CyberSafety Guidelines for Government Websites/Applications developing Vendors

INTRODUCTION

The citizens of the Goa state are using the Internet for business, education, finance and various applications and services including Digital Government services. Internet provides growth and innovation but at the same time it has seen rise in cybercrimes, user harm and other challenges to the online safety.

The policies of the Government are aimed at ensuring an Open, Safe & Trusted and Accountable Internet for its users. Government is fully cognizant and aware of the growing cyber security threats and attacks. It is Government's objective to ensure that Government service end users experience a Safe & Trusted Internet.

Along with ubiquitous applications of Information and Communication Technologies (ICT) in almost all facets of service delivery and operations, continuously evolving cyber threats have become a concern for the Government. Cyber-attacks can come in the form of malware, ransomware, phishing, data breach etc., that adversely affect an organisation's information and systems. Cyber threats leading to cyber-attacks or incidents can compromise the Confidentiality, Integrity, and Availability of an organisation's information and systems and can have far reaching impact on essential services and national interests.

To protect against cyber threats, it is important for government entities and its SDA/ vendors/contractors to implement strong cybersecurity measures and follow best practices. As ICT infrastructure of the Government entities is one of the preferred targets of the malicious actors, responsibility of implementing good cyber security practices for protecting computers, servers, applications, electronic systems, and data from digital attacks, also remain with the ICT assets' owner and its partners.

These Cyber safety guidelines for Government designated SDA/vendors/contractors have been prepared by Department of Information Technology, Electronics and Communications (DITE&C), Altinho – Goa using "**Guidelines for Information Security Practices for Government Entities**" document as a baseline/reference document compiled by Indian Computer Emergency Response Team (CERT-In) and National Informatics centre (NIC) with an objective to ensure security framework is followed/considered when Government designated SDA/vendors/contractors handles ICT Projects (Government Application / Service / Website development) for the Government Departments/Corporations/Autonomous Bodies.

The purpose of these guidelines is to establish a prioritized baseline for cyber security measures and controls to be followed by Government organisations and their associated SDA/ vendors/contractors. The guideline shall assist their security teams to implement baseline and essential controls and procedures to protect their Cyber infrastructure from prominent threats.

1. ACRONYMS

API	Application Program Interface
CERT-In	Indian Computer Emergency Response Team
DITE&C	Department of Information Technology, Electronics and Communications
GEL	Goa Electronics Limited
HTTPS	Hyper Text Transfer Protocol - Secure
ICT	Information and Communication Technology

IDOR	Insecure Direct Object Reference
NDA	Non-Disclosure-Agreement
NIC	National Informatics Centre
OWASP	Open Web Application Security Project
SBOM	Software Bill of Material
SDA	State Designated Agency (GEL)
SSL	Secure Sockets Layer
SQL	Structured Query Language
TLS	Transport Layer Security
VAPT	Vulnerability Assessment and Penetration Testing

2. APPLICATION SECURITY

2.1 The concerned SDA/vendors/contractors must incorporate security at each level of software/website/application development lifecycle such as during development, deployment and maintenance of application etc. to reduce vulnerabilities. During development secure coding practices should be followed. Testing should be conducted during development, deployment and maintenance of application/website/service.

2.2 Ensure privacy protection of citizen data at each stage of application life cycle.

2.3 The concerned SDA/vendors/contractors should ensure that the developed applications/websites address the Open Web Application Security Project (OWASP) top 10 vulnerabilities.

2.4 The concerned SDA/vendors/contractors must maintain an updated document containing the list of custodian(s) assigned to each application/service/website, level of criticality, version implemented, number of installed instances, application license details etc.

2.5 Authorization and access to applications/services should be based on role, affiliation and membership of group rather than individual basis. Periodic review of authorization should be performed by SDA/vendors/contractors in consultation with the concerned Government entity.

2.6 The concerned SDA/vendors/contractors in consultation with the NIC Cloud Authorities, Managed Service Provider for the cloud Services and concerned Government entity must identify ports, protocols and least privileged services required to carry out daily operations of applications/platforms and restrict or block all others.

