Guidelines for compliance to

Quality requirements of eProcurement Systems (GCQE)

Ministry of Electronics &Information Technology,
Electronics Niketan, 6 CGO Complex,
Lodhi Road, New Delhi – 110003

1.0**Introduction**

The Government including public sector is one of the biggest purchasers of goods & services. The Government of India acknowledges that automating procurement process using electronic tools/techniques and enabling opportunities to suppliers fully supports the objective of non-discrimination, fair & open competition. E-Procurement is identified as a mission mode project under national E-Governance plan. The objective is to transform Government /public sector purchase activity from labor-intensive paper based to efficient eProcurement process. Electronic Procurement (eProcurement) is the use of Information and Communication Technology (specially the Internet) by the buyer (in this case Government) in conducting their procurement processes with supplier for the acquisition of goods (supplies), works and services. Use of Information Technology promotes the aims of open, non-discriminatory and efficient government procurement through transparent procedures.It is the technology-enabled acquisition of goods and services, required by an organization, at the best value obtainable in the most efficient manner possible.

The factors driving the adoption of eProcurement are:

- Reduced purchasing cost and improved efficiency
- Standardized purchasing processes across the organization
- Reduced administrative costs with better effectiveness
- Significant reduction in the procurement cycle
- Reduced discretion

At the same time the inhibitors to adoption are:

- Lack of supplier readiness
- System integration issues (compatibility and interoperability)
- Confidence on the system (Security, Functionality and Performance)
- Insufficient skilled staff

This document provides the guideline for compliance to quality requirements of eProcurement systems. The essential quality characteristics of eProcurement system cover Security, Transparency & Functionality.

1.1 Scope

This document covers the guideline for compliance of e-Procurement applications and e-Procurement System. The e-Procurement System (EPS) may include the following:

A. eProcurement Applications:

I. E-Tendering: Include registration process, bid publishing, bid submission and bid opening,

II. E-Auction: E-Auction includeseither forward or reverse auction or both, as per the requirement of customer/ user /developer's claim or any other technique with any of the following requirement:

a) Auction methodology, business rules and SRSshould be signed off by the intended specific user (s), if any.

b) NIA (Notice inviting Application), if any.
c) Govt. of Indiaguidelines/Any other applicable guideline

III. E-Tendering and E- Auction(as part of single application): As per detail in (I) and (II)

B. eProcurement System:

e-Procurement applications, with deployment Infrastructure (Servers, Network devices,storage, etc. either on premise or Cloud infrastructure located within India)

1.2 Objective

- To provide guidelines that could be followed for designing/developing an e-Procurement Application/system as well as the necessary process for monitoring adherence to the security and transparency requirements of an eProcurement application/system during the implementation and post implementation by the e-procurement application developers, service providers and other stakeholders.
- To provide Guidelines for assuring Quality and Security of an e-Procurement application/system so that confidence can be provided to its stakeholders that the system is secure, transparent, auditable & compliant with government procurement procedures.

1.3 Target Audience

- Purchase/ Head of Public Service Organization
- eProcurement Service Provider
- eProcurement Solution Provider/ Application Developer
- Third Party Testing and Audit Organization

1.4 General Requirements of eProcurement Application/System

The basic requirements of any eProcurement application/system are to achieve the goal of Government procurement, standardization of procurement processes and information entities in an efficient and transparent way. Hence the key requirements are to:

- **Adherence to GFR:**
  For public procurement of goods, services, works (e.g. construction) compliance with GFR rules, processes, roles (purchasing officer, local purchasing committee etc.) are mandatory requirements. The GFR rules needs to be applied into the application workflow of e-tendering process. eProcurement application /system (EPS) should be designed as per defined workflow with adequate security measures.
- **Confidentiality and Integrity of Information**

The key requirement of procurement in public service organization is to maintain the confidentiality & integrity of the information in procurement life cycle to protect the interest of buyer & supplier and to encourage the competitiveness in the business. The eProcurement platform transacts confidential procurement data and is exposed to several security threats. This requires employing a combination of security technologies and security best practices which result in reduced threat of data loss, leakage or manipulation. In eProcurement application/systemClass 3 Digital Certificate (Signature or Encryption or both)should only be used.

- **Vigilance Guidelines**
  The system should meet the requirements of guidelines issued from time to time by Central Vigilance Commission.
- **System Adaptability & customization**
  EPS need to have templates to offer flexibility in bidding methodologies as prevailing and followed currently in the manual process. Further, system should have templates to adopt bidding methodologies as may be prescribed by respective authorities.

