Document Title /Name	**Security Guideline for Project**
Document /Policy Number	ISMS/GuL/001
Current Version	2.0
Document/Policy Owner	Chief Technology Officer, Securitysense.org
Document Author	Firoz Haider Khan,
Approver	Chief Executive officer /Chief Technology Officer, Securitysense.org
Effective From	15th March 2012
Next Revision Date	As required
Document Type/Classification	Internal
Document Font	Axiata Book
File Name	Security Guideline for Project Ver2.0.docx, MS word 2010
Document /File Location	

Document Amendement Records

A =Added, M = Modified, D = Deleted

Version No.	Date	Section No.	A/M/D	Description	Author
Version 1.0	1st October 2010	-	-	1st version.	Firoz Haider Khan
Version 2.0	15th March 2012	-	-	2nd version.	Firoz Haider Khan

Table of Contents

1. INTRODUCTION

Information security vulnerabilities are often introduced when changes take place in the organization's business processes, systems, or facilities. Since these organizational changes are implemented through projects, it is essential for the security program to be tightly integrated with the project management function. Therefore, an important element of project management should be to address the security implications of the changes that are being introduced.

New or expanded project must addresses the security needed for the effective business operation of the information system. Security controls must be an integral part of project planning, development and implementation.

2. OBJECTIVE

The purpose of these guidelines is to ensure that appropriate level of information security control is in place for new business initiatives/project.

3. SCOPE

This document defines the general information security guideline required to securely deploy project which is initiated or administered by Robi.

This guidelines applies to all Vendor, Project Manager, System Owner, Application Owner, Database Owner, consultants, temporaries, and others not mentioned who is associated with any new business initiatives/project or enhanced projects.

4. EXCEPTION

If any control is not applicable or not viable considering situation must be recorded and justified with risk assessment where applicable. This document will be prepared by respective project manager, recommended by respective business owner unit head, respective system/application/database administrator and head of network security & audit and approved by respective business owner department head.

5. GENERAL INSTUCTIONS

To ensure proper evaluation of the information security guideline project manager has to follow below rules/instructions.

1. Project Manager will provide supporting document(s) for project - project scope, project charter, schematic diagrams for service, network diagrams, ip addresses, service ports, hostname and encryption documentation (if encryption is used) etc.
2. Project Manager will provide the Information Security Checklist to vendor during RFP.
3. Project team will provide evaluated document during RFQ to Network Security & Audit team. Network Security & Audit team will verify the feedback.
4. Vendor will ensure all complied controls are implemented and provide certificate of those implementation.
5. Project Manager must ensure that all complied controls are implemented within the project, if any complied control found not implemented within the product lifetime concern vendor is solely responsible to remediate/implement the control(s).
6. Project team will provide signed Information Security Checklist to stake holder and Network Security & Audit during handover of the project.
7. System Business Owner/Operation team will not accept the project without singed Information Security Checklist.
8. Without information security controls implementation and signed information security checklist (filled up) will be considered as incomplete project/task.
9. Securitysense Network Security and Audit team reserves all the rights to verify any system any time for Security Compliance.

6. GUIDELINES

The following guidelines shall be used to consider information security requirements during the planning, design and implementation of any new business initiatives/projects or enhanced projects.

5.1 General

[1] Project Manager, Vendor need to ensure to comply with all information security policies and Procedures.

[2] All default account of the system/database/application must have to be disabled/ locked before the service going to live.

[3] Restriction of application bypass: What if a user connects to the database and bypasses the application, how to enforce security regarding this? There must be some mechanism to protect from such occurrence.

[4] Use of static IP address in application for scripting is not allowed.

[5] The Servers must be security hardened before going live by the corresponding OS's native hardening tools (e.g. Solaris JASS Script) and hardening document shall be handed over to the operation team.

[6] Test Platform can co-exist with Development platform but Test/Development platform must be isolated with production platform.

[7] The systems must be scanned by Securitysense Information Security scanning testing tools before going Live and the result must be satisfactory.

