Checklist for *Secure Code Programming* in Applications

S.No.	Action Item(s)	Is implemented?
1	Implement CAPTCHA on all entry-forms in PUBLIC pages. Implement CAPTCHA or account-lockout feature on the login form. [Alpha-numeric CAPTCHA with minimum 6 characters]	☐ YES ☐ NO ☐ Not Applicable
2	Implement proper validations on all input parameters in client and server side (both). [White-listing of characters is preferred over Black-listing]	☐ YES ☐ NO ☐ Not Applicable
3	Use parameterized queries or Stored-procedures to query output from databases, instead of inline SQL queries [Prevention of SQL Injection]	☐ YES ☐ NO ☐ Not Applicable
4	Implement proper Audit/Action Trails in applications	☐ YES ☐ NO ☐ Not Applicable
5	Use different Pre and Post authentication session-values/Authentication-cookies	☐ YES ☐ NO ☐ Not Applicable
6	Implement proper Access matrix (Access Control List-ACL) to prevent un-authorized access to resources/pages/forms in website [Prevention of Privilege escalation and restrict in of access to authorized/authenticated content]	☐ YES ☐ NO ☐ Not Applicable
7	Do not reference components (such as javascripts,stylesheets etc.) directly third-party sites. [They may be downloaded and self-referenced in website]	☐ YES ☐ NO ☐ Not Applicable
8	Use third-Party components from trusted source only. [Components with known vulnerabilities are not recommended.]	☐ YES ☐ NO ☐ Not Applicable
9	Store critical data such as PAN number,Mobile Number,Aadhar Card number etc. in encrypted form in the database. [Hashing of sensitive information is preferred over encryption, unless required to be decrypted]	☐ YES ☐ NO ☐ Not Applicable
10	Prevent critical information from public access by any mean [Critical information like credit card number, account number, aadhar number etc. should be restricted to authorized persons only. If such information is stored in static files such as excel,pdf etc., sufficient measures should be taken so that is it not accessible to unauthorized persons or in public.]	☐ YES ☐ NO ☐ Not Applicable
11	Hash the password before it is relayed over network, or is stored in database. [During login, password should be salt-hashed using SHA-256/512. However, it should be stored as plain hash (SHA-256/512) in database. On every login attempt, new salt should be used, and it should be generated from server-side only]	☐ YES ☐ NO ☐ Not Applicable
12	Implement Change Password and Forgot password module in applications [not required in applications, using LDAP for authentication]	☐ YES ☐ NO ☐ Not Applicable
13	Comply with Password Policy, wherever passwords are being used.	☐ YES ☐ NO ☐ Not Applicable
14	Use Post methods to pass parameters as values from one-page/website to another. [GET methods should be avoided]	☐ YES ☐ NO ☐ Not Applicable
15	Implement proper error-handling. [System/application errors should not be displayed to viewer]	☐ YES ☐ NO ☐ Not Applicable

Application Security Division, Cyber Security Group
National Informatics Centre
A-Block, CGO Complex, Lodhi Road,
New Delhi - 110003

16	Implement token-based system that changes on every web-request in application, to prevent CSRF. [CSRF Guard or Anti-forgery tokens can be implemented in non-critical applications. Websites using payment-gateways etc. are categorized in critical websites.]	☐ YES ☐ NO ☐ Not Applicable
17	Do not implement File upload in public modules	☐ YES ☐ NO ☐ Not Applicable
18	Store uploaded files in database, rather than storing them in file-system [Files, stored in database cannot be executed directly, hence this is more secure than storing them in file system.]	☐ YES ☐ NO ☐ Not Applicable
19	Generate unique, un-predictable and non-sequential receipt numbers/acknowledgement numbers/application numbers/roll numbers/ File-names etc. It is preferable that strong algorithm be used to generate such numbers.	☐ YES ☐ NO ☐ Not Applicable
20	Implement proper Session Timeout [Logged-In user should be logged-out after a specific period(say 20 minutes) of inactivity]	☐ YES ☐ NO ☐ Not Applicable
21	Assure admin/Super-Admin URL's is/are accessible from restricted IP's only [For this, segregate public URL from Admin/Super-Admin module. Public modules and Admin/Super-Admin modules should be deployed on separate URL's. Admin/Super-Admin URL's should be accessible from restricted IP's only. It is preferable to allow access for Admin/Super-Admin modules through VPN]	☐ YES ☐ NO ☐ Not Applicable
Other Action Item(s)		
1	Assure third-Party links/page(partial/full) open in different tab, with a disclaimer.	☐ YES ☐ NO ☐ Not Applicable
2	Disable Trace/PUT/DELETE and other non-required methods in application/web-server.	☐ YES ☐ NO ☐ Not Applicable
3	Assure that Email addresses, where ever used, are in form of an image. [Alternatively, replace "@" with [at] and "." with [dot] in email addresses]	☐ YES ☐ NO ☐ Not Applicable
4	Disable directory listing	☐ YES ☐ NO ☐ Not Applicable
5	Set "Auto Complete" off for textboxes in forms	☐ YES ☐ NO ☐ Not Applicable
6	Prevent pages from being stored in history/cache. [Each time that the user tries to fetch a page, it should request server to serve with a fresh copy of the page]	☐ YES ☐ NO ☐ Not Applicable
7	Implement Logout buttons in all authenticated pages	☐ YES ☐ NO ☐ Not Applicable
Implementation Guidelines		
1	Restrict each application for minimum access (only required access) [Allow access of application for restricted network access. Websites, those are to be used in local-network, should not be accessible from any other network. For exceptional cases, VPN may be used. Websites, those are required to be accessed from within the country, should be restricted for access on Indian ISP's **ONLY**.]	☐ YES ☐ NO ☐ Not Applicable
2	Use the latest and non-vulnerable versions of Application Server (IIS/Apache etc.), Jqueryetc.	☐ YES ☐ NO ☐ Not Applicable
3	Enable audit-trails and system logs on server [e.g. :Web-Access logs, Application Logs, Security Logs etc.	

4	Take regular backups of data and application [Sufficient arrangements should be made to take proper and regular backups of database,application and other related objects/components, for retrieval on undesirable circumstances. It is preferable to maintain a set of last 5 backups. It is advised to store backups on hard-drive/tape-disks/SAN-storage. Networked servers/machines should be avoided for this activity]	☐ YES ☐ NO ☐ Not Applicable

For detailed checklist for developers and secure codingguidelines, visit:
https://security.nic.in/appsec_new.aspx?pid=114&id=118&index=2