1.5. Evaluation of eProcurement Application /System:

The evaluation & certification is essential to assure the Quality and Security of an eProcurement application/system. Through this process confidence can be provided to its stakeholders that the system is secure, transparent, auditable & compliant with government procurement procedures. The main components of an eProcurement system are:

- Data (eProcurement related documents & information)
- Software Application
- IT infrastructure (hardware & network)
- Operational (Security) processes
- Standards & Guidelines (GFR-2017, CVC Guideline, IT Act, MeitY EPS Guidelines)

These components need to be evaluated using techniques such as review, testing and audit under suitable conditions/ environments.

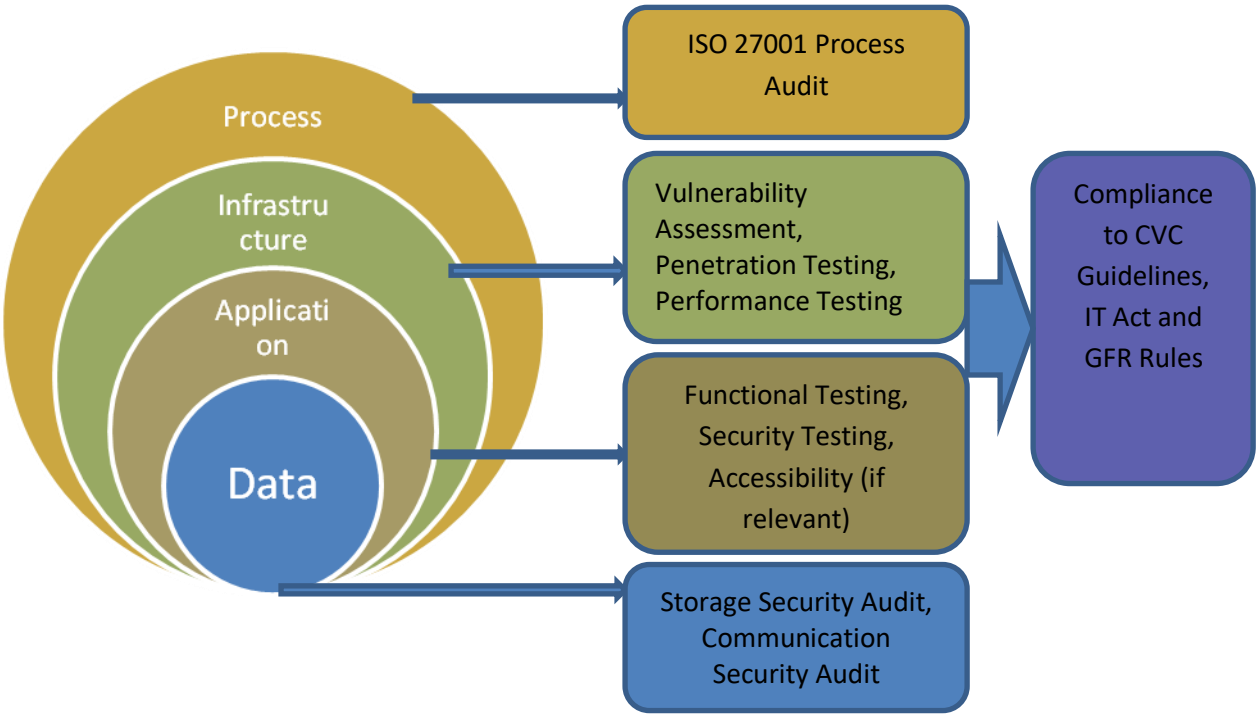
1.6 Approach for Evaluation of eProcurement System:

To evaluate an eProcurement System (covering data, software, hardware, network, and process) following approach will be adopted. This will ensure correct & complete implementation of the purchaser's organizational procurement policies & procedures:

- Testing and audit of the eProcurement solution to verify compliance with GFR rules, CVC guidelines, IT Act (including amendments)
- Assuring Security of the eProcurement system through testing & audit
- Security audit of data during Storage and Communication
- Testing of nonfunctional requirements of the eProcurement system such as Performance and Accessibility (if relevant).

2.0 Framework for Assessment

E-Procurement System



2.1 eProcurement Quality and Security Assurance Model

The Quality & Security evaluation model consist of four layers namely, Data, Application, Infrastructure and Process. Layer by layer assessment will ensure compliance with applicable requirements such as CVC, IT Act, GFR /Other applicable guidelinesand concerns of other stakeholders.