2.7 Concerned SDA/vendors/contractors should ensure that applications/services validate the data on the server-side/Cloud.

2.8 Ensure that all Websites and Applications are “https” enabled with a valid SSL/TLS Certificate.

2.9 Ensure applications execute proper error handling and should not provide detailed system information, deny service, should not impair security mechanisms, or crash the system.

2.10 Application security testing, Vulnerability Assessment and Penetration Testing (VAPT), should be performed at a frequency determined by sensitivity of the information handled by applications/websites (at least once in a year or whenever there is change in application).

2.11 Implement measures for securing Application Program Interfaces (APIs). Include API security in Vulnerability Assessment and Penetration Testing and mitigate vulnerabilities in APIs.

2.12 Log monitoring on a continuous basis to be carried out with the ability to alert the operations team when a security anomaly is suspected.

2.13 Implement Integrity checks and disallow the binary from executing that does not confirm to the application/system security.

3. MOBILE APPLICATION SECURITY

3.1 The concerned SDA/vendors/contractors should ensure that their mobile applications address the Open Web Application Security Project (OWASP) Mobile Top 10 vulnerabilities.

3.2 The mobile application must implement SSL Pinning to prevent man-in-the-middle attacks.

3.3 No secret keys used by the application should be stored unencrypted in the application storage.

3.4 User data should not be stored in unencrypted/plain-text form on the device.

3.5 The final build of the application must not contain any test code and all debug logs must be disabled. Obfuscation of the code by packers, encryptors and related tools could be considered for preventing reversing the applications.

3.6 Only permissions required for essential functionality of the application should be sought from the user.

3.7 Sensitive data should be shared over secure SSL/TLS connection only.

3.8 Develop applications/services such that whenever data is accessed by an application/service, data is encrypted i.e. when data is at rest, data is in use and when data is in transit.

3.9 Review and change any default/weak/misconfigured settings with appropriate authentication & authorization controls for all database applications.

3.10 Audit and remediate vulnerabilities in applications on priority, which could cause data breaches/leaks that include Insecure Direct Object Reference (IDOR), SQL injection, Insecure API endpoints, Directory listing etc.

3.11 Implement Micro-segmentation for controlled granular access to database applications.

3.12 Backups should be made for application under development and data conversion efforts.

4. THIRD PARTY ACCESS AND OUTSOURCING BY GOVERNMENT ORGANISATIONS

4.1 Government organisation should ensure that third party access to information should be restricted and should only be shared after signing Non-Disclosure-Agreement.

4.2 Wherever any activity is outsourced or awarded as work contract to any 3rd party/vendor, it shall be ensured that the contract specifies the information security requirements, and the same are complied with, in addition to the regular contractual details.

4.3 The following information security requirements should be documented as part of the contract:

i. General policy on information security
ii. Procedures to protect organisational assets

iii. Restrictions on copying/disclosure
iv. Controls to ensure return of information/assets in their possession at the end of the contract
v. The right to monitor and the right to terminate services in the event of a security incident or a security breach
vi. Right to audit contractual responsibilities or to have the audits carried out by third parties
vii. Arrangements for reporting, notification and investigation of security incidents and breaches

4.4 Information security audit report of the concerned SDA/vendors/contractors to be made available to Procuring entity (Government organisation) on periodic basis or when required.

4.5 Detailed list of all components of the software (including open source)/solution in the form of Software Bill of Material (SBOM) shall be provided by the concerned SDA/vendors/contractors. They are also responsible for informing any identified vulnerabilities in the system to the Government organisation within reasonable time period.

4.6 Data collected and processed by the concerned SDA/vendors/contractors should be protected appropriately (cannot be shared with any others without explicit consent/agreement) and made available to the procuring Government entity as and when required.

4.7 Concerned SDA/vendors/contractors' personnel should comply with the information security policies, processes and procedures of the Government organisation.

4.8 Any concerned SDA/vendors/contractors found in violation to this policy shall be subjected to termination of contract and/or will be handled as per applicable laws, rules & regulations.