

SECURITY GUIDELINES

INFORMATION SECURITY MANAGEMENT SYSTEM FOR COMPUTERISATION OF LAND RECORD

1. PURPOSE & SCOPE:

The purpose of security initiative is to enlist the procedures and guidelines, which are required to establish basic Security framework for **Computerization of Land Records** in India. It is also envisaged to create and adopt an Information Security policy and standards for Land Records Information system domain.

Committee of Revenue Secretaries, Govt. of India that was given mandate to formulate the necessary Security framework for CLR domain deliberated in depth about it and is ready with its report. NIC has prepared a detailed base document (Annexure I) for security guidelines, which was subsequently presented to the members of the committee. Committee discussed the issues and concerns for physical, technical and administrative security vis-à-vis existing system. Security guidelines and report primarily covers the following:

- It aims to extend necessary guidance and standards to revenue departments regarding various IT-security related issues such as physical technical and administrative concerns, which needs to be addressed from implementation/operational perspective of Land Record Computerization at Tehsil (Revenue circle) level.
- ISO/IEC BS 17799 has been referred for cyber security standards. ISO –BS 17799 is internationally recognized security framework, which extensively deals with almost all security mechanism in terms of 127 controls. According to domain needs 60 security controls have been short listed out of these 127 controls for the purpose of security mechanism. Information security Management for LR domain also takes care of policy; planning; security methodology; procedures etc.
- Security audit and Risk assessment that are necessary constituents for reducing vulnerabilities.

- Important technological devices and methods to strengthen the security in operational workflow environment.
- Information for designers & developers of applications software and database, which should be taken into account by technology service providers.

2. REQUIREMENTS FOR BUILDING SECURITY FRAMEWORK FOR CLR DOMAIN:

As on today, there are several states, which are successfully implementing Computerization of Land Records and have also accorded it necessary legal sanctity. Prime focus of CLR scheme is to achieve comprehensive digital system of land records across the country. It is obvious that in such a scenario, it is very much required to create a security management for land record systems and documents, which are of significant value. *It may also be noted that without adequate physical and administrative security mechanism, reliable digital security is not possible.* In case of digital data, issues and concerns regarding Integrity and authentications of data needs to appropriately addressed. Necessary provision for backup, storage, archival of digital data is to be made to fit to the requirements of domain.

Extent of security management is directly dependent on risk assessment. It will be very difficult to determine the severity of the risk without any critical assessment study. If we take into account, case of total automation, it may be visualized that severity of impact of any damage to IT system will be very serious because of non-availability of manual system of records. Thereby it is very much required to emphasis upon security management to avoid any such eventuality.

In manual system of land records, procedures have been very clearly laid down for maintenance and security of records, accountabilities, roles of various functionaries. But same may not be case for computerized system. There may be very few states, which are incorporating desirable changes in land administration with regard to security. While we are working for total automation, it is also desirable that conventions and procedures needs to be properly modified keeping in view the requirements of digital environment. Legally valid digital signatures should be considered as substitute to conventional signatures.

3. RECOMMENDATIONS:

The report herewith is based on views and observations made by Committee members concerning various issues relating to Security:

- It was noted that existing manual system has various safeguards, descriptive procedures, roles and responsibilities, which constitutes State Land administrative manuals. It is necessary that while switching over to IT enabled system for LR, appropriate steps may be initiated to incorporate suitable provisions catering to the requirements for secured computerized environment

for Land Records. It is necessary to accord high priority to confidentiality; Integrity; availability of data, records, process and system.

- Committee observes that as on today, our security prime security concerns are relating to PHYSICAL as well as CYBER security. Accordingly, it is required to have a composite strategy for domain security.
- Committee is of opinion that there are several areas pertaining to physical; technological and administrative security that needs attention in existing scenario of computerized operations at Tehsil level.
- Security requirements are dynamic in nature. In order to build an appropriate security management system, it is necessary that each state should follow Security policy guidelines. Each state should create continuous mechanism to assess the risks and vulnerabilities; strengthen the security measures in terms of rules; procedures; responsibilities and technology.
- Committee understands that ISO/IEC BS 17799 is an internationally accepted standard, which could be used to define standard framework for Land Record domain. ISO/IEC 17799 standards covers various aspects regarding policy; review mechanism; risk assessment; Confidentiality, integrity needs for Information Security management system. It was agreed that ISO/IEC 17799 covers 127 security controls. All of these controls are not relevant for LR domain. Accordingly, NIC and DIT have enlisted relevant security controls from domain security perspective (Annexure II).
- Committee recommends that in order to strengthen the existing security provisions, following steps must be initiated:
 - Adoption of Security policy guidelines and regular audit of security of data; software and hardware.
 - Risk assessment for operational sites and incident management.
 - Budgetary allocation for accepted level of security provision.
 - Policy and procedures for backup of data and software for defined period.
 - Policy for access control for system and data and other resources.
 - Arrangement for physical security of digital infrastructure.
 - Technical updates for users and responsible officials are required.
 - Policy for Password; Confidentiality; Accountability and Availability of data and system is required.
 - Policy for hardware; software; system software configuration management.
 - Policy for data access over network and distribution.

- Provision; documented procedures for legal compliance and security.

3.1 Approach for Security Management & Information Security Management System:

Committee agreed that there is a need for uniformity in standards and protocols for security management among all the states. "ISMS" is an approach by which management can monitor and control information security to reduce the business risk to an acceptable level and ensure that security continues to fulfill their corporate; customer and legal requirements. Implementation of Security management requires that

- Security controls are still in place and are effective
- Residual risks are still acceptable
- Assumptions about threats remain valid.

The security measures may be taken up for smooth functioning of the land records application system. These security controls (Annexure II) will help in minimizing the risks of human error, theft, fraud or misuse of the facilities. These measures may be adopted to secure Confidentially and to maintain accountability, integrity of records/system. For this purpose, it will be needed to address the various issues concerning Physical and Cyber Security in LR domain. There are areas like Access Control; Security Awareness and training; System configuration; Data management etc.

The security guideline document provides detailed description of various security measures, which shall be adopted to reduce the risk and curtail the vulnerabilities.

Cyber security is ongoing process and it is desirable that security concerns should be resolved by a permanent mechanism.

3.2 Security Audit:

Security audit is an important aspect of our defense initiatives. Risk assessment; evaluation of threats; vulnerabilities improvises domain security environment. Keeping this in mind, Committee agreed that each state should create a security review mechanism and Incident management. Further, it is also recommended that a third party security audit should be carried out for each state. It may be suggested that NIC should take necessary steps to ensure the application software security. The major steps involved in LR Information system security are:

- a) System study
- b) Application Security audit
- c) Infrastructure audit for known vulnerabilities & configurations

The security audit should be carried out as per guidelines issued by Government of India in this regard.

It is necessary that approach should focus upon:

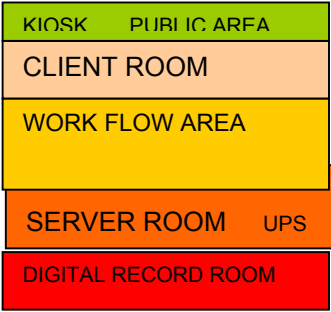
(i) At site of operation

- a. Physical security and access control at Taluk level, which is actual site of operation.
- b. System hardening and Incident detection /reporting at site of operation.
- c. Workflow authentication and non-repudiation and record management.
- d. Backup and Archival of data; software and records.
- e. Security updation; Version control and Configuration management

(ii) At State Level

- a. Steering committee to review the security of operations
- b. Incident management mechanism and support
- c. Technological and financial support
- d. Periodic reviews
- e. Coordination with vertical formations
- f. Steering committee to address various legal & policy issues emanating from routine experiences.

4. SUMMARY OF COST-ESTIMATES FOR RECOMMENDED TECHNICAL MEASURES FOR SECURED OPERATION AT TEHSIL LEVEL:

	Issues	Proposed Solutions
1	<p>Physical Security of the Site</p> <ul style="list-style-type: none">- Access Control- For Public- Work- flow area- Server Area- Client Area- Digital Record Room <p>Equipped with Access Control Device and Log Register</p>	 <p>Cost : Rs. 30,000.00*2 =60000 for two way access control for entry and exit and Construction of area as per specifications.</p>
2	<p>Electrical and Fire Safety</p>	<p>As per the fire safety and electrical devices. (Expenditure to be supported under site preparation fund)</p>

3.	LAN Connection <ul style="list-style-type: none"> - Server and Client - Wireless Device - Server and kiosk 	Protected connectivity to avoid interception of the client/server over/through LAN .Entire set-up should be within restricted access area. (No cost as of now. In future hub may be replaced with switch)
4	HARDWARE <ul style="list-style-type: none"> - Server - Clients - Printer - Scanner 	All the servers/client/printers/scanner and other equipments should be restricted and the configuration should be as prescribed . SI no of all these devices should be documented. Each m/c should be authenticated. It should be ensured that each site is having recommended configuration. Cost for providing hw is included in Hw funding.
5	System Software	Valid copy of OS should be used for installation of OS. The Hard Disk should be partitioned for the OS and data .The os should be installed in the Drive other then the default drive Funds for this is being given under s/w Allocation.
6	Password <ul style="list-style-type: none"> - Administrator - Default accounts - Guest accounts - BIOS level password - Bio Metric Thumb impression - Digital Signature(Digital Signature Certificate to authenticate server and client(with secure communication) may be taken from NIC 	<p>The administrator password should be of eight characters incorporating the special characters and alphanumeric. All guest and default accounts should be disabled. System should have BIOS password The user is accountable for keeping the password with himself. Only specified finger is to be used</p> <p>There will be nil expenditure in password maintenance. Funds for Biometrics are already allocated. DSC for each site may be acquired from NIC For Rs. 3600 per site for card readers (one for each m/c).</p>
7	Latest Updates of OS	Update the OS with latest updates. (Funds may be allocated under s/w)
8.	Virus and Intrusion Detection System <ul style="list-style-type: none"> - Disabling unwanted ports 	Update of vaccines with latest updates. Virus protection and provision of latest updates (Funds should be allocated in s/w category)
9.	Version Control <ul style="list-style-type: none"> - Key validation - Key revalidation with request 	<p>During installation the Land Record Application S/W will ask for the key, which is valid for a fixed duration.</p> <p>Duration is based on the version of the</p>

	- Same version of s/w at all sites	Land Record application s/w. Duration of the Land Record application s/w can be extended by request and keys granted by the administrator. One version at all sites.
10.	Disabling of Floppy Drive/Desktop - Desktop should be disabled	Floppy Drive may be disabled Application s/w should run directly at the system startup
11	Installation of Database - Certified copy - Database users password	SQL database should be installed using the authorized CD. "sa" should be password protected
12	Creation of LRC Users - Authentication and authorization - Role bases Access - Unused accounts	Authenticated users with password / biometrics. Role based authentication and function All unused accounts/guest should be disabled.
13	Backup/Restore of Database	Backup of database with password Backup Stored at different location Back under the custodian of the officer in charge System before shutdown must prompt for backup. (Cost for one high-end backup server should be considered under hw.)
14	Routine Check up of the System for unwanted s/w and games	Only authorized s/w should be installed in the server/client
15.	Use of LR s/w beyond schedule hours - Use of s/w on holidays - Use of s/w beyond working hours	Use of the computer center and application s/w beyond schedule hours should be recorded and permitted only on permission from competent authority.
16.	Security breaches log / report - Breaches of security - Unintended use of a module - Wok flow violation	Periodic Documentation of all breaches Periodic Report on workflow violation by users.
17.	Audit log	Periodic log will be kept separately in CD's with time stamp
18.	Backup of Application & Language s/w	LR s/w and Language Related Application s/w will be backed up in CD's with all keys.

In order to improve physical and IT security; backup of records, one time capital investment in tune of Rs. 0.60 Lakhs/Site will be required for physically setting the computer center and providing DSC. Further, technical support provider from concerned district may be requested to visit operational site for review and support on periodic basis. These review visits need to be financially supported. In order to meet the miscellaneous expenditure to support district level security formation Rs. 10000 per taluk may be allocated.

4.1 Cost Estimates for third party security audit for CLR operations:

At present, there are several states, where mutation updation workflow has been automated and computerized copies of ROR are being distributed. Keeping this in view, it may be appropriate to consider Security audit exercise for states at National level. This study may be carried out approximately at two to three sites in each state. It shall include the following:

- i. Assessment of present security status and Gap analysis
- ii. Vulnerability assessment of servers /clients
- iii. Penetration testing
- iv. Imparting training to revenue staff/officers involved in managing the project.
- v. Review of risk assessment methodology
- vi. Application software testing

It will likely to cost Rs. 2.0 lakhs per site at tehsil level. (Expenditure estimates are based upon the projections given by STQC). However, this task may be assigned at National level by Dept. of Land Resources, MRD to an appropriate agency.

4.2 Cost Estimates for creation of Incident management; review mechanism and response site:

Based upon the security audit and risk assessment, each site in every state may be regulated as per national security guidelines. This will involve necessary infrastructure; portal management and a small control room at state monitoring center. Cost-estimates for setting up of primary control room, managing operation, (CIRT) computer Incident Response Team and web based reporting and solutions will be placed @ 2.00 lakh. This expenditure will be met out from funds provided for setting up of monitoring cell at State level under the CLR scheme.