2.2 Description of the model

Brief description of the layers (from outermost to inner) are given below.

Process-Layer: ISO 27001 Certification(forinfrastructure hosting of eProcurement/ e-Auction services)

The hosting infrastructure e.g. DC/DR locations should have certification as per ISO/IEC 27001. The development facility of eProcurement application/System should be verified for the IT security processes to ensure that secure and best practices are followed in operation and maintenance of the e-Procurement System in line with international standard on Information Security Management System, ISO 27002.

Infrastructure Layer

Vulnerability Assessment (Servers & Network Devices)

System configuration checking or verification of hardening and service vulnerability scanning shall be performed to find out weaknesses, vulnerabilities and miss-configuration in the target hosts (Servers, Routers, Firewalls, Switches etc.) which hosts the e-procurement application.

Penetration Testing of the System

Penetration Testing (PT) shall be normally conductedremotely from public domain (Internet) and also can be conductedfrom internal network to find out exploitable vulnerabilities. Series of testing conducted like information gathering from public domain, port scanning, system fingerprinting, service probing, vulnerability scanning, manual testing, password cracking etc. using state-of-the-art tools (commercial and open source) and other techniques shall be used with the objective of unearthing vulnerabilities and weaknesses of the overall e-procurement system and its underlying IT infrastructure. The exercise should be carried out on production environment.

Performance Testing of the System

Performance testing of the e-procurement system shall be done to ensure that system is capable of handling defined user as well as transactional load, especially for the system handling auction application. Developer /user should specify their requirement towards number of simultaneous user. The performance testing of the e-procurement system essentially means measuring the response time of the system for defined scenarios. While measuring the response time it is important to record the resource (CPU, Memory, etc.) utilization.

The exercise should be carried out on production environment. If the application uses DSC based authentication during login, performance test may be restricted only to the home page (before DSC based login).

Application Layer

Application Functional Testing

The functional testing of the e-procurement software application shall be carried out to validate the application meets the specified functional requirements covering the work flows, navigations, and business & data Validation rules for the defined user categories with access rights. The functional testing should be conductedfollowing black box approach and using end-to-end user scenarios.

Application Security Testing

The test is conducted to unearth various application security vulnerabilities, weaknesses and concerns related to Data /Input Validation, Authentication, Authorization /Access Control, Session Management, Error Handling, Use of Cryptography, etc. Typical issues which may be discovered in an application security testing include Cross-site scripting, Broken ACLs/Weak passwords, Weak session management, Buffer overflows, Forceful browsing, Form/hidden field manipulation, Command injection, SQL injection, Cookie poisoning, Insecure use of cryptography, mis-configurations, published vulnerabilities, errors triggering sensitive information leak etc. OWASP (Open Web Application Security Project) guidelines shall beused for the testing.

Application AccessibilityTesting (if relevant)

The accessibility of the eProcurement site, if required to be evaluated, then the same will be conducted as per the checklist given in Annexure-iii

Data Layer

Data Storage Security Audit

This aspect of assessment is conducted to ensure the use of standard and strong cryptography while storing the sensitive data and user credentials in the application or associated database.

Data Communication Security Audit

This aspect of assessment is conductedto ensure that secure communication channel like SSL, TLS or equivalent is used for transmission of sensitive data and credentials by the e-procurement system. The cryptographic algorithms and the key size implemented by the system should be standard, strong and compliant with the IT ACT and the CVC guidelines.
It is recommended that the complete data transmission to and from the e-procurement website should be SSL/ TLS enabled.

3.0 Evaluation and Certification Process

APPLICATION LAYER:

- **Request for Conformity Assessment indicating scope etc**.: The solution provider/service provider or user of the EPS will make the formal request to STQC by submitting the application form.Application form will be assigned a number and will be forwarded to lab for test/ evaluation of e-Procurement system

- **Submission of Functional, Application Security Reports from independent third party Test laboratory :** The solution provider/service provider or user of the EPS will submit the test report for functional testing (black box), application security from third party test agency [ERTL(E), ERTL(N), ETDC (Hyd), ERTL(S), ETDC (Bg), ETDC (Ch) etc. of STQC approved ITTL]. If the test reports submitted for assessment are fromNon-STQCLaboratory, then auditors / assessors shall carry out a sample audit /repeat test for functional aspect and sample security test.However, the reports from the agencies other than STQC Laboratory /STQC approved ITTL are not acceptable.

