | Transaction /Traffic (carried /expected) |
|---|---|---|---|---|
| 1. | | | | |
| 2. | | | | |
| 3. | | | | |

*** Server to be co-located should be Blade/ Rack Mountable only.**

Science & Technology Dept. Govt. of Guj

6. Clearance of Security Audit (including firewall rules) is enclosed [ ]

7. Disk Space required on SAN: Y/N [ ]

If Y, specify size _____ GB

8. Proposed Backup Policy & Procedure:

9. Remote Administration Procedure:

10. In case of E-mail /GIS service, clearance of concerned group is enclosed:

11. System Administrator / Project Coordinator's

Name & Address: _____

_____

Phone: (off)_____ (Res.)_____

(Email)_____

12. I have read and agree to comply and abide by all SDC Policies, rules & regulations.

Signature of HOD

Name of HOD: _____

Tel No / Intercom No. _____

Email:_____

***Please fill the form correctly and completely***

Science & Technology Deptt. Govt. of Guj.