Standard Security Requirements for IT RFPs

Title	Standard Security Requirements for IT RFPs			
Description	The purpose of this document is to define standard security requirements that can be utilized by organizations designing RFPs for procurement of IT products, services or support.			
Version Number	**Created By**	**Reviewed By**	**Date Modified**	**Date Reviewed**
1.0	Ms Vibha Chakrala Project Manager, CySecK	Mr Karthik Bappanad Centre Head, CySecK	20 Jan 2021	22 Jan 2021

Contents

..... 2

General Security Requirements 3

Privacy & Confidentiality 3

Application Development 4

Incident Response 4

Audit & Inspection 4

System Configuration & Maintenance 4

Annexure 1 – Non-Disclosure Agreement for Vendors 5

Annexure 2 – Non-Disclosure Agreement for Bidders 10

About CySecK.....14

General Security Requirements

- Bidder must have security controls in place to protect sensitive and/or confidential information shared with the vendor.
- Bidder must ensure that any agent, including a vendor or subcontractor, to whom <Organization Name> provides access to information systems, agrees to implement reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability of the information systems.
- Bidders must not copy any <Organization Name> data obtained while performing services under this RFP to any media, including hard drives, flash drives, or other electronic device, other than as expressly approved by <Organization Name>
- All personnel who will be part of this engagement deployed at <Organization Name> premises will need to adhere <Organization Name>'s security policy.
- All personnel who will be part of this engagement will need to sign NDA with <Organization Name>.
- Bidder must carry out Background checks which includes Address, Education, past employment and criminal checks for all personnel that will be deployed at <Organization Name> for the implementation.
- Bidder must disclose the origin of all software components used in the product including any open source or 3rd party licensed components.
- <Organization Name> holds the rights to conduct periodic Security Risk Assessment either remotely or onsite at the Bidder's office location(s). The security requirements for Bidder mentioned in these sections will be evaluated during the Security Risk Assessment. Any gaps identified during this Security Risk Assessment that can result in a security risk to <Organization Name> shall be remediated by the Bidder at no additional cost.
- The solution proposed by the Bidder must have the ability to support encryption of sensitive/confidential information
- The Bidder must ensure that the execution of the contract, including the solution must be in compliance with all applicable legal and regulatory requirements.
- The Bidder must have a valid ISO27001:2013 certificate issued by an authorized independent third-party auditor.

Privacy & Confidentiality

- The Bidder shall treat all Information obtained as part of this procurement and any subsequent contract as Confidential Information must hold Confidential Information in strict confidence and not disclose it to any third parties nor make use of such data for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon.
- The Bidder shall protect and secure all confidential Information in transit (collected, copied and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer.
- The Bidder shall not copy any <Organization Name> data obtained while performing services under this RFP to any media, including hard drives, flash drives, or other electronic device, other than as expressly approved by <Organization Name>
- The Bidder shall maintain all copies or reproductions of Confidential Information with the same security it maintains the originals. At the point in which the confidential Information is no longer useful for its primary or retention purposes, as specified by <Organization Name>, Bidder must destroy such data, making it unusable and unrecoverable.
- The Bidder shall maintain and use all information only for the purposes of the Contract/Agreement and only as permitted by <Organization Name>

- Any disclosure of any information to such of their employees, agents need to be strictly on a “need to know” basis.
- The Bidder shall only make copies as specifically authorized by the prior written consent of <Organization Name> and with the same confidential or proprietary notices as may be printed or displayed on the original.
- The Selected Bidder shall be required to sign a Non-Disclosure Agreement within 15 days of issuing the purchase order/notification of award.

Application Development

- Bidders shall have a comprehensive secure development lifecycle system in place consistent with industry standard best practices, including policies, training, audits, testing, emergency updates, proactive management, and regular updates to the secure development lifecycle system itself.
- Code for Applications that handle Confidential Information must comply with Secure Coding Standards.
- All developers deployed for developing the work in scope must have undergone training in secure coding.
- Bidder must review and test all application code for security weaknesses and backdoors prior to deployment with <Organization Name>.
- All security findings and exploitable vulnerabilities must be resolved before the application is released. Any exception to this will only be with the approval of the CISO of <Organization Name>.