- **Submission of compliance report against CVC, GFRor any other applicable purchase guideline, IT Act:**These compliances will be verified by the auditors.

INFRASTRUCTURE LAYER:

- **Submission of Vulnerability Assessment (Server, Network devices), Penetration Testing and performance testing report**: The solution provider/service provider or user of the EPS will submit the test report for VA/PT form independent third party Test laboratory [ERTL(E), ERTL(N), ETDC (Hyd), ERTL(S), ETDC (Bg), ETDC (Ch) etc. of STQC approved ITTL]. If the test reports submitted for assessment are from Non-STQC Laboratory, then a sample audit /repeat test forSecurity vulnerabilities, performance testing and Penetration Testing will be carried out by the Auditors /Assessors.However, the reports from the agencies other than STQC Laboratory /STQC approved ITTL are not acceptable.

PROCESS & DATA LAYER

- **Security Audit of stored data, Communication:**Verification of valid certificate of ISO 27001 for hosting infrastructure.

- **Sample Process audit as per ISO 27001:**Audit of development facility as per some specific controls.

- Hash value of the complete application or any other data in support if unique integrity of the application code

- Audit of CM System

Conformity Assessment

- **Evaluation of the reports (Functional, Security, Performance, etc.):** These test reports pertain to the EPS deployed at target hardware/software

- **Evaluation of Compliance reports (CVC, GFR & IT Act):** Compliance of deployed EPS

- **Evaluation of Audit reports (Process) :**Analysis of ISO 27001 certificate, audit report of development facility which include configuration management system, relevant control of ISO 27001 and SLA, if any.

- **Review of Assessment Report and issue of Statement of Conformity.**

  Note: If there are multiple instances of the EPS with or without customization then single certificate will be issued by mentioning the names of all the intended users, provided suitable objective evidences available that there is no change in the business rule across the intended users.

4. Periodicity of certificate, Re-assessment and withdrawal criteria

The conformity assessment certificate will be issued for three years. Before the completion of the one year the service provider/ user/ developer will resubmit the EPS for surveillance, the conditions for surveillance and Re-assessment are as under:

Surveillance (at the end of 1st and 2nd year)

1) In case of changes resulting in significant impact in functionalities and /or security functionalities of the software, full testing/ audit shall be conducted like the initial certification and corresponding charges shall be levied.

2) In case of no significant changes in functionalities and/or security functionalities of the application, a declaration is to be submitted by client; only software security testing of the relevant software modules within the scope (e.g. e-Tendering, e-Auction etc.), Vulnerability Assessment of servers & Network devices including network architecture and deployment review, Penetration Testing and the Compliance Verification shall be conducted and corresponding charges shall be levied accordingly.

Re-Certification (To be carried before the expiry of 3 years of Certification Validity)

During Recertification of the e-Procurement application/System, Complete re-testing of the solution shall be conducted like the initial certification by STQ C and corresponding charges shall be levied accordingly.

- Audit of the software to verify no changes from previous version (Not complete testing)
- Application Security testing
- Vulnerability Assessment (Servers & Network Devices)
- Penetration Testing of the Application System from Internet.Performance testing
- Process audit

Withdrawal of certificate: The certificate of conformance can be withdrawn in the following scenarios:

1. Change in software or deployedinfrastructure within the validity period.
2. Complaint received from the user of the Certified eProcurement application /system service that the sanctity of the eProcurement Application /system has been compromised and the same is established and the service provider is unable to justify for the same.

Show cause notice will be issued to the service provider to explain the reasons. If reply found non-satisfactory, then the certificate can be put on abeyance or suspended for rest of the validity period.

