ಕರ್ನಾಟಕ ಸರ್ಕಾರ

ಸಂಖ್ಯೆ: ಸಿಆಸುಇ 165 ಇಜಿಎಂ 2020

ಕರ್ನಾಟಕ ಸರ್ಕಾರ ಸಚಿವಾಲಯ,
ಬಹುಮಹಡಿಗಳ ಕಟ್ಟಡ,
ಬೆಂಗಳೂರು, ದಿನಾಂಕ:17ನೇ ಜುಲೈ 2020.

ಸುತ್ತೋಲೆ

ವಿಷಯ: Orders, Circulars, Policies on e-Governance subjects-reg

*****

ರಾಜ್ಯ ಸರ್ಕಾರದ ಅನೇಕ ಇಲಾಖೆಗಳು ತಮ್ಮ ಸಾಫ್ಟ್‌ವೇರ್ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಮತ್ತು ಡೇಟಾಬೇಸ್ ಗಳನ್ನು ಹೋಸ್ಟ್ ಮಾಡಲು ಸ್ಟೇಟ್ ಡೇಟಾ ಸೆಂಟರ್ ಬಳಸುತ್ತಿವೆ. ಕೋವಿಡ್ - 19 ಸನ್ನಿವೇಶದಿಂದಾಗಿ ಅನೇಕ ಇಲಾಖೆಗಳು ಅಪ್ಲಿಕೇಶನ್‌ಗಳನ್ನು ತ್ವರಿತವಾಗಿ ಅಭಿವೃದ್ಧಿಪಡಿಸಲು ಮತ್ತು ಹೋಸ್ಟ್ ಮಾಡಲು ಸ್ವೀಕೃತವಾಗುತ್ತಿದೆ. ಸ್ಟೇಟ್ ಡೇಟಾ ಸೆಂಟರ್‌ನಲ್ಲಿ ರಾಜ್ಯ ಸರ್ಕಾರದ ಬಹುಮುಖ್ಯವಾದ ಅನೇಕ ಅಪ್ಲಿಕೇಶನ್‌ಗಳು ಮತ್ತು ದತ್ತಾಂಶ ಇರುವುದರಿಂದ ಅಲ್ಲಿ ಹೋಸ್ಟ್ ಮಾಡಲು ಭದ್ರತಾ ಕಾರಣಗಳಿಗಾಗಿ ಎಲ್ಲರೂ ಹಲವಾರು ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಅನುಸರಿಸಬೇಕಾದ ಅನಿವಾರ್ಯತೆ ಇದೆ. ಆದ್ದರಿಂದ, ಅಂತಹ ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಮತ್ತು ದತ್ತಾಂಶ ರಕ್ಷಣಾ / ನಿರ್ವಹಣಾ ನೀತಿಯನ್ನು ಒಂದು ಡಾಕ್ಯುಮೆಂಟ್‌ನ ರೂಪದಲ್ಲಿ ತುರ್ತಾಗಿ ಪ್ರಕಟಿಸುವುದು ಅವಶ್ಯಕವಾಗಿರುತ್ತದೆ. "Processes, Procedures in Application Hosting and Best Practices in Data Protection" ದಾಖಲೆಯನ್ನು ಇ-ಆಡಳಿತ ಕೇಂದ್ರ ಸಿದ್ಧಪಡಿಸಿರುತ್ತದೆ. ಈ ಸುತ್ತೋಲೆಯೊಂದಿಗೆ ಲಗತ್ತಿಸಲಾದ ದಾಖಲೆಯನ್ವಯ ರಾಜ್ಯ ಸರ್ಕಾರದ ಎಲ್ಲಾ ಇಲಾಖೆಗಳು ಮಾರ್ಗಸೂಚಿಗಳನ್ನು ಮತ್ತು ದತ್ತಾಂಶ ರಕ್ಷಣಾ / ನಿರ್ವಹಣಾ ನೀತಿಯನ್ನು ಪಾಲಿಸಲು ಸೂಚಿಸಲಾಗಿದೆ.

17/7

(ರಾಜೀವ್ ಚಾವ್ಲಾ)
ಸರ್ಕಾರದ ಅಪರ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿ
ಸಿಬ್ಬಂದಿ ಮತ್ತು ಆಡಳಿತ ಸುಧಾರಣೆ ಇಲಾಖೆ
(ಇ-ಆಡಳಿತ)

ಇವರಿಗೆ:

1. ಸರ್ಕಾರದ ಎಲ್ಲಾ ಅಪರ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿ /ಪ್ರಧಾನ ಕಾರ್ಯದರ್ಶಿ / ಕಾರ್ಯದರ್ಶಿಯವರುಗಳಿಗೆ
2. ಎಲ್ಲಾ ಇಲಾಖಾ ಮುಖ್ಯಸ್ಥರುಗಳಿಗೆ- ಮುಖ್ಯ ಕಾರ್ಯನಿರ್ವಹಣಾಧಿಕಾರಿ, ಇ-ಆಡಳಿತ ಕೇಂದ್ರ ಇವರ ಮುಖಾಂತರ
3. ಮುಖ್ಯ ಕಾರ್ಯನಿರ್ವಹಣಾಧಿಕಾರಿ, ಇ-ಆಡಳಿತ ಕೇಂದ್ರ, ಬಹುಮಹಡಿಗಳ ಕಟ್ಟಡ, ಬೆಂಗಳೂರು.
4. ಸರ್ಕಾರದ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿಗಳ ಆಪ್ತ ಕಾರ್ಯದರ್ಶಿ, ವಿಧಾನ ಸೌಧ, ಬೆಂಗಳೂರು
5. ಸರ್ಕಾರದ ಅಪರ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿಗಳ ಆಪ್ತ ಕಾರ್ಯದರ್ಶಿ, ವಿಧಾನ ಸೌಧ, ಬೆಂಗಳೂರು
6. ಸರ್ಕಾರದ ಅಪರ ಮುಖ್ಯ ಕಾರ್ಯದರ್ಶಿ ಹಾಗೂ ಅಭಿವೃದ್ಧಿ ಆಯುಕ್ತರು, ವಿಧಾನ ಸೌಧ, ಬೆಂಗಳೂರು
7. ಇಲಾಖಾ ವೆಬ್ ಸೈಟ್‌ನಲ್ಲಿ ಪ್ರಕಟಿಸಲು
8. ಶಾಖಾ ರಕ್ಷಾ ಕಡತ

Government of Karnataka (GoK)

Processes, Procedures in Application Hosting and Best Practices in Data Protection v1.0

Table of Contents

1 Introduction

This document is a "Quick Start Guide" that describes the Processes, Procedures and Best Practices in Data Protection and Application Hosting to be followed by all departments under Government of Karnataka. This became urgent and important to be published as many departments wanted to develop and host applications on a fast mode because of the Covid-19 situation.

1.1 Audience

All departments under Government of Karnataka which want to develop and host IT applications can use this document to make sure the application and data is secure and complies with a) guidelines laid out by MeitY, Government of India, b) processes followed in KSDC environment and c) in accordance with the best practices.

1.2 Acknowledgements

This document is derived from various sources. Below is the list:

#	Details	Source
1	NDA	CeG internal document updated to suit the requirement
2	Data Protection Guidelines	Derived from Meity - Personal_Data_Protection_Bill, 2019 https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
3	Privacy Policy Template	CeG internal document updated to suit the requirement
4	Terms and Conditions Template	Derived from https://www.mygov.in/simple-page/terms-conditions/
5	Cloud Services Usage Guidelines	Derived from MeitY - Guidelines for Government Departments On Contractual Terms Related to Cloud Services
6	Checklist for Securing Application	Points 1-7 from Oracle Points 8-10 from Gartner

1.3 Document Control

#	Action	Name	Designation	Date
1	Drafted by	K.R.Chandrashekar	Senior Consultant, SeMT, Centre for eGovernance, Govt. of Karnataka	5th May 2020
2	Reviewed by	Belur Sudarshana	Advisor to CM on eGovernance, Govt. of Karnataka	6th May 2020
3	Reviewed by	Vipin Singh	CEO, Centre for eGovernance, Govt. of Karnataka	7th May 2020
4	Approved by	Rajeev Chawla	ACS, DPAR(e-Governance) Govt. of Karnataka	2nd July 2020

1.4 Hosting of IT applications by departments

Many departments are working with private companies in the area of application development and support. It is common for developers to exchange data on email, WhatsApp, etc., during development and testing. It is important that all the people who are working on the project sign Non-Disclosure Agreement (Please refer to Annexure 2.1 for NDA Template) and follow it in letter and spirit. The private companies and the departments should make sure that there are no exceptions. Non-compliance should be considered as a serious breach of contract.

After development and testing, the departments may choose to host/deploy the application on the cloud or at Karnataka State Data Centre (KSDC).