Incident Response

- <Organization Name> must be notified in writing within 24 hours of the earliest indication or report of a potential breach or unintended disclosure of Confidential Information or a System belonging to <Organization Name>.
- Response to incidents that might affect Confidential Information or Systems must be conducted quickly and with ample resources. Bidder must hire a professional third-party incident response team if inhouse resources do not have sufficient skill or availability.
- <Organization Name> shall have the right to view all incident response evidence, reports, communications and related materials upon request.
- If requested by the <Organization Name>, or if required by law, the Bidder shall notify in writing all persons affected by the incident, at its own cost and expense.

Audit & Inspection

- Bidders must engage an independent third party annually to assess the practical security of Bidder's systems. These reviews must include penetration tests from the perspective of an external attacker and an internal user with common and administrative privileges. The penetration tests must include all Systems exposed to the internet and any Systems, internal or external, that handle Confidential Information. Such annual assessment shall be at Bidder’s sole expense.

System Configuration & Maintenance

- All operating systems, servers, software and network devices that are included in the scope must be kept hardened and patched.
- Bidders must maintain technical best security practices configuration guidelines for all such systems and update them at least annually.
- All security-related patches must be installed on systems within defined timeframe.

Annexure 1 – Non-Disclosure Agreement for Vendors

To be signed with selected vendor post bid selection

Mutual Non-Disclosure Agreement

This Mutual Non-Disclosure Agreement (this "**Agreement**"), with an effective date of 24 Dec 20XX, is made between Organization A ("**Abbreviation"**) and the organization identified as Organization B ("**Abbreviation**") (each a "Party" and collectively, the "**Parties**").

WHEREAS both the Parties herein wish to pursue discussions and negotiate with each other for the purpose of entering into a potential business arrangement in relation to [Please fill in details of proposed transaction] ("**Proposed Transaction**");

AND WHEREAS the Parties contemplate that with respect to the Proposed Transaction, both the Parties may exchange certain information that is confidential and proprietary either during the discussions or during the course of the business relationship (hereinafter referred to as "Confidential Information", more fully detailed in clause 1 herein below) and

AND WHEREAS, each Party wishes to review such Confidential Information of the other for the sole purpose of determining their mutual interest in engaging in the Proposed Transaction;

In connection with the above, the parties hereby agree as follows:

1. **Confidentiality**.
    a. For purposes of this Agreement, "Confidential Information" means and includes all information or material that has or could have commercial value or other utility in the business in which Parties are engaged and any data or information that is proprietary to the Parties and not generally known to the public, whether in tangible or intangible form, whenever and however disclosed, including, but not limited to:
    b. Any Trade Secrets, Proprietary documents, business plans, process, structure or practices;
    c. Any marketing strategies, plans, financial information, or projections; operations, sales estimates, business plans and performance results relating to the past, present or future business activities of such party, its affiliates, subsidiaries and affiliated companies;
    d. Any information related to the cost of project execution or delivery of service;
    e. Plans for products or services, and client or partner lists;
    f. Any algorithm, software, design, process, procedure, formula, source code, object code, flow charts, databases, improvement, technology or method;
    g. Any concepts, reports, data, know-how, works-in-progress, designs, development tools, specifications;
    h. Any invoices, bills, e-mail communications, mobile text communications, and any other communication related to the projects, products or services undertaken by either of the Parties for the other Party or on the behalf of the other Party or its vendors;
    i. Any other information that should reasonably be recognized as confidential information of the other Party.

j. Confidential Information need not be novel, unique, patentable, copyrightable or constitute a trade secret in order to be designated Confidential Information. The Parties acknowledge that the Confidential Information is proprietary to the other Party, has been developed and obtained through great efforts by the Party and that Parties regard all of their Confidential Information as trade secrets.
k. The Parties shall use the Confidential Information solely for and in connection with the Purpose.
l. Notwithstanding any other provision of this Agreement, the Parties acknowledge that Confidential Information shall not include any information that:
m. Is or becomes legally and publicly available to either Party without breach of this Agreement;
n. Was rightfully in the possession of either Party without any obligation of confidentiality; or
o. Is disclosed or is required to be disclosed under any relevant law, regulation or order of court, provided the other Party is given prompt notice of such requirement or such order and (where possible) provided the opportunity to contest it, and the scope of such disclosure is limited to the extent possible.

2. No Warranty.

The Parties acknowledge that, as between the Parties, the Discloser retains all right, title and interest in and to the Confidential Information and no license is granted or implied by the disclosure of Confidential Information to the Receiver hereunder. The Confidential Information is disclosed "as is" and no representation, warranty, or obligation with respect to the accuracy or completeness of the Confidential Information is made or undertaken by the Discloser.