Annexure-I -CVC Guidelines

S. No	Security Considerations	Compliance Status
1.	Whether the application is secure from making any temporary distortion in the electronic posing of tender notice, just to mislead certain vendors?	
2.	If yes at 2 above, then whether any automatic systems alert is provided in the form of daily exception report in the application in this regards?	
3.	Whether application ensures that the tender documents issued to/downloaded by bidders are complete in shape as per the approved tender documents including all its corrigendum?	
4.	Is there any check available in the application to detect and alert about the missing pages to the tenderer, if any?	
5.	Whether application ensures that all the corrigendum issued by the Competent Authority are being fully communicated in proper fashion to all bidders including those who had already purchased/downloaded the bid documents well ahead of the due date and before uploading the corrigendum?	
6.	Whether system is safe from sending discriminatory communication to different bidders about the same e-tendering process?	
7.	Whether e-procurement solution has also been customized to process all type of tenders viz Limited/Open/Global Tenders?	
8.	Whether online Public Tender opening events feature are available in the application?	
9.	Whether facilities for evaluation/loading of bids, strictly in terms of criteria laid down in bid documents are available in the application?	
10	Whether sufficient safeguards have been provided in the application to deal with failed attempt blocking?	
11	Whether application is safe from submission of fake bids?	
12	Whether encryptions of bids are done at clients end?	
13	Whether safety against tampering and stealing information of submitted bid, during storage before its opening is ensured?	
14	Whether application is safe from siphoning off and decrypting the clandestine copy of a bid encrypted with Public key of tender opening officer?	
15	Whether application is safe from multiation/sabotage of otherwise rendering the encrypted bid in the e-tender box during storage, to make it unreadable/invalid in any form, before opening of the bids?	
16	Whether introduction of special characters/executable files etc by users are restricted in the application?	

17	Whether validity check of DSC is being done at server end?	
18.	Whether system supports the feature that even though if a published tender is being deleted from the application, does not allow permanent deletion of the published tender from the Database?	
19.	Whether sufficient security features are provided in the application for authentication procedure of the system administrator like ID, password, digital signature, biometric etc.	
20.	Whether audit trails are being captured in the application on media not prone to tampering, such as optical write once?	
21.	Whether log shipping featuring available, where a separate dedicated server receives the logs from the application over web service in real time?	
22.	Whether integrity and non-tampering is ensured in maintaining the server clock synchronization and time stamping?	
23.	Whether application generates any exception report/system alerts etc to indicate the resetting of the clock, in case the application for time stamping is killing at the server level and time is manipulated?	
24.	Whether application ensures that the quotes from various bidders with their name are not being displayed to any one including to the organization during carrying out of the e-reverse auctioning process?	
25.	Whether application is fit for usage complying with the requirements of tender processing viz authenticity of tender, non-repudiation and secrecy of information till the actual opening of tenders	
26	Whether any comprehensive third party audit (as per statutory requirement and also as per the requirements of e-tender processing (compliance to IT Act 2000) was got conducted before first putting it to public use?	
27	Whether application complies with the Commission/s Guidelines dated 17.9.2009 on Security consideration for e-procurement systems	

Security Infrastructure level:

S. No	Security Issue	Best Practices to Achieve the security Considerations	Compliance Status
1.	Perimeter Defence	Deployment of routers, firewalls. IPS/IDS, Remote Access and network segmentation.	
2.	Authentication	Network authentication through deployment of password policy for accessing the network resources. To minimizeunauthorised access to the e-procurement system, at system level.	
3.	Monitoring	Deployment of logging at OSI network level and monitoring the same.	

4.	Secure configuration of network host.	The security of individual servers & workstations is a critical factor in the defence of any environment, especially when remote access is allowed workstations should haveSafeguards in place to resist common attacks.	
5.	System patching	As the vulnerability of the system is discovered almost regularly and the system vendors are also releasing the patches, It is expected that the host are patched with latest security updates.	
6.	Control of Malware	Suitable control like anti-virus, anti spyware ext. should be deployed on the host associated with e-procurement system. However, option for running the services at non-privileged user profile may be looked for. Otherwisesuitable operating system which is immune to virus, Trojanand malware may be deployed.	
7.	Structured cabling	The availability of the network services is critically dependent on the quality of interconnection between thehosts through structured including termination & marking. It is expected the e-procurement system has implemented structured cabling and other controls related with network and interconnection.	

Security at Application level:

S. No	**Security Issue**	**Best Practices to Achieve the security Considerations**	**Compliance Status**
1.	Authentication	The authentication mechanism of the e-procurement application should ensure that the credentials are submitted on the pages that are served under SSL	
2.	Access Control	The application shall enforce proper access control model to ensure that the parameter available to the user cannot be used for launching any attack.	
3.	Session management	The design should ensure that session tokens are adequately protected from guessing during an authenticated session.	
4.	Error handling	The design should ensure that the application does not present user error messages to the outside world which can be used for attacking the application.	
5.	Input validation	The application may accept input at multiple points from external sources, such as users, client applications, and data feeds. It should perform validation checks of the syntactic and semantic validity of the input. It should also check that input data does not violate limitations of underlying or dependent components, particularly string length and	

		character set. All user-supplied fields should be validated at the server side.	
6.	Application logging and monitoring	Logging should be enabled across all applications in the environment. Log file data is important for incident and trend analysis as well as for auditing purposes. The application should log failed and successful authentication attempts, changes to application data including user accounts, serve application errors, and failed and successful access to resources	