A Checklist for securing application is provided as Annexure 2.6.

The application should comply with the Data Protection Guidelines (Please refer to Annexure 2.2) and for a complete document please refer to Personal_Data_Protection_Bill, 2019 introduced in the Parliament.

The application must have Privacy Policy (Please refer to Annexure 2.3 for a Template) and Terms and Conditions (Please refer to Annexure 2.4 for a Template) and display in the website/application.

If the department chooses to deploy the application on public cloud, Government of India has provided guidelines to be followed (Please refer to Annexure 2.5).

If the department chooses to deploy the application at KSDC, the Core IT Infrastructure of the Government of Karnataka that provides Infrastructure as a Service to the line departments for hosting their applications, there are laid out processes that need to be followed in the DC environment.

1.5 Hosting of a departmental application at KSDC

Following are the steps to be followed:

1. Letter from the competent authority from the concerned department to ACS eGovernance.
2. Upon administrative approval by EGov Department, SDC team communicates a Requirement Form to the department (Please refer to Annexure 2.7).
3. Department fills and send the CeG Requirement gathering template to ksdc.helpdesk@karnataka.gov.in. Department should share dedicated DB admin contact, application contact and administrative contacts.
4. KSDC creates a request ticket and takes action to provision the infrastructure and handover to the department.
5. The application needs to comply with the following:

i. Application needs to be at least two-tier architecture, that is web and database on separate tiers. All DB servers should be in trust zone only.
ii. For Applications / tools which are not standard offerings of KSDC, it does not take any responsibility on installation, configuration and supporting these software
iii. Domain Name: Department has to confirm the domain name with the suffix as ".karnataka.gov.in".
iv. To host the application on the internet: As per the SDC security policy the application needs to be security audited by one of the CERT-In empaneled vendors: https://www.cert-in.org.in/PDF/Empanel_org.pdf and the department has to provide "safe-to-host" certificate.

6. Once the application gets "safe to host" certificate, SDC will do an internal testing before clearing the application.
7. Public IP will be provided only after SDC receives the safe to host certificate from the department.
8. Department should provide DB admin contact details, who should be a departmental government official. KSDC does not take responsibility of ownership of the database and its responsibility is limited to assistance in maintenance activities of Database like Indexing, backup and restore Database consistency check.
9. KSDC will not own any data and admin credentials for the department databases. Database maintenance support is available as on today only for MS SQL database.
10. For procurement of SSL certificates, there are no empaneled vendors with CeG for providing the SSL certificate and the SSL certificate is not supplied by CeG. Department has to directly procure the SSL certificate. On request CeG shall provide list of vendor email Ids for procuring SSL certificates.
11. Once the KSDC allocates the public IP, the application can be Go Live from KSDC.
12. **In case the application undergoes a version change, the department shall inform the data center and undertake a fresh security audit before implementing the change in production**.
13. Department shall adhere to and comply with all security related advisories issued by the Data Centre security teams from time to time.
14. Data center shall provide only generic system software and undertake patch management related to such a system software.
15. Data Centre provides data backups as per the backup policy of the department.
16. Department shall take steps to ensure that application specific software including application, system software, database, middleware, third party software components are patched regularly. It is understood that failure of the department to apply patches to its application and its components can expose its application to online threats including unauthorized access, manipulation and loss of departmental data.
17. Data Centre has implemented a IT Security Policy in compliance to Data Centre standards. It is monitored by NCIIPC, CERT IN and Security Operations Centre.

18. Data Centre carries out a periodic security audit through its Third Party Auditor (at least once a year). Department must take action to comply with the TPA observations on their applications.
19. Patch Management - Patching is a process to repair a vulnerability or a flaw that is identified after the release of an application or a software. Newly released patches can fix a bug or a security flaw, can help to enhance applications with new features, fix security vulnerabilities. It is important that patching is done in a timely manner.

Other Policies and Procedures

Department must ensure that the application hosted on KSDC/Cloud has the following:

1. Privacy Policy
2. Terms and Conditions
3. Nominate a Departmental Single Point of Contact (SPOC) for interacting with the Data Centre

1.6 Migration from Public Cloud to KSDC

The following steps may be followed:

1. From steps: 1 to 4 provided above in Section 1.5
2. KSDC provides a staging server
3. The application to be migrated should be hosted on a staging server on KSDC
4. From steps: 5 to 18 provided above in Section 1.5
5. Once public IP is given and SSL certificate is ready and the application is tested
   a. Migrate data from the cloud to KSDC
   b. After testing, traffic can be redirected to KSDC from public cloud
   c. Follow the laid out procedure to delete the data on public cloud and de-provision servers on public cloud

2 Annexures

2.1 Non-Disclosure Agreement Template

NON-DISCLOSURE UNDERTAKING

From: BANGALORE

…… Date:

……

……

To:

……

……

……

Dear Sir,

Sub: Letter of Undertaking regarding Non-Disclosure of Information

****

Parties

1. I, …… Son / daughter / wife of ……aged about…Years, presently residing at……submit as under in the above regard.

2. WHEREAS I am deployed by << >> to << >>, Govt. of Karnataka, Bangalore [hereinafter referred to as < >] for providing service as a ……

3. WHEREAS during the course of providing of my services as a……at << >>, I may handle or have access to information/data pertaining to << >>> and its stakeholders which is confidential information/data or sensitive personal information/data or proprietary information/data.

Confidential Information

4. For the purpose of this undertaking, "Information" / "confidential information/ proprietary information/data include the following

   a) All information/data such as personal health data and personally identifiable data or any other data of the citizens which I may have access to as part of my duties.
   b) All documents which are prepared or received by me whether in writing or electronic format.
   c) Process information, User IDs/ Passwords, OTPs, Reports, email communication, oral or written instructions.

This is an indicative list and << >> may notify any other information from time to time which shall be included in the scope of this undertaking.

Scope

5. I, hereby undertake and agree to comply with the following both during the tenure of my deployment and / or after cessation of the tenure of my deployment to << >>.
   (a) to keep confidential and not to divulge any/ or all such information described in para 4 (a) to (c) above which may come to my knowledge, either directly or indirectly.
   (b) not to engage in any capacity, in any venture which conflicts with / jeopardizes the interest of << >> or it stakeholders.
   (c) Make any audio / video or any electronic record of activities of operations.
   (d) Make any social media post with regard to activities of operations.
   (e) not to make, any public statement, in any media, on any matter/s relating to << >>>.
   (f) not to authorize any person or entity to divulge any information (both confidential and proprietary) or to any media on any matter/s relating to << >>>
   (g) use data or any information, facilities provided to me during the tenure of my deployment solely for the purpose of carrying out of the activities defined as part of responsibility assigned by << >>from time to time.
   (h) Immediately bring to the notice of << >>, any breach committed or noticed during the course of the deployment.

7. I, further undertake to comply with the following upon (i) cessation of my deployment to << >>, and (ii) receipt of instructions (in writing or oral) from << >> as the case may be.
   a) shall return all documents and all other records containing information (both confidential/proprietary) and all other materials and all copies thereof or in any way obtained by me during the tenure of my deployment.
   b) shall not retain copies, notes or abstracts of the foregoing whether in writing or stored or maintained in or by electronic, magnetic or other means of media or devices.

8. I undertake that << >> shall be entitled to disciplinary action in the event of any breach of the provisions of this undertaking in addition to all other remedies available to << >> at law or in equity.

9. The intellectual property or software code developed is the property of << >> and shall not be copied or used in part or full or in any form whatsoever.

10. Finally, I hereby state that this undertaking shall have effect from date of my deployment to << >>.

(Signature)
<<Name>>

2.2 Data Protection Best Practices

Sec 43A and Sec 72A of the Information Technology Act 2000 provide the right to compensation for improper disclosure of personal information. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 impose additional requirements relating to the collection and disclosure of sensitive personal data or information. The Supreme Court of India has recognized the right to privacy as a fundamental right under Article 21 of the Constitution.

Government of India has issued the Personal Data Protection Bill 2019 that will be India's first law on the protection of personal data. It proposes a broader law, applying to both manual and electronic records and create a Data Protection Authority of India. It deals with reasonable security practices and procedures relating to the collection and disclosure of sensitive personal data or information. It also prescribes fine and punishment for disclosure of information in breach of lawful contract.