3. No Waiver. The Parties agree that a failure to enforce any of the provisions of this Agreement will not constitute a waiver.

4. Non - Disclosure

a. The Parties shall use the Confidential Information only for the Purpose and not disclose any or part or summary or extract of the Confidential Information to any third party, including third parties affiliated with the other Party, without that Party's prior written consent, which prior consent the Party may refuse to give without assigning any reasons.

b. The Parties shall hold and keep in strictest confidence any and all Confidential Information and shall treat the Confidential Information with at least the same degree of care and protection as it would treat its own Confidential Information.

c. Either Party shall not copy or reproduce in any way (including without limitation, store in any computer or electronic system) any Confidential Information or any documents containing Confidential Information without the Party's prior written consent.

d. The Party shall immediately upon request by the other Party deliver to the Party owning the Confidential Information that has been disclosed to the other Party, including all copies (if any) made in terms of these.

e. Either Party shall not commercially/non-commercially use or disclose any Confidential Information or any materials derived therefrom to any other person or entity other than persons in the direct employment of the other Party who have a need to have access to and knowledge of the Confidential Information solely for the Purpose as defined above, and such persons are under similar obligation of confidentiality and non-disclosure as these presents. In the event that any employees, agents or affiliates of either Party disclose or cause to be disclosed the Confidential Information, that Party shall be liable for such disclosure.

f. The Parties may not disclose Confidential Information to any third party under any circumstances regardless of whether the third party has executed a Non-Disclosure Agreement with the Party.

g. Both Parties agrees to notify the other Party immediately if it learns of any use or disclosure of the Party's Confidential Information in violation of the terms of this Agreement.

h. The Parties further acknowledge and agree that no representation or warranty, express or implied, is or will be made, and no responsibility or liability is or will be accepted by either Party, or by any of its respective directors, officers, employees, agents or advisers, as to, or in relation to, the accuracy of completeness of any Confidential Information made available to the other Party or its advisers; it is responsible for making its own evaluation of such Confidential Information.

i. During the term of this agreement, either Parties may use the association with the other Party only towards the purpose as envisaged under their business association under this Agreement.

5. **Return or Destruction of Confidential Information.**

a. Upon demand by the Discloser, the Receiver shall promptly destroy or return the Confidential Information and any copies thereof to the Discloser.

b. If destroyed upon the written consent of the Discloser, the Receiver shall certify in writing to the Discloser that all such Confidential Information, including all copies thereof, has been destroyed.

6. **Term and Survival.**

a. This agreement terminates _____ years after the Effective Date. The obligations of confidentiality will continue for a period of five years from the date of disclosure of Confidential Information.

b. Upon any demand made by either Party, the other Party shall immediately cease any and all disclosures or uses of Confidential Information, and at the request of the Party, shall promptly return or destroy all forms and copies of the Confidential Information in accordance with this clause and Section 6 of this Agreement.

c. The obligations of the Parties with respect to disclosure and confidentiality shall continue to be binding and applicable without limit in point in time except and until such information enters the public domain.

7. **Export.** The Parties acknowledge that Confidential Information may be subject to, and agree to comply with, the applicable export control laws and regulations of the Government of India.

8. **Governing Law and Jurisdiction.** This Agreement will be construed in accordance with the laws of India. Each party irrevocably submits to the exclusive jurisdiction of the courts of […..] India, for the adjudication of any dispute hereunder or in connection herewith.

9. **Remedies.**

a. The Parties acknowledge that the disclosure of Confidential Information in a manner not authorized by this Agreement or if either Party fails to comply with any of its obligations hereunder, the other Party may suffer immediate, irreparable harm for which monetary damages may not be adequate.

b. The Parties acknowledge that damages are not a sufficient remedy for the other Party for any breach of any of the Party's undertakings herein provided

c. Each Party agrees that the other Party may specifically enforce this Agreement and may seek such injunctive or other equitable relief as may be necessary or appropriate to prevent such unauthorized disclosure.

d. The parties acknowledge that the affected Party is entitled to, without limitation to the other rights guaranteed under this Agreement, to specific performance or injunctive relief (as appropriate) in addition to any other remedies available to the affected Party in law or in equity.