Security during application deployment & Use:

S. No	Security Issue	Best Practices to Achieve the security Considerations	Compliance Status
1.	Availability Clustering Load balancing	Depending on the number of expected hits and access the option for clustering of servers and load balancing of the web application shall be implemented	
2.	Application and data recovery	Suitable management procedure shall be deployed for regular back-up of application and data. The regularity of data backup shall be in commensurate with the nature of transaction/ business translated into the e-procurement system.	
3.	Integrity of the Application, Control of source code. Configuration management	Suitable management control shall be implemented on availability of updated source code and its deployment. Strict configuration control is recommended to ensure that the latest software in the production system.	

Security in Data storage and communication:

S. No	Security Issue	Best Practices to Achieve the security Considerations	Compliance Status
1.	Encryption for data storage	Sensitive data should be encrypted or hashed in the database and file system. The application should differentiate between data that is sensitive to disclosure and must be encrypted, data that is sensitive only to tampering and for which a keyed hash value (HMAC) must be generated, and data that can be irreversibly transformed (hashed) without loss of functionality (such as passwords). The application should store keys used for decryption separately from the encrypted data.	

2.	Data transfer security	Sensitive data should encrypted prior to transmission to other components. Verify that intermediate components that handle the data in clear-text form, prior to transmission or subsequent to receipt, do not present an undue threat to the data. The application should take advantage of authentication features available within the transport security mechanism. Specially, encryption methodology like SSL must be deployed while communicating with the payment gateway over public network.	
3.	Access control	Applications should enforce an authorization mechanism that provides access to sensitive data and functionality only to suitably permitted users or clients. Role-based access controls should be enforced at the database level as well as at the application interface. This will protect the database in the event that the client application is exploited. Authorization checks should require prior successful authentication to have occurred. All attempts to obtain access, without proper authorization should be loggedConduct regular testing of key applications that process sensitive data and of the interfaces available to users from the Internet include both "black box" informed" testing against the application. Determine if users can gain access to data from other accounts.	.

(ITACT 2000 and Amendment 2008) –Annexure-II

Sl. No.	Issues to be Checked	Compliance Status
1	Electronic Signature Implementation: i) ESC (Electronic Signature Certificate) used for the e-Procurement System by the users are Issued by CC (Certifying Authority) recognized by Govt. of India CCA (Controller of Certifying Authority). ii) The private key or the signature creation data should not be stored in the e-Procurement System or kept under the control of the e- Procurement Service Provider. iii) By the use of a public key of the subscriber/ signer, it should be possible to verify the electronic record. This may be read in conjunction with Sch-2, 13 85B(2)(b) "except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature". (Explanation: This implies that important electronic records of an e-procurement application, like – Tender Notice, Corrigenda, Tender Documents, Addenda, Clarifications to Tender Documents, Bids, etc should not only be electronically signed, there should also be provision in the e-procurement application to verify the electronic signatures). iv) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure (Explanation: There should be no limitation in the functionality of the e-procurement system which may necessitate for the tendering processes to continue uninterrupted that the private key of any officer be handed over to anybody else (who may be absent or unavailable), or where a private key is shared by multiple users due to any reason such as – absence of detailed hierarchy within a user organization, or multiple users of a group using a common key. v) Similarly, functionality of the e-procurement system should cover other aspects outlined in various sections (specified in the adjacent column) of the IT Act vi)	
2	Electronic Document & Record Control: Suitable controls are established for electronic documents / records generated, processed, stored, disposed of by the e-Procurement System to comply i) The information contained in e- Documents/e-Records remains accessible/usable for subsequent reference; ii) The e-Records are retained in the original format, it was generated, to accurately demonstrate how it was generated/sent/received. iii) The e-Records should be maintained with identification of origin, destination, date and time of dispatch or receipt. iv) The retention period of the e-Records should be compliant with the legal and contractual requirements.	

