

(On Company's Letter head)

Annexure-O

To,
The Dy. General Manager,
IT – Platform Engineering – II Department,
State Bank of India, Global IT Centre,
CBD-Belapur, Navi Mumbai

Dear Sir,

SELF CERTIFICATION

APPLICATION NAME: _____

I/We, _____ hereby declare that the Application _____ (developed)/(deployed) by us _____ (Name of organization) on _____ for SBI has followed all the security measures while developing.

Following secure source code related security aspects have been taken care of while developing the Application _____, version number _____:

| Sl. No. | Security Aspects | Remarks |
|---------|---|----------|
| 1 | Secure coding practices have been followed | Yes / No |
| 2 | Application was subjected to Source Code Review and patched against all known vulnerabilities including those defined under OWASP Top 10 and SANS 25, prior to handover to the Bank | Yes / No |
| 3 | No static details regarding Application (e.g. Default username, password) are mentioned in the code | Yes / No |
| 4 | Obfuscation of code has been done while putting the Application into production | Yes / No |
| 5 | Secure SDLC processes have been followed | Yes / No |
| 6 | Application was free from malware at the time of sale, free of any obvious bugs and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent Versions/modifications done) | Yes / No |
| 7 | The application is safe from potential bottlenecks and single points of failure vulnerable to DDoS attacks from source code perspective | Yes / No |

We also confirm that the Application version number _____
(to be deployed)/(deployed) in the Bank has been subjected to thorough Risk Assessment procedures with focus on Source code review by (Internal)/(External) Reviewers using :

a) _____ (Name of Source Code Review Tool) or

b) A Proprietary Source Code Review Tool developed by us

The last review was performed on ____/____/____ and observations have been duly closed with the following exceptions. The roadmap and the timeline for these exceptions are mentioned below:

| Timelines for Closure | Count of Observations | | | | | Total |
|-----------------------|-----------------------|------------------------|------------------------|-------------------------|-------------|-------|
| | Upto 3 months | > 3 months to 6 months | > 6 months to 9 months | > 9 months to 12 months | > 12 months | |
| High | | | | | | |
| Medium | | | | | | |
| Low | | | | | | |
| Informational | | | | | | |

We also undertake the responsibility to provide timely mitigation for any future vulnerability/zero-day vulnerability observed in the product or the underlying infrastructure that may impact the security assurances of the product.

Signature:

Name and Designation in the Organization
(to be signed by an officer of CIO/CEO rank)

Date:

Place:

