Chapter 7: Application Development and Security

1. In-principle approval shall be obtained from COIS for development of any new software/ applications/ Systems in case the Application shall be deployed across Division/ Corporation or shall require additional resources in terms of corporate network/ security/ licenses/ enterprise data.
2. Any Application development, for enterprise-wide application, should be done with approval of Divisional IS Head.
3. Application development should be done in a manner to provide seamless access from multiple devices such as mobile, desktop, tablets etc.
4. Development of mobile friendly version, of internet hosted application, like PWA (progressive web application) etc. should be considered while developing software applications.
6. The platform being used for hosting the application should have enterprise support. “End-of-life” for the same should be 5 years or more.
7. The licensing of the software being used for development needs to be in line with the licensing policy of the OEM.
8. For any application requiring data exchange to and from SAP, SDMS-CRM or any other enterprise -wide application, approval to be obtained from COIS prior to development of software application.
9. Information security shall be incorporated at each level of Software Development Lifecycle (SDLC) such as during requirement analysis, design, development, deployment, maintenance, and improvement.
10. Inventory shall be maintained for all application software developed in-house or out-sourced. The inventory shall contain the list of applications, level of criticality, version implemented, No. of installed instances, language,
platform, and license details.
11. The applications, whether in-house or out-sourced, shall be developed as per secure coding guidelines. For web applications, at least, latest Open Web Application Security Project (OWASP) guidelines shall be followed.
12. For all applications where sensitive data is getting stored, the source code shall be reviewed for vulnerabilities prior to deployment. This would be applicable to both internally and externally developed applications.
13. All applications developed for internal Users shall integrate with Active Directory to authenticate Users.
14. Applications shall have the capability to generate logs of exceptions, errors etc.
15. Changes to the application software during development and maintenance shall be controlled through formal change request form.
16. Vulnerability Assessment and Penetration Testing shall be conducted for all critical applications before deployment and thereafter as per GoI guidelines.
17. A version control system must be used to track and retain information about changes in the source code. The version control system should be able to describe the change, record who made the change, retain the date/time of change, retrieve past versions, and compare versions.
18. Development, quality, testing environment shall be separated from production environment.

Chapter 2: Network and Infrastructure

1. Physical Security: Network and infrastructure facilities shall be secured from any unauthorized access.
2. Redundancy: Critical infrastructure facilities shall be implemented with sufficient redundancy to meet availability requirements.
3. Inventory of Assets and Infrastructure: Inventory shall be maintained for all network and infrastructure devices. All the IT Resources shall be grouped and classified in accordance to the criticality of the information that they transmit, process or store.
4. Network Cabling: Structured cabling shall be used. All network cabling routes shall be documented.
5. Network Diagram: Network diagram shall be maintained. All changes to the network diagram shall be as per change management procedure.
6. Device Configuration: Device configuration for all critical devices shall be documented and reviewed periodically. Any change shall follow change management procedure.
7. Authentication, Authorization and Accounting shall be enabled for Core Switch, Router and Security Equipment.
8. Network Security: Network security shall be established in the data center by means of Perimeter security. At least firewall and IPS shall be in place. In addition, content filter, Gateway Anti-Virus, DDoS protection etc. may be considered as per the requirement.
9. Network Security Zones: Networks shall be divided into multiple network zones according to the sensitivity and criticality of the information or services in that zone. Different zones shall be securely interconnected.
10. Network Traffic Control: Network traffic to outside world shall be controlled by means of web security gateway, content filtering, firewall etc.
11. Network Time Synchronization: All Network, security and Infrastructure devices shall implement Network Time Protocol (NTP) to synchronize time with common source. The identified NTP server should synchronize the time with standard time source set to Indian Standard Time (IST).
12. IPV6 - All new network and infrastructure equipment shall be IPV6 compliant.
13. LAN and WAN 13.1. No leased line, MPLS VPN line, Internet line, Point to Point (P2P) communication link and similar such connectivity between locations can be provided without prior approval from COIS.
13.2. Based on the needs, line bandwidth enhancement or reduction requirements can be initiated by Divisions and sent to COIS for review and approval.
13.3. IP address scheme and allocation for LAN/WAN shall be governed by COIS.
13.4. A rate contract (RC) and agency of MPLS service for WAN shall be finalized by COIS for corporation’s requirement. Divisions shall utilize this RC for their requirement. For Division’s additional requirement, the same RC can be used with prior approval from COIS.
13.5. Default settings and passwords shall be changed before deployment of any network and security device. Password to be defined as per password policy.
13.6. Secure protocols like SSH, SSL or IPsec shall be used for remote access. Insecure communication protocols like telnet shall be disabled.
13.7. Unused ports and interfaces on devices shall be disabled.
13.8. Network equipment shall be configured to close inactive sessions.
13.9. Only approved routing protocols shall be used for WAN.
13.10. Device configuration shall be backed up at least once in a month and whenever there is a change in the configuration.