Data Protection Features:

1. Any personal data that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005 or under any other law in force shall not be regarded as 'sensitive personal data or information' ("**SPDI**"). Further, SPDI may be disclosed to government authorities mandated under law to obtain information for the purpose of verification of identity or for prevention, detection, investigation without obtaining the consent of the 'provider of information'.
2. Personal data under the Indian laws and rules is termed "**personal information**". Personal information has been defined under the Rules as "any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person, including any inference drawn from such data for the purpose of profiling".
3. The processing of personal data must comply with seven principles for processing:
   (i) processing of personal data has to be fair and reasonable
   (ii) it should be for a specific purpose
   (iii) only personal data necessary for the purpose should be collected
   (iv) it should be lawful
   (v) adequate notice of the processing should be provided to the individual
   (vi) personal data processed should be complete, accurate and not mis-leading
   (vii) personal data can be stored only as long as reasonably necessary to satisfy the purpose for which it is processed.
4. The personal data of a child should be processed such that the rights and the best interests of the child are protected. Further, such processing can be done only after verifying the age of the child and obtaining consent from the parent or guardian. Entities which process the personal data of children, or provide services directed at children will be categorized as 'guardian' data and will be prohibited from profiling, tracking or processing the data such that it may cause significant harm to the child.
5. PDP would not apply to anonymized data or non-personal data. The Government can also exempt the processing of personal data of individuals not based in India by data processors in India where that processing is under a contract with a company incorporated outside India. Further, PDP identifies a number of exemptions including

processing of personal data for reasons such as security of state, law enforcement, during legal proceedings, for research and archiving purposes or where processing is by small entities.

6. PDP identifies financial data, data about caste, tribe, religious and political belief or affiliation as sensitive personal data. The list is as follows:
   (i) passwords
   (ii) financial information such as bank account or credit card or debit card or other payment instrument details
   (iii) physical, physiological and mental health condition
   (iv) sexual orientation
   (v) medical records and history
   (vi) biometric information
   (vii) any detail relating to the above items provided to a body corporate for providing services
   (viii) any of the information received under the above items by a body corporate for processing, that is stored or processed under lawful contract or otherwise
7. The key rules on collection are:
   (i) it is necessary to obtain consent of the provider of information prior to the collection. The provider of information must be given an option not to provide the requested sensitive personal data or information and to withdraw its consent by informing the body corporate in writing
   (ii) sensitive personal data or information can only be collected where necessary for a lawful purpose that is connected with a function or activity of the body corporate or any person on its behalf
   (iii) the body corporate should provide additional information to the provider of information (see below)
8. The body corporate must not keep sensitive personal data or information for longer than is required and ensuring it is kept secure or applying reasonable security practices and procedures which contain managerial, technical, operational and physical security control measures.
9. The body corporate and any person acting on its behalf are not allowed to publish any sensitive personal data or information.
10. Consent of the provider of information should be obtained in writing (which includes any mode of electronic communication) regarding the purpose of its usage and before further transfer or disclosure to any third party.
11. The body corporates are required to designate a grievance officer and appoint a data protection officer and publish the name and contact details on its website.
12. The grievance officer shall address any discrepancies or grievances of providers of information with respect to processing of information in a time-bound manner.
13. The body corporate who processes personal information should provide a privacy policy. This privacy policy should serve to protect the personal information and users should be able to review the policy on the website. The policy should be:
   (i) clear and accessible statements relating to its practices and policies
   (ii) the type of personal information or sensitive personal data or information that is being collected
   (iii) the purpose of collecting and using of such information
   (iv) the instances in which disclosure of such information may be made under the rules

(v) reasonable security practices and procedures required under the rules

14. A privacy policy is required even when no sensitive personal data or information is being processed to ensure transparency and accountability.
15. A body corporate collecting sensitive personal data or information should keep the provider of information informed about:
    (i) the fact that the information is being collected
    (ii) the purpose for doing the same
    (iii) the intended recipients
    (iv) the name and address of the agency collecting and retaining the information
16. The IT Act and Rules do not impose any conditions regarding the usage of sensitive personal data or information for direct marketing. However, where the information is collected prior consent must be obtained, including the purpose for which the information is being collected.
17. The provider of information has the right to review the information provided and withdraw consent that was previously provided. A body corporate cannot refuse such a request. Additionally, any discrepancies and inaccurate information can be corrected by the provider of information.
18. The Rules provide that reasonable security practices and procedures need to be maintained by each body corporate and has listed the International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" as one such standard.
19. Under the Rules, a body corporate handling and processing sensitive personal data is required to have its security practices and procedures certified and audited by an independent auditor who is approved by the central government at least once every year, or when there is a significant upgrade in its computer resource.
20. Certain types of cyber security incidents need to be mandatorily reported to the Indian Computer Emergency Response Team ("**CERT-In**") created under Section 70B of the IT Act. These incidents include:
    (i) compromise of critical systems or information
    (ii) targeted scanning or probing of critical networks and systems
    (iii) identity thefts, spoofing or phishing attacks
    (iv) unauthorized access of IT systems or data;
    (v) defacement of a website or intrusion into a website;
    (vi) malicious code attacks including attacks on servers
    (vii) Denial of Service or Distributed Denial of Service (DoS or DDoS) attacks.

2.3 Privacy Policy Template

When you use <Name of the application>, some personal information is collected from and about you. We are committed to protecting the security of this information and safeguarding your privacy. This privacy policy sets forth the details of the personal information collected, the manner in which it is collected, by whom as well as the purposes for which it is used. At registration you accepted the terms of this Privacy Policy and your use of the App signifies your continued acceptance thereof. This Privacy Policy may be revised from time to time and you will be notified of all such changes. In order to use the App, you will be required to consent to the terms of the Privacy Policy as revised from time to time.

1. DETAILS OF INFORMATION COLLECTED AND MANNER OF COLLECTION

a. When you register on < name of the application>, the following personal information is collected from you and stored securely on a server operated and managed by the Government (Server) – (i) < >; (ii) < >; (iii) < >; (iv) . The information may be used to identify you in all subsequent transactions and will be associated with any data or information uploaded to the Server.

b. In addition to the above information shared voluntarily by the user, the application also collects following information during use of the application: (i) < >; (ii) < >.

c. The department may also use data from other sources to help improve the services.

2. USE OF INFORMATION

a. The personal information collected from the user and information about the user collected from other sources shall be used for the purpose of providing services as per the scope of the application's services.

3. RETENTION

a. The personal information collected from the user shall be retained for as long as user account remains in existence and for such period thereafter as required under prevalent laws.

b. All personal information collected will be retained for a period of < > days from the date of collection after which, if it has not already been uploaded to the Server, will be purged from the App.

c. All personal information uploaded to the Server will be purged from the Server < > days after being uploaded unless the service requirement mandates retention of records for a longer duration or permanently.

c. Nothing set out herein shall apply to the anonymized, aggregated datasets generated by the data of users of the application or any reports, heat maps or other visualization created using such datasets. Nothing set out herein shall apply to reports.

4. DATA SECURITY

The application is equipped with standard security features to protect the confidentiality and security of your information. Data is encrypted in transit as well as at rest. Personal information provided at the time of registration is encrypted before being uploaded to the server where it is stored in a secure server. Data security breach owing to lapses on the part of the user (such as not patching OS updates, loss of device, etc.) is not the responsibility of the Government.

5. DISCLOSURES AND TRANSFER

Save as otherwise set out in Clause 2, no personal information collected by the application will disclosed or transferred to any third party, without prior consent of the user.

6. GRIEVANCES

If user has any concerns or questions in relation to this Privacy Policy, he/she may address them to the Grievance Officer whose name and address are as follows: <Name and Designation of the Departmental Officer>; <Address>; <Email ID>.

2.4 Terms and Conditions Template

These terms of use describe your rights and responsibilities as a user of the <website address>. To have an account, you must accept these terms of use.

<Department name> reserve the right to make changes to <application> and these terms of use at any time. If those changes affect your rights or responsibilities, you will be notified through <application>.

The following terms of use supersede and replace any terms and conditions you may have previously accepted governing your use of <application>. The following Terms & Conditions come into effect as soon as you have accepted it and created your <application> account.

As a user of <application> you are granted a nonexclusive, non-transferable, revocable, limited license to access and use <application> and content in accordance with these Terms of Use. Provider may terminate this license at any time for any reason.

Though all efforts have been made to ensure the accuracy and currency of the content on <application>, the same should not be construed as a statement of law or used for any legal purposes. In case of any ambiguity or doubts, users are advised to verify/check with the concerned Ministry/Department/Organization and/or other source(s), and to obtain appropriate professional advice.

Under no circumstances will the Government Ministry/Department/Organization be liable for any expense, loss or damage including, without limitation, indirect or consequential loss or damage, or any expense, loss or damage whatsoever arising from use, or loss of use, of data, arising out of or in connection with the use of <application>.