3	Data Protection: i) Adequate and reasonable security practices and procedures are in place to protect confidentiality and integrity of the users data and credentials ii) The e-procurement system has to satisfactorily address the above) through suitable functionality built into the e- procurement application. Where, in addition, some issues are being further addressed through organizational procedures, these should be explicitly defined with satisfactory explanations. The reasonable security practices and procedures followed should be documented in line with the international standard ISO/IEC 27001.	
4	Due diligence exercise: i) The Service Provider shall publish the terms and conditions of use of its e-Procurement System, user agreement, privacy policy etc. ii)The Service Provider shall notify users not to use, display, upload, modify, publish, transmit, update, share or store any information that: (a) belongs to another person; (b) is harmful, threatening, abusive, harassing, blasphemous, objectionable, defamatory, vulgar, obscene, pornographic, pedophilic, libelous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever; (c) harm minors in any way; (d) infringes any patent, trademark, copyright or other proprietary rights; (e) violates any law for the time being in force; (f) discloses sensitive personal information of other person or to which the user does not have any right to; (g) causes annoyance or inconvenience or deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature; (h) impersonate another person; (i) contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer resource; (j) Threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any other nation. iii) The Service Provider shall not itself host or publish or edit or store any information or shall not initiate the transmission, select the receiver of transmission, and select or modify the information contained in the transmission as specified in (ii) above. iv) The Service Provider shall inform its users that in case of non-compliance with terms of use of the services and privacy policy provided by the Service Provider, it has the right to immediately terminate the access rights of the users to the e-Procurement System. v)The Service Provider shall publish on the e- Procurement website about the designated agent to receive notification of claimed infringements.	

Annexure-iii

Accessibility Checkpoints (if applicable)

Checkpoint No.	Details
1.	All non-text content (like images) has a text alternative that provides equivalent information as the image itself.
2	Scanned Images of text have not been used.
3	The visual presentation of text and images of text has a contrast ratio of at least 4.5:1 between the foreground and background. Large scale text and images of text have a contrast ratio of 3:1.
4	Text can be resized without assistive technology up to 200 percent without loss of content or functionality.
5	There is a mechanism to pause, stop or hide scrolling, blinking or auto updating content that starts automatically and lasts for more than 5 seconds.
6	Web pages do not contain any content that flashes for more than three times in a second.
7	Instructions provided for understanding and operating content do not rely solely on sensory characteristics such as shape, size, visual location, orientation, or sound.
8	Color is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.
9	Captions or transcript are provided for all prerecorded and live audio and video content.
10	For any audio on a Web page that plays automatically for more than 3 seconds, a mechanism is available to pause, stop or control the volume of the audio independently by from system volume level.
11	Information, structure, and relationships that are conveyed visually on a web page must also be programmatically determined or are available in text.
12	When the sequence in which content is presented affects its meaning, a correct reading sequence can be programmatically determined.
13	All functionality that is available on the web page is operable through keyboard.
14	Complete web page is navigable using keyboard only (using tab or arrow keys).
15	Current navigation location (Keyboard focus indicator) is visible on the webpage while operating or navigating the page through a keyboard.
16	Web pages allow the user to bypass blocks of content like navigation menus that are repeated on multiple pages (by using the skip to content link).
17	Any web page within the website is locatable either through “search” or a “sitemap”.
18	Navigational mechanisms that are repeated across the website occur in the same relative order on each page.
19	If a webpage can be navigated sequentially and the navigation sequence affect the meaning of operation, then all components must receive focus in the same meaningful sequence (Creating a logical tab order through links, form controls, and objects).
20	The purpose of each link is clear.
21	Time limit for time dependent web functions is adjustable by the user.
22	Complete & self-explanatory title that describes the topic and purpose of the page has been provided.
23	Headings wherever used, correctly describe topic or purpose of content.
24	Language of the complete web page has been indicated. If there is a change in language within a webpage it also indicated.
25	Nomenclature of components that have the same functionality is uniform across the

	website.
26	When any component on the web page receives focus or its settings are changed it does not initiate change in context.
27	Changing the setting of any user interface components does not automatically cause a change in context.
28	If an input error is detected, the item is identified and the error is described to the user in text. Suggestions for correction if known are provided to the user.
29	Labels or instructions have been provided wherever input from the users is required.
30	For Web pages that cause legal commitments or financial transactions a mechanism is available for reviewing, confirming, and correcting information before finalizing the submission.
31	Web Page uses markup language as per specification.
32	Name and Role of all interface components can be programmatically determined.