10. **Amendment.** This Agreement may be amended only by a written agreement executed by each of the Parties hereto. No amendment of or waiver of, or modification of any obligation under this Agreement will be enforceable unless set forth in a writing signed by the Party against which enforcement is sought. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable.
11. **Severability.** If any provision of this Agreement is deemed unenforceable or illegal, such invalidity shall not be deemed to affect any other provision hereof or the validity of the remainder of this Agreement, and such invalid provision shall be deemed deleted here from to the minimum extent necessary to cure such violation.
12. **Entire Agreement.** This Agreement constitutes the complete and exclusive statement of the terms and conditions between the Parties with respect to the subject matter hereof and supersedes all prior and contemporaneous oral or written agreements regarding this subject matter.
13. **Mandatory Disclosure.**
    a. In the event that the Receiver is requested or required to disclose any Confidential Information of the Discloser, the Receiver shall provide the Discloser with a written notice of any such request so that the Discloser may seek a protective order or any other appropriate remedy, or, waive compliance with the provisions of this Agreement.
    b. If the Receiver is legally compelled to disclose Confidential Information of the Discloser pursuant to such process, the Receiver may disclose only that portion of Confidential Information of the Discloser which the Receiver is legally required to be disclosed.
14. **Dispute Resolution**
    a. **Mediation** - The Parties agree to first mediate any disputes or claims between them in good faith and resolve the disputes amicably and share the cost of mediation equally.
    b. **Arbitration** - In the event that mediation fails, any controversy or claim arising out of or relating to this Agreement or breach of any duties hereunder shall be settled by Arbitration in accordance with the Arbitration and Conciliation Act of India, 1996. All hearings will be held in […..] India and shall be conducted in English. The parties shall each appoint an arbitrator who shall then appoint a sole arbitrator to preside over the Arbitration proceedings.

ORGANIZATION A

ORGANIZATION B:

By:

Name:

Title:

Address:

By:

Name:

Title:

Address:

Annexure 2 – Non-Disclosure Agreement for Bidders

To be shared by Bidders at the time of proposal submission

WHEREAS, we the undersigned Bidder, _____, having our principal place of business or registered office at _____, are desirous of bidding for RFP No. <<>> dated <<DD-MM-YYYY>> "**Title of RFP"** (hereinafter called the said 'RFP') to the "Organization Name", hereinafter referred to as '**Business Name'**

And,

WHEREAS, the Bidder is aware and confirms that <Business Name>'s business or operations, information, application or software, hardware, business data, architecture schematics, designs, storage media and other information or documents made available by <Business Name> in the RFP documents during the bidding process and thereafter, or otherwise (confidential information for short) is privileged and strictly confidential and/or proprietary to <Business Name>,

NOW THEREFORE, in consideration of disclosure of confidential information, and in order to ensure the <Business Name>'s grant to the Bidder of specific access to <Business Name>'s confidential information, property, information systems, network, databases and other data, the Bidder agrees to all of the following conditions.

It is hereby agreed as under:

1. The confidential information to be disclosed by the <Business Name> under this Agreement ("Confidential Information") shall include without limitation, any and all information in written, representational, electronic, verbal or other form relating directly or indirectly to processes, methodologies, algorithms, risk matrices, thresholds, parameters, reports, deliverables, work products, specifications, architecture, project information, security or zoning strategies & policies, related computer programs, systems, trend analysis, risk plans, strategies and information communicated or obtained through meetings, documents, correspondence or inspection of tangible items, facilities or inspection at any site to which access is permitted by <Business Name>.

2. Confidential Information does not include information which:

a. the Bidder knew or had in its possession, prior to disclosure, without limitation on its confidentiality;

b. information in the public domain as a matter of law;

c. is obtained by the Bidder from a third party without any obligation of confidentiality;

d. the Bidder is required to disclose by order of a competent court or regulatory authority;

e. Is released from confidentiality with the written consent of <Business Name>.

The Bidder shall have the burden of proving hereinabove are applicable to the information in the possession of the Bidder.