LIMITATION ON USE:

The Content on <application> is for your personal use only and not for commercial exploitation. You may not decompile, reverse engineer, disassemble, rent, lease, loan, sell, sublicense, or create derivative works from <application>. Nor may you use any network monitoring or discovery software to determine the site architecture, or extract information about usage, individual identities or users. You will not use any robot, spider, other automatic software or device, or manual process to monitor or copy <application> without Provider's prior written permission. You will not copy, modify, reproduce, republish, distribute, display, or transmit for commercial, non-profit or public purposes all or any portion of <application>, except to the extent permitted by the copyright policy of this terms of use. Any unauthorized use of <application> is prohibited. The use of any software (e.g. bots, scraper tools) or other automatic devices to access, monitor or copy the website pages is prohibited unless expressly authorized by the <application> in writing.

POLICY WITH REGARD TO YOUR CONTENT:

Uploading content or submitting any materials for use on <application>, you grant (or warrant that the owner of such rights has expressly granted) <application> a perpetual, worldwide, royalty-free, irrevocable, non-exclusive right and license, with right to sublicense, to use, reproduce, modify, adapt, publish, publicly perform, publicly display, digitally display and digitally perform translate, create derivative works from and distribute such materials or incorporate such materials into any form, medium, or technology now known or later developed throughout the universe. You agree that you shall have no recourse against Provider for any alleged or actual infringement or misappropriation of any proprietary right in your communications to us.

USER RESPONSIBILITY:

You must:

- Be a natural person to access or seek to access <application> or a Member Service;
- Not access or link to or seek to access or link to (either directly or indirectly) any other person's <application> or Member Service account;
- Not permit any other person to use your username and password; keep your <application> account username, password, at all times and not disclose your password to anyone else;
- Report the Helpdesk immediately if you suspect that the security of your <application> account may have been compromised e.g.: your password or username has been lost or stolen. Contact <application> using the details at Contact Us;
- Ensure your personal details (including your name and date of birth) are accurate and keep up to date with <application>;
- You are responsible for any use of your <application> account using your username and password, whether or not such use has been authorized by you.
- Details on <application> may only be accessed through the <application> website, and only using the username and authentication details which have been specifically allocated to you.

You must use <application> and your <application> account only for lawful purposes and in a manner that does not infringe the rights of or restrict or inhibit the use and enjoyment of <application> by any third party. This includes conduct which is unlawful or which may harass or cause distress or inconvenience to any person, the transmission of obscene or offensive content or disruption to <application>.

You must not post or transmit via <application> any unlawful, defamatory, obscene, offensive or scandalous material, or any material that constitutes or encourages conduct that would contravene any law.

INFORMATION THAT YOU PROVIDE ON <APPLICATION>:

If, within your <application> account, you are asked to provide information, the information you supply must be complete and accurate. You acknowledge that if you supply incomplete, inaccurate or false information, use <application> to perform (or attempt to perform) an unauthorized action, or otherwise misuse <application>, the it may suspend or terminate your <application> access.

Giving false or misleading information is a serious offence. Providing incomplete, inaccurate or false information via <application> will be treated in the same way as providing incorrect information on a form or in person and may result in prosecution and civil or criminal penalties.

COPYRIGHT POLICY:

Material featured on this website may be reproduced free of charge. However, the material has to be reproduced accurately and not to be used in a derogatory manner or in a misleading context. Wherever the material is being published or issued to others, the source must be prominently acknowledged. However, the permission to reproduce this material shall not extend to any material which is identified as being copyright of a third party (user submitted content). Authorization to reproduce such material must be obtained from the copyright holder concerned.

HYPERLINKING POLICY:

Links to external websites/portals

At many places on <application>, you shall find links to other websites/portals. These links have been placed for your convenience. <application> is not responsible for the contents of the linked websites and does not necessarily endorse the views expressed in them. Mere presence of the link or its listing on this website should not be assumed as endorsement of any kind. We cannot guarantee that these links will work all the time and we have no control over availability of linked destinations.

Links to <application> by other websites/portals

We do not object to you linking directly to the information that is hosted on this web site and no prior permission is required for the same. However, we would like you to inform us about any links provided to this website so that you can be informed of any changes or updates therein. Also, we do not permit our pages to be loaded into frames on your site. The pages belonging to <application> must load into a newly opened browser window of the User.

PRIVACY POLICY

This website does not automatically capture any specific personal information from you (like name, phone number or e-mail address), that allows us to identify you individually. If you choose to provide us with your personal information, like names or addresses, when you visit

our website, we use it only to fulfill your request for information. To participate and engage with government through <application> requires your registration. Information so collected is used to facilitate interaction.

<application> conducts many Quizzes, Hackathons, and Contests in collaboration with Ministries and Departments. The personal details of the winners can be shared with the Contest Creators/ Collaborating Departments. The names of the winners, without any Personally Identifiable Information, can be used by the <application> Team and the Contest Creator/ Collaborating Departments for display in public by means of Electronic/ Print Media.

<application> do not sell or share any personally identifiable information volunteered on this site to any third party (public/private) except for the winners as explained in para above. Any information provided on <application> will be protected from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

<application> gather certain information about the User, such as Internet protocol (IP) address, domain name, browser type, operating system, the date and time of the visit and the pages visited. <application> make no attempt to link these addresses with the identity of individuals visiting our site unless an attempt to damage <application> has been detected.

COOKIES POLICY

A cookie is a piece of software code that an internet web site sends to your browser when you access information at that site. A cookie is stored as a simple text file on your computer or mobile device by a website's server and only that server will be able to retrieve or read the contents of that cookie. Cookies let you navigate between pages efficiently as they store your preferences, and generally improve your experience of a website. <application> use following types of cookies to enhance your experience and interactivity with <application> its sub-domains:

1. Analytics cookies for anonymously remembering your computer or mobile device when you visit our website to keep track of browsing patterns.

2. Service cookies for helping us to make our website work efficiently, remembering your registration and login details, settings preferences, and keeping track of the pages you view.

3. Non-persistent cookies a.k.a per-session cookies. Per-session cookies serve technical purposes, like providing seamless navigation through <application> and its sub-domains. These cookies do not collect personal information on users and they are deleted as soon as you leave our website. The cookies do not permanently record data and they are not stored on your computer's hard drive. The cookies are stored in memory and are only available during an active browser session. Again, once you close your browser, the cookie disappears.

You may note additionally that when you visit <application> and its sub-domains where you are prompted to log in, or which are customizable, you may be required to accept cookies. If

you choose to have your browser refuse cookies, it is possible that sub-domains of <application> may not function properly.

2.5 Cloud Services Usage Guidelines

While departments must host their applications and data in SDC, some departments may be required to host in private clouds set up at Amazon, Azure, etc.,

One of the most critical issues that need to be addressed in the Cloud Service Agreement is the security of the data. This issue further poses a significant risk if the data is sensitive in nature.

The following contractual terms may be included in the agreements.

1. CERTIFICATION / COMPLIANCE:

i. Departments need to ensure that the Cloud service provider or CSPs facilities/services are certified to be compliant to the following standards based on the project requirements:
ii. ISO 27001 - Data Centre and the cloud services should be certified for the latest version of the standards
iii. ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology
iv. 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds.
v. ISO 20000-9-Guidance on the application of ISO/IEC 20000-1 to cloud services
vi. PCI DSS - compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud – This standard is required if the transactions involve credit card payments.

MeitY with the help of STQC is carrying out the audit and is in the process of certifying the service offerings of CSPs for the above three standards. Therefore, the Departments may include the following clauses in the agreements.

1. The CSP/Service Provider shall comply or meet any security requirements applicable to CSPs/Service Providers published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP/Service Providers by MeitY as a mandatory standard
2. The CSP/Service Provider shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply to the audit criteria defined by STQC
3. (The Departments may refer the Information Classification, National Information Security Policy and Guidelines, Ministry of Home Affairs (MHA) while choosing to deploy on cloud)

2. PRIVACY AND SECURITY SAFEGUARDS.

The Department may ensure that specific clauses pertaining to the following are included

in to the contracts.

i. If the data is classified as very sensitive, the Departments may include a clause to ensure that the data is encrypted as part of a standard security process for highly sensitive content or choose the right cryptographic algorithms evaluating security, performance, and compliance requirements specific to their application and may choose from multiple key management options.

ii. The Department may include a clause that the provider notifies the agency promptly in the event of security incidents or intrusions, or requests from foreign government agencies for access to the data, to enable the agency to manage these events proactively.

iii. At the end of the agreement, the Department shall ensure that all the storage blocks or multiple copies of data if any are unallocated or zeroed out by the CSPs so that data cannot be recovered. If due to some regulatory reasons if it is required to securely decommission data, departments can implement data encryption at rest using departments managed keys, which are not stored in the cloud. Then customers may delete the key used to protect the decommissioned data, making it irrecoverable.

iv. The CSP/Service Provider shall report forthwith in writing of information security breaches to the Department by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Project's Data, facilities or Confidential Information.

v. The CSP undertakes to treat information passed on to them under this Agreement as classified. Such Information will not be communicated / published / advertised by the CSP to any person/organization without the express permission of the Department.

3. CONFIDENTIALITY

In cases where the CSP has access to highly sensitive information (in case of departments like defense), Departments may include the following clause in the agreements:

i. The CSP/Service Provider shall execute non-disclosure agreements with the Department with respect to this Project. For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:

i. information already available in the public domain;

ii. information which has been developed independently by the Service Provider;

iii. information which has been received from a third party who had the right to disclose the aforesaid information;

iv. Information which has been disclosed to the public pursuant to a court order.

ii. The Subcontractors will be permitted to obtain customer data only to deliver the services the CSP has retained them to provide and will be prohibited from using

customer data for any other purpose. The CSP remains responsible for its subcontractors' compliance with CSP's obligations under the Project."

4. LOCATION OF DATA

The location of the data could be located in one or more discrete sites in foreign countries. Therefore, it has to be specifically mentioned in the agreement. The terms and conditions of the Empanelment of the Cloud Service Provider has taken care of this requirement by stating that all services including data will be guaranteed to reside in India. Therefore, the following clause should be included in the contract:

The location of the data (text, audio, video, or image files, and software (including machine images), that are provided to the CSP for processing, storage or hosting by the CSP services in connection with the Department's account and any computational results that a Department or any end user derives from the foregoing through their use of the CSP's services) shall be as per the terms and conditions of the Empanelment of the Cloud Service Provider.

5. E-DISCOVERY

Electronic discovery (e-discovery) is the process of locating, preserving, collecting, processing, reviewing, and producing Electronically Stored Information (ESI) in the context of or criminal cases/proceedings or investigation. The Department must be able to access and retrieve such data in a CSP environment in a timely fashion for normal work purposes.

6. LAW ENFORCEMENT REQUEST

The Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the Service Provider. The onus shall be on the Service Provider to perform all due diligence before releasing any such information to any such law enforcement agency.

7. AUDIT

In the traditional Information Technology agreements, under the Article – Audit, Access and Reporting, clauses related to carrying out inspection and auditing are usually included to ensure compliances by the Service Provider. However, as the cloud services are provided to multitude of customers, the CSPs do not permit access to ensure security for all customers. Therefore, Departments can check compliances by accessing and verifying all the global compliance certification audit reports. In addition, the Departments shall mention the standards that the CSPs need to demonstrate compliance to the standards such as ISO 27001, ISO 27018 etc. rather than physical access and audits. As STQC/MeitY is carrying out the audit and certification of the cloud service offerings of various CSPs, the Departments shall ensure that the Cloud Service Provider's services offerings are audited and certified by STQC/MeitY. The Departments may include the following clauses in the Agreement:

i. The Cloud Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC /MEITY guidelines as and when published).

ii. The Audit, Access and Reporting Requirements should be as per the terms and conditions of the Provisional Empanelment of the Cloud Service Provider.

8. TRANSITIONING/EXIT

Transitioning can be a critical issue and it is important for the Departments to include the following clauses in the agreement:

a. The CSP shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Department. Any cost for retaining the data beyond 45 days shall be paid to the Service Provider based on the cost indicated in the commercial quote.

b. The CSP shall be responsible for providing the tools for import / export of VMs & content and the MSP shall be responsible for preparation of the Exit Management Plan and carrying out the exit management / transition

Clauses related to managed service provider (MSP)

c. The MSP shall provide the Department or its nominated agency with a recommended exit management plan ("Exit Management Plan") or transition plan indicating the nature and scope of the CSP's transitioning services. The Exit Management Plan shall deal with the following aspects of the exit management in relation to the Agreement as a whole or the particular service of the Agreement:

i. Transition of Managed Services

ii. Migration from the incumbent cloud service provider's environment to the new environment

d. The MSP is responsible for both Transitions of the Services as well as Migration of the VMs, Data, Content and other assets to the new environment.

e. The MSP shall carry out the migration of the VMs, data, content and any other assets to the new environment created by the Department or any other Agency (on behalf of the Department) on alternate cloud service provider's offerings to enable successful deployment and running of the Government Department's solution on the new infrastructure.

f. The format of the data transmitted from the cloud service provider to the new environment created by the Department or any other Agency should leverage standard data formats (e.g., OVF…) whenever possible to ease and enhance portability. The format will be finalized by the Government Department.

g. Transitioning from the CSP including retrieval of all data in formats approved by

Department

h. The MSP shall ensure that all the documentation required by the Department for smooth transition (in addition to the documentation provided by the Cloud Service Provider) are kept up to date and all such documentation is handed over to the Department during regular intervals as well as during the exit management process.

i. The MSP will transfer the organizational structure developed during the Term to support the delivery of the Exit Management Services. This will include:

i. Document, update, and provide functional organization charts, operating level agreements with Third-Party contractors, phone trees, contact lists, and standard operating procedures.

ii. Transfer physical and logical security processes and tools, including cataloguing and tendering all badges and keys, documenting ownership and access levels for all passwords, and instructing Department or its nominee in the use and operation of security controls.

j. Some of the key activities to be carried out by MSP for knowledge transfer will include:

i. Prepare documents to explain design and characteristics.

ii. Carry out joint operations of key activities or services.

iii. Briefing sessions on process and process Documentation.

iv. Sharing the logs, etc.

v. Briefing sessions on the managed services, the way these are deployed on cloud and integrated.

vi. Briefing sessions on the offerings (IaaS/PaaS) of the cloud service provider

k. Transfer know-how relating to operation and maintenance of the software and cloud services.

9. CSP PREREQUISITES:

i. Certification Requirements: ISO 27001, ISO 20000:1, ISO27017, ISO 27018, TIA 942/Uptime Institute

ii. Data Residency: Hosting of government data within the country mandatory.

iii. There shall not be any outside legal framework applicable on CSPs (undertaking provided by CSPs)

iv. CSPs shall be required to offer their services in two categories (Basic and Advanced) as per the Cloud Service Bouquet prepared by MeitY

v. DC and DR to be separated by a distance of 100 Kms

vi. CSPs are required to offer the empaneled Cloud services to government organizations through GeM platform

vii. CSPs to comply with specify additional security requirements based on the department applications

viii. Successful STQC audit is prerequisite for offering Cloud Services to Govt. Dept.

10. SECURITY IN CLOUD IS A SHARED RESPONSIBILITY

Department Responsibility

i. Identity and access management - Specifying the roles of users for managing access to application, data and platform
ii. Ensuring the security of endpoints that are used to access Cloud services
iii. Configuring operating system, network, firewall & security settings associated with the Cloud service being consumed
iv. Applying data and server side encryption
v. Reviewing and validating security configurations created by CSP/MSP

CSP Responsibility

i. Security of infrastructure components (compute, storage, network, etc.) including upgrade, maintenance and patch deployment
ii. Virtualization & hardening of hypervisor
iii. Physical and Logical network segmentation
iv. Perimeter security services
v. Providing tools for backup, migration and replication
vi. Offering Disaster Recovery Services

2.6 Checklist for Securing Application

The checklist is categorized into seven sections:

1. SecOPS and Configuration Management
2. Data Protection
3. Authentication and Access Control
4. I/O Handling
5. Logging
6. Error Handling
7. Session Management

1. SecOPS and Configuration Management

From the outset, it's important to ensure that all security requirements are documented, and that these requirements are accounted for in deployment, design, review, testing and change management processes.

Checklist Item	Notes
Document security requirements	Work with the cloud Governance, Risk, and Compliance (GRC) group and the application team to document all the security-related requirements. These can be across functional and non-functional requirements. Transforming requirements to user stories allows you to track them using your agile ticketing system (like Rally or Jira).
DevSecOps friendly change management	Automate the change management process and align with the current CI/CD process so that new releases can be deployed only after proper testing and associated documentation.
Automated deployment	Use automation for Continuous Integration and Continuous Deployment to ensure that releases are consistent and repeatable in all environments.
Continuous design review	Continuously review the design and architecture of the application throughout its life cycle. Security analysis, risk identification, and mitigation are key focus areas.
Continuous code review	Continuously review the code of the application as the application is updated or modified. Security analysis, risk identification, and mitigation are key focus areas.

Checklist Item	Notes
Continuous security testing	Continuously test the application for security vulnerabilities throughout the DevOps process and the application lifecycle.
Infrastructure hardening based on releases	Harden all components of the logical infrastructure that the application uses as per the guidelines and compliance required for that application environment.
Incident response automation	Automate and continuously update the defined incident-handling plan.
Continuous training	Train developers, cloud engineers, and architects on the new features of the cloud services that the application uses.

2. Data Protection

It is also important to ensure these data protection capabilities. Many are built into cloud infrastructure by default, and others are available as a service.