3. The Bidder agrees to hold in trust any Confidential Information received by the Bidder, as part of the Tendering process or otherwise, and the Bidder shall maintain strict confidentiality in respect of such Confidential Information, and in no event a degree of confidentiality less than the Bidder uses to protect its own confidential and proprietary information. The Bidder also agrees:

a. to maintain and use the Confidential Information only for the purposes of bidding for this RFP and thereafter only as expressly permitted herein;

b. to only make copies as specifically authorized by the prior written consent of <Business Name> and with the same confidential or proprietary notices as may be printed or displayed on the original;

c. to restrict access and disclosure of Confidential Information to their employees, agents, and representatives strictly on a "need to know" basis, to maintain confidentiality of the Confidential Information disclosed to them in accordance with this clause; and

d. To treat Confidential Information as confidential unless and until <Business Name> expressly notifies the Bidder of release of its obligations in relation to the said Confidential Information.

4. Notwithstanding the foregoing, the Bidder acknowledges that the nature of activities to be performed as part of the Tendering process or thereafter may require the Bidder's personnel to be present on premises of <Business Name> or may require the Bidder's personnel to have access to software, hardware, computer networks, databases, documents and storage media of <Business Name> while on or off premises of <Business Name>. It is understood that it would be impractical for

<Business Name> to monitor all information made available to the Bidder's personnel under such circumstances and to provide notice to the Bidder of the confidentiality of all such information.

Therefore, the Bidder shall disclose or allow access to the Confidential Information only to those personnel of the Bidder who need to know it for the proper performance of their duties in relation to this project, and then only to the extent reasonably necessary. The Bidder will take appropriate steps to ensure that all personnel to whom access to the Confidential Information is given are aware of the Bidder's confidentiality obligation. Further, the Bidder shall procure that all personnel of the Bidder are bound by confidentiality obligation in relation to all proprietary and Confidential Information received by them which is no less onerous than the confidentiality obligation under this agreement.

5. The Bidder shall establish and maintain appropriate security measures to provide for the safe custody of the Confidential Information and to prevent unauthorized access to it.

6. The Bidder agrees that upon termination or expiry of this Agreement or at any time during its currency, at the request of <Business Name>, the Bidder shall promptly deliver to <Business Name> the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Bidder or its Affiliates or directors, officers, employees or advisors based on the Confidential Information and promptly certify such destruction.

7. Confidential Information shall at all times remain the sole and exclusive property of <Business Name>. Upon completion of the Tendering process and or termination of the contract or at any time during its currency, at the request of <Business Name>, the Bidder shall promptly deliver to <Business Name> the Confidential Information and copies thereof in its possession or under its direct or indirect control, and shall destroy all memoranda, notes and other writings prepared by the Bidder or its Affiliates or directors, officers, employees or advisors based on the Confidential Information within a period of sixty days from the date of receipt of notice, or destroyed, if incapable of return. The destruction shall be witnessed and so recorded, in writing, by an authorized representative of <Business Name>. Without prejudice to the above the Bidder shall promptly certify to <Business Name>, due and complete destruction and return. Nothing contained herein shall in any manner impair rights of <Business Name> in respect of the Confidential Information.

8. In the event that the Bidder hereto becomes legally compelled to disclose any Confidential Information, the Bidder shall give sufficient notice and render best effort assistance to <Business Name> to enable <Business Name> to prevent or minimize to the extent possible, such disclosure.

Bidder shall not disclose to a third party any Confidential Information or the contents of this RFP without the prior written consent of <Business Name>. The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the Bidder applies to its own similar Confidential Information but in no event less than reasonable care.

For and on behalf of:

(BIDDER)

Authorized Signatory	Office Seal:
Name:	Place:
Designation:	Date:

About CySecK

CySecK is the Karnataka state government's K-Tech Centre of Excellence in Cybersecurity, housed in the IISc (Indian Institute of Science) campus, with IISc as the anchor institute and KSCST (Karnataka State Council for Science and Technology) as the implementation agency. CySecK was setup by KITS (Karnataka Innovation and Technology Society) of the Department of IT, BT and S&T.

The key objectives of the CoE are to promote a cyber-safe and conducive environment for industry collaboration, address skills gap, build awareness and foster innovation in the emerging technology field of cybersecurity. To achieve these objectives, the CoE has various outreach programme focused towards citizenry, technology community, industry and the state government.

We solicit support from cybersecurity experts in industry and academia to collaborate with us for our various initiatives. An overview of our various activities can be seen on our website at https://cs-coe.iisc.ac.in/.

You can get in touch with us through the following channels.

Email: ops.cyseck@karnataka.gov.in

LinkedIn: https://www.linkedin.com/company/cyseck/

Twitter: https://twitter.com/CySecKCoE

Website: https://cs-coe.iisc.ac.in/