Checklist Item	Notes
HTTPS only	Use HTTPS (TLS) for front end and backend application flows.
HTTP access disabled	Disable HTTP for all publicly exposed interfaces. Ideally disable it globally.
Use vaults for user password stores	Use secret management with Wallet or Key Vault.
Use of Strict-Transport-Security header	Strict-Transport-Security header helps to mitigate any HTTP downgrade attacks using variations of the sslsniff tool.
Secure key management	Properly store, secure, and rotate keys. Cloud Infrastructure Key Management can provide this solution.
Strong TLS configuration	Use TLS 1.2 or above with strong EC cipher strength. Cloud Infrastructure LBaaS uses TLS 1.2 with following cipher sets: ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 DHE-RSA-AES256-GCM-SHA384 DHE-RSA-AES256-SHA256 DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES128-SHA256
Reputable certificate authority	Ensure certificates are valid and signed by reputable certificate authorities. Match the name on the certificate with the FQDN of the website.
Browser data caching	Configure browsers not to cache data using cache control HTTP header or meta tags.

Checklist Item	Notes
Data at rest	In Cloud Infrastructure, by default, all storage types (block, file, and object) are encrypted.
Key exchange	Exchange keys over a secure channel.
Tokenization of sensitive data	Where possible, don't store sensitive data at the web or application layer. If necessary, use tokenization to reduce exposure.

3. Authentication & Access Control

When it comes to authentication and access control over cloud infrastructure, these guidelines may be followed.

Items	Notes
Access control checks	Apply access controls checks consistently all along the stack following the principle of complete mediation.
Least privilege	Apply the principle of the least privilege by using a mandatory access control systems such as Identity Cloud Service (IDCS) and Cloud Infrastructure IAM mediation.
Direct object reference	Avoid referring to objects directly. Always use relative pointers based on the authenticated user identity and trusted server-side information.
Unvalidated redirects	Don't permit unvalidated redirects. Put a strong access control policy in place to validate any redirect requests.
Credential security	Avoid hardcoding credentials. Secure the database storing the credentials using multiple tiers of security controls.
Strong password policy	Implement a strong password policy along with an automated multi-factor identity-based password reset system.
Account lockout policy	Implement an account lockout policy to protect against brute-force attacks. Display appropriate nonspecific messages around wrong credentials to confuse an attacker.
Multi-factor authentication	Ensure multi-factor authentication is in place using Yubikeys or other hardware or software-based tokens.

4. I/O Handling

To help ensure secure I/O handling, it is recommended to review this checklist to mitigate possible security attacks.

Checklist Item	Notes
Whitelist	Use whitelists in place of blacklists. Validate each input or output within the context of use.
Standard encoding for the application	Use standard encoding like UTF-8 consistently for all the application pages using HTTP headers or meta tags to reduce risks like cross-site scripting attacks.
Nosniff header usage	X-Content-Type-Options: Use nosniff headers to stop browsers from guessing the data type.

Checklist Item	Notes
Tabnabbing	Prevent tabnabbing by denying the linked page the ability to change the opener's tab. This is a common look-a-like phishing attack.
Well-formed SQL queries	Use parameterized SQL Queries with user content passed into a bind variable to make queries safe against SQL injection attacks. Never build SQL Query strings dynamically from user input.
X-Frame-Options	Use Content-Security-Policy (CSP) header frame-ancestors directive to mitigate clickjacking.
Secure HTTP response header	To defend against MITM and XSS attacks, use X-XSS-Protection, CSP, and Publik-Key-Pin headers.

5. Logging

Logging is a critical part of ensuring adherence to compliance and for maintaining a good security posture. Below are some guidelines on the types of activities to log.

Checklist Item	Notes
Sensitive data access logging	Log sensitive data access to meet regulatory compliance such as PCI and HIPAA.
Privilege escalation logging	Log all privilege escalation requests for audit and compliance.
Administrative activities using Console, CLI, and API logging	Log all administrative access for application configurations or infrastructure configurations.
Authentication and validation activities logging	Log all authentication, session management, and input validations.
Ignore unimportant data	Avoid logging unimportant or inappropriate data to reduce storage and the associated encryption overhead.
Secure all logs	Securely store logs using encryption and as per the established log retention policy.

6. Error Handling

Below are some best practices for how to handle unexpected errors and the error messages the system sends.

Checklist Item	Notes
Handle all exceptions	Handle unexpected errors and gracefully return to the user or the invoking application.
Generic error messages	Display generic error messages to the user to protect details of the application stack.
Framework generated messages	Suppress framework-generated messages because they can reveal sensitive information about the framework used and can lead to sophisticated exploits.

7. Session Management

Implement these session management attributes to avoid any potential security risks.

Checklist Item	Notes
Session tokens	Every time a user authenticates or escalates their privilege level, generate a new session token. Regenerate the token even if the encryption status changes.
Idle session timeout	To prevent against Ajax application-based attacks, implement an idle session timeout.
Absolute session timeout	To mitigate against a session hijacking, log users out every 4–6 hours.
Session destruction	In case any tampering or intrusion is detected, immediately destroy the session.
Cookie domain path	Restrict the domain and the path scope for the application in context. Avoid any wildcard domain setting.
Cookie expiration time	Set a reasonable expiration time for every session cookie.
Cookie attributes	Set secure attributes using Http Only and secure flags to make the session id invisible to any client-side scripts.
Session log out	Once the user logs out of their session, invalidate and destroy the session.

8. Security-Related Operational Capabilities

Capability	Sensitive Applications	Nonsensitive Applications	Notes and Comments
Third-party attestations viewable by customers	Required	Recommended	SOC 2 and ISO 27001 are common. Others may be appropriate for certain regions or industries.
Ability to support compliance requirements	Required	Optional	Examples include: PCI, HIPAA, GDPR. Not a direct capability but instead is provider guidance explaining how customers may achieve compliance.
Ability to specify where data is stored	Optional	Optional	May be needed for compliance purposes or regulations that require storing data in specific geographic regions.
Isolation of compute and data between customers	Required	Required	Almost always a function of the underlying delivery platform, which may be one of the major IaaS cloud providers.
Denial of service protection	Required	Required	Provider should withstand common DoS attacks without data loss or significant outages.
Data encrypted in transit	Required	Required	Should be TLS 1.2 or higher with perfect forward secrecy and no certificate pinning (so that traffic inspection may operate normally).
Data encrypted at rest by the service provider	Optional	Optional	Not visible at the customer level. Protects against the unlikely scenario of a disk drive escaping provider control.
Secure APIs for all functionality	Required	Required	Published APIs for accessing customer data should require authentication to avoid accidental or malicious exposure.

Ability to operate through a forward or reverse proxy	Recommended	Optional	Allows unmanaged devices to access the application and be monitored.
Ability to enumerate plug-ins	Recommended	Optional	Some SaaS applications offer a PaaS-like development environment; tracking installed plug-ins should be possible.
Ability to gain enterprise visibility across multiple instances	Required	Optional	Necessary for IT to obtain visibility into and regain control of instances provisioned by business units.

9. Security Features Customers Can Enable

Capability	Sensitive Applications	Nonsensitive Applications	Notes and Comments
Documentation describing how to use security features	Required	Required	Expect documentation to vary in quality, if it exists at all. Providers must be pressured to always improve their documentation.
Identity creation and management	Optional	Optional	Native identities may exist, but the more common approach is to integrate with some other existing identity service.
Higher trust (such as multifactor) authentication for admins	Required	Recommended	Powerful accounts must be afforded strong protection. May be offered natively or via third-party IdP/IDaaS.
Higher trust (such as multifactor) authentication for users	Required	Recommended	Configure at least for commonly targeted users or those who routinely work with sensitive information. Native or third-party.
Access controls on objects in storage	Required	Required	The fundamental strategy for implementing the principle of least privilege.
Role-based access controls	Required	Recommended	Simplifies day-to-day administration but requires additional planning.
Adaptive access control	Recommended	Optional	Allow reduced functionality in certain situations (e.g., personal computer or unenrolled phone) rather than outright blocking.
Privileged access management	Recommended	Recommended	Eliminates the need to configure powerful accounts attractive to attackers. May be provided through identity integration rather than natively.
Granular authorization policies	Recommended	Optional	Contextual authorization that evaluates multiple signals and makes a just-in-time decision to allow or limit access.
Administrator activity logging, auditing and alerting	Required	Recommended	Necessary for demonstrating that use of the cloud is being governed. A SIEM can be a useful add-on or substitute.
User activity logging, reporting and alerting	Required	Recommended	A CASB or a SIEM may be preferred to track user activity across multiple applications in a single place.
Ability to set default sharing scopes (internal, external)	Required	Required	SaaS provider defaults favour maximum utilization of their services, which likely do not align with an organization's preferences.
Ability to set expirations on shares and links	Required	Required	An organization wide default (which few users will feel the need to change) may

			be the single most significant means for stopping leaks.
Ability to quarantine unstructured data if malware is detected	Recommended	Recommended	Prevents the further spread of malware.
Unstructured data encrypted at rest in the subscription	Recommended	Optional	Not a substitute for access controls. May be required for certain compliance schemes.
Structured data encrypted or tokenized in the subscription	Recommended	Optional	Useful for concealing certain sensitive elements from the larger user community.
Customer-controlled encryption key management	Recommended	Optional	Service is native but keys are provisioned by customers only, not by the provider. May be hardware-backed.
Host- and bring-your-own-key (HYOK, BYOK)	Optional	Optional	Because the subscription has access to keys, it's largely irrelevant where the keys are generated.
Content scanning and hygiene (anti-malware, sandboxes)	Recommended	Optional	Applicable only to services that allow users to store files. Never a substitute for endpoint anti-malware.
Sensitive data monitoring and data loss prevention (DLP)	Recommended	Optional	A CASB may be preferred. Individual per-SaaS DLP is likely to be inconsistent from one application to another.
Data classification or labelling	Recommended	Optional	These do nothing on their own, but are useful inputs for policies created elsewhere. Automatic classification is much more useful than manual.
Geofencing	Optional	Optional	It may be useful to limit the activity of certain users based on the geographic location.
Security health check or scoring tool	Recommended	Optional	SaaS providers that are often strategic have begun offering mechanisms for customers to measure their security posture.

10. Integration Points With Existing Products and Services

Product or Service	Sensitive Applications	Nonsensitive Applications	Notes and Comments
Documented APIs to facilitate integration	Recommended	Recommended	Integration may not always be configurable via a graphical interface, and instead may require writing a small amount of code.
Identity provisioning, governance and administration	Recommended	Recommended	Necessary to synchronize and provision identity information. Can occur through provisioning APIs or SCIM standard.
Access management integration for single sign-on	Required	Recommended	Necessary for single-sign on (SSO), with (at least) SAML2 support. May require synchronizing IDs and passwords to destination services.
Security incident and event monitoring (SIEM)	Recommended	Optional	Reduces the number of consoles that security teams must monitor.
User and entity behaviour analysis (UEBA)	Optional	Optional	Typically a function of a SIEM tool.

Cloud security access broker (CASB)	Required	Recommended	Ensure support in existing CASB for new SaaS applications during POC evaluation phase.
CASB API inspection	Required	Recommended	API inspection can interrogate data at rest in SaaS applications and can assess events and incidents stored in SaaS application logs.
CASB proxy inspection	See notes	See notes	Required for use cases that rely on DLP, adaptive access control or other real-time action. Choose accordingly.
Secure web gateway (SWG)	Optional	Optional	SWG awareness of SaaS applications not only increases visibility and control but can also improve application performance.
Enterprise digital rights management (EDRM)	Optional	Optional	A useful technique for extending control and visibility to documents and data downloaded locally to devices.
SaaS management platform (SMP)	Recommended	Optional	Ensure support in existing SMP for new SaaS applications during POC evaluation phase.
Ticketing system	Recommended	Optional	Eliminates the requirement for incident responders to check multiple locations for closing help desk requests.

2.7 KSDC - Requirement Gathering Template

KSDC uses this template to gather requirements from the departments.

Slno	Department	Server Type Web/App / Database	Configuration			OS	Additional software (to be installed by application Team)	Requested on
			RAM	CPU	HD			
			Requested	Requested	Requested	Requested		
1								
2								
3								
4								
5								
6								
7								

Name of the Application		
Name of the Department		
Department contact		
	Nodal Officer name	
	Phone number	
	email Address	
	Postal address	
		Seal and Signature of the nodal officer
Application Contact		
	Name	
	Phone number	
	email Address	
	Postal address	
List of Cert-IN empanelled vendor for Safe to host certificate		
	https://www.cert-in.org.in/PDF/Empanel_org.pdf	
List of vendors for SSL certificate		
1	aman@jnrmanagement.com	
2	guna.shekar@frontier.in	
3	ssl@apexitservices.in	
4	rohit.parmar@diinfotech.com	

2.8 KSDC - Questionnaire Document - Web Application Security

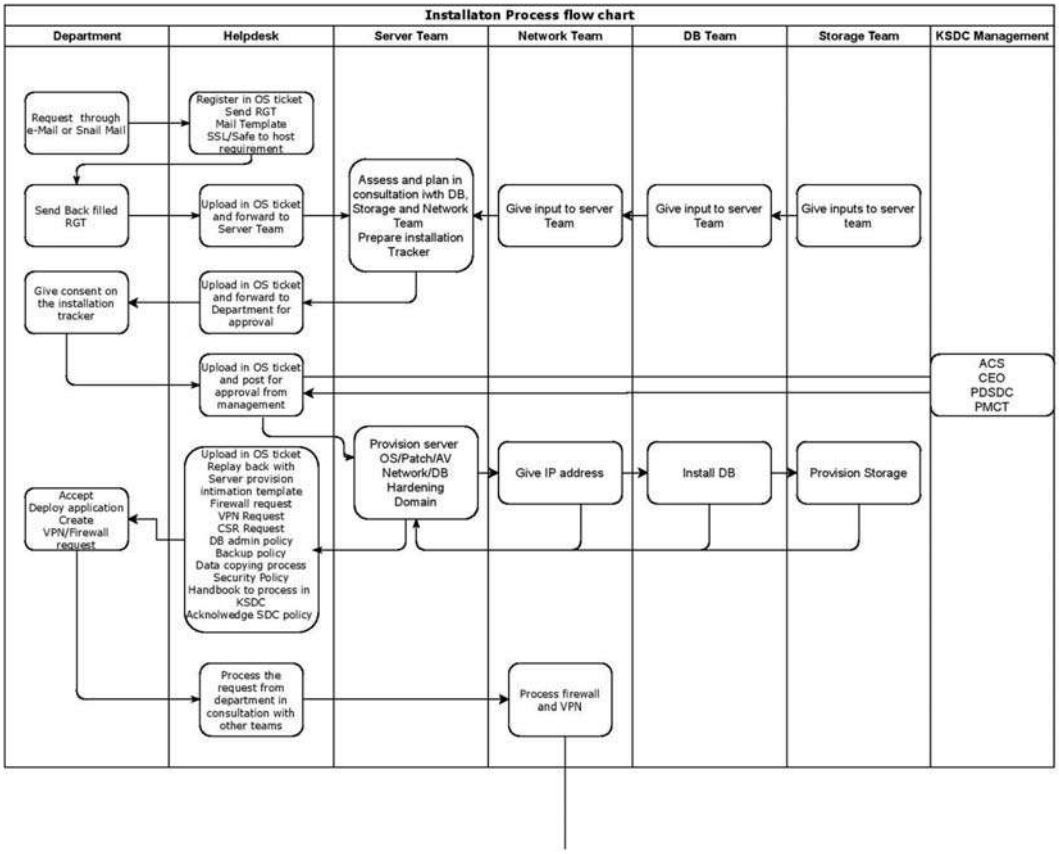
Offering Information	
Offering Name	Security Audit
Brief Description	
Management Contact	
Approver Name	
Technical focal (primary and secondary)	
Testing environment (Standalone / Staging / Production)	
Desired Test Dates	
If the application was Audited earlier. Please provide the Report	
Web Application	
Web Application Count Include applications that communicate over http(s)	
Name	
Description	
URL	-
Inputs from the Threat Modelling exercise, functional walk through & navigation of web application critical paths and workflow	-
Systems hosting the web applications need to be of higher resource configuration since the pen testing may involve sending many http requests.	-
Exclusive access to the test systems for the entire duration of (depends on size of application) the pen testing should be part of the plan.	-
Number of Web Pages Count a web page tab as a separate web page	
User authentication and authorization (basic auth, SAML, LDAP, HTML forms, certificates, etc.)	
Web Application Server (WAS, Tomcat, etc.)	
Database (DB2, MySQL, Cloudant, etc.)	

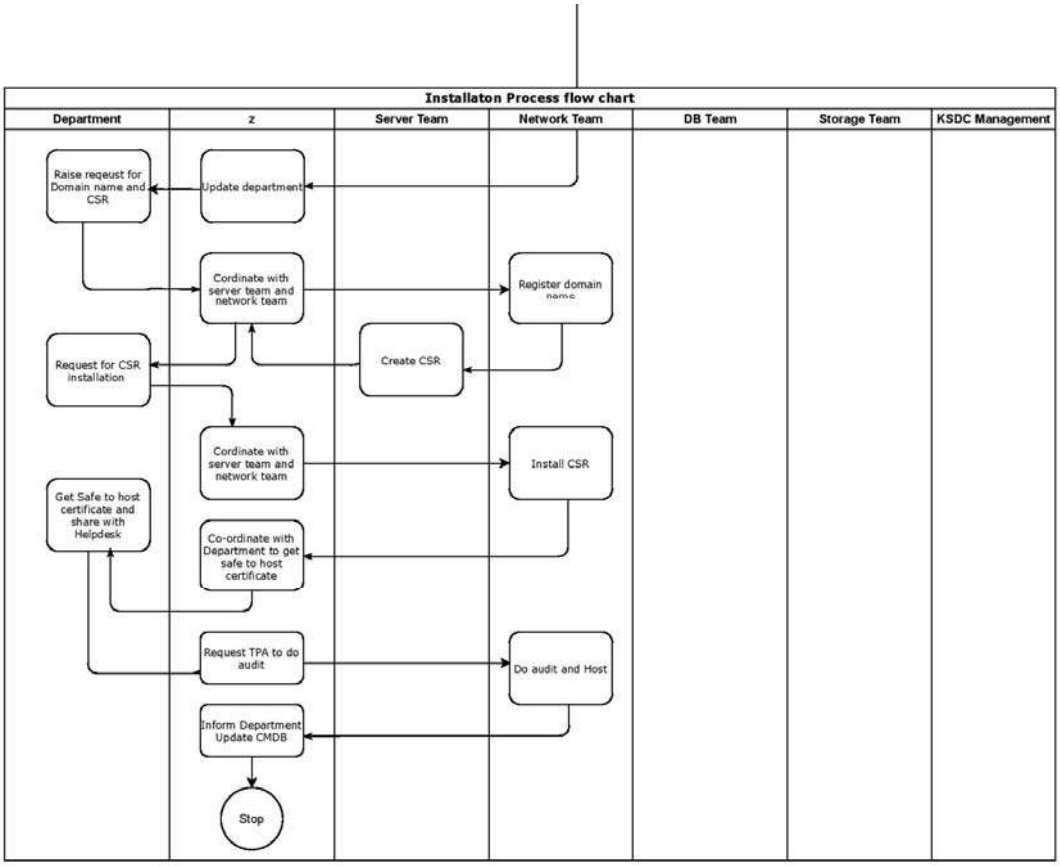
Technology and programming language used in Server back end and UI front end code (.Net, Java, JSP, XML, SOAP, AJAX, Dojo, HTML5, JavaScript, AngularJS, Flash, GWT, etc.)	
What is the size of the application in terms of no. Static and Dynamic pages?	
Whitelisting of the IP of testing machine	
Number of Entry and Exit Points	
Access to different roles such as with admin and non-admin privileges.	
The necessary passwords to get into the "locked" sections of the web application, if required.	
Technical consultation about the code/functionality involved with the target application.	
System administration if the application/test system goes down, freezes or becomes slow in response.	
User Manual/guide/Help documents, if any	
Scan Window (Restrictions, if any, on the timings to avoid impact on business as usual)	

Classification of Application based on Criticality

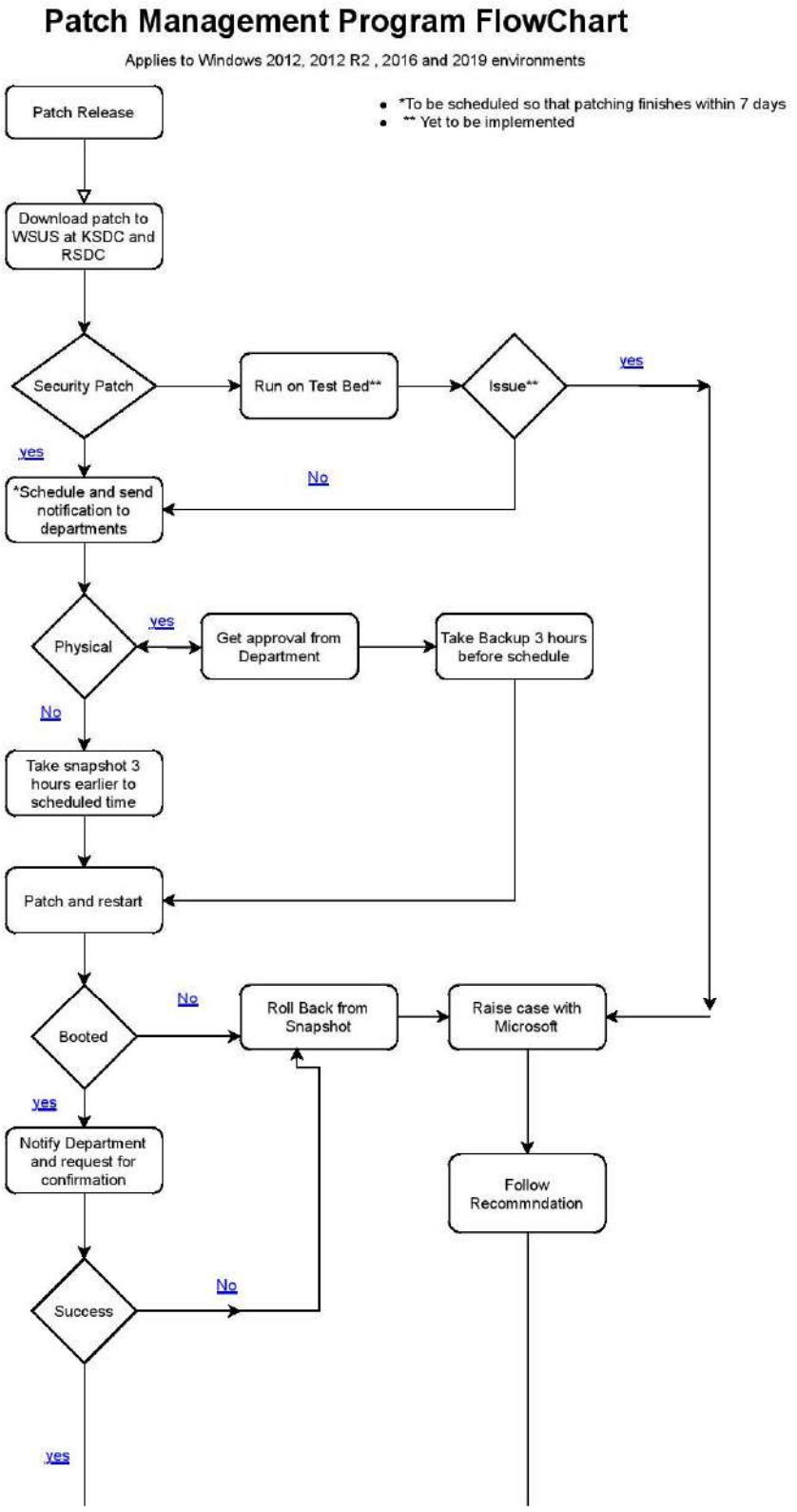
Category	Application	Description
Safety/Mission	Emergency Action	Always Critical
Business	Payment Processing	Often Critical
	Critical Department's Application	Often Critical
	Revenue impacting applications	Often Critical
Monitoring	Data Collection	Depends on criticality of the data
	Logging and Downloading/Uploading/Reporting	Usually Non-Critical

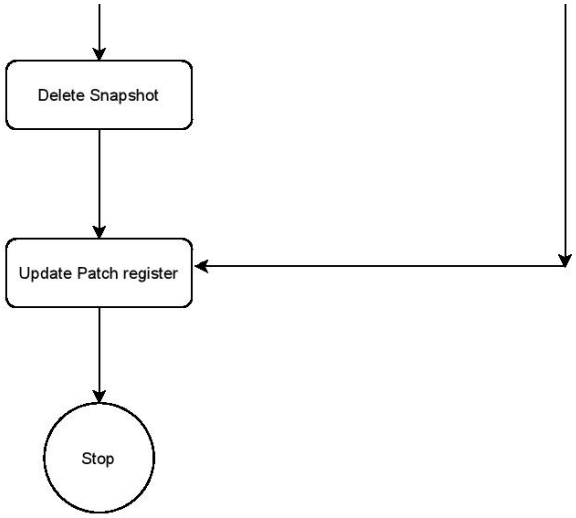
2.9 Flow Chart for Application Hosting at the State Data Center




Installaton Process flow chart
Department
z
Server Team
Network Team
DB Team
Storage Team
KSDC Management
Raise reqeust for Domain name and CSR
Update department
Cordinate with server team and network team
Register domain name
Request for CSR installation
Create CSR
Cordinate with server team and network team
Install CSR
Get Safe to host certificate and share with Helpdesk
Co-ordinate with Department to get safe to host certificate
Request TPA to do audit
Do audit and Host
Inform Department Update CMDB
Stop

2.10 Flow Chart for patch deployment at State Data Center (specific for Windows OS)




Delete Snapshot
Update Patch register
Stop