[8] There shall be no limitation of conducting penetration testing and vulnerability assessment on the designated system/database/application and Securitysense Information Security (Network Security & Audit) can perform the penetration test anytime without any notification.

[9] Vendor must have facilities/support to reduce the vulnerability and threat detected by Scanner or any tools.

[10] The systems must be protected and updated with standard antivirus software to protect any malicious attack.

[11] Use of "Admin" or "Administrator" username with administrative privileged should be avoided in the system/database/application.

[12] PING cannot be a way of monitoring or heartbeat between two hosts. So, others forms of monitoring criteria except ICMP will have to use. If the service is published to Internet, ICMP service must be disabled.

[13] Project Manager must consult with associate team for Database selection or design, hardware design and hardware placement in data center issue in the beginning of project.

[14] Project Manager will ensure to implement respective security policy/guideline/procedure (OS, application, database and Network etc.) in the system.

5.2 Network Security

[15] Perimeter devices (Router, Switch, Wireless Access Point and Firewall etc.) must be configured as per security policy/guideline/procedure.

[16] All incoming or outgoing communications to External/Public Sites must go through a staging server or via web server. The staging server must be located at the DMZ and only DMZ is allow to communicate to outside. The external communication should not be directly to/from the application or database server.

[17] If the service is published in Internet, then the front end server must have to place in firewall DMZ zone and the application access from Internet must be through a DMZ reverse proxy. Inside Firewall access from Extranet shall not be allowed and Vendor shall provide necessary solution to achieve this requirement.

[18] The front end to back end communication (Between DMZ and Inside network) should be through FQDN or DMZ mapped IP address using only required ports. Inside IP segment will never be published to DMZ.

[19] If vendor requires remote access to the server to provide operation and maintenance or application support, the access should be through VPN connection. Securitysense will provide necessary VPN client support to the vendor.

[20] There must have a network security architecture design indicating operational connectivity with every server in port level. The security architecture design must be approved by Information Security (Network Security & Audit).

5.3 Application Security

[21] Vendor supplied application must have mechanism or control that application team will never require administrative password for any kind of application operation. If they require, they may be collect it from System Administrator to perform the activity.

[22] Application team and System Administrator will have right to change any password any time without asking permission from vendor.

[23] An application must be (needs to) be capable of auditing the activities of the real user with reporting system.

[24] Application need to be capable of storing and protecting authentication credentials for batch Jobs/database logon information in an encrypted form. (The encryption algorithm must be worldwide recognized. E.g. RSA/DSA etc).

[25] Application must have encryption mechanism that sensitive information (E.g. Credit Card Numbers & PINS, Salary Information etc.) in a table or column must be encrypted. Only application can be decrypt & read the information, no other can.

[26] Telnet and FTP is not preferred in Securitysense environment. Secured Shell (SSH) should be used to replace Telnet & FTP and HTTPS instead of http.

[27] The application must not run the following services.

19/Chargen	6665-6669/IRC	512/rexec
1080/MyDoom	6699/Napster	VDOLIVE
1214/Kazaa	6881-6999/ BitTorrent	Real Audio
1241/Nessus	7648-7649/ CU-SeeMe	554/RTSP
2745/Bagle.H	8866/Bagle.B	SQL*Net2
3127/MyDoom	9898/Dabber	FreeTel
4444/Blaster	9988/Rbot/Spybot	CoolTalk
4672/eMule	14567/Battlefield	H.323
5050/Yahoo Msg	27015/Half-Life	NetShow
5190/AIM/ICQ	27374/Sub7	Backweb
5554/Sasser	31337/Back Orifice	IIOP
6112/Battle.net	69/TFTP	CVP
6346-6347/Gnutella	2049/NFS	
6500/GameSpy Arcade	513/rlogin	

(If the above service(s) is needed, please provide justification at the remark column and attach a document of what will be done for risk mitigation.)

[28] File sharing or shared drive across LAN is prohibited. Secure method should be used.

[29] Client-server-based application should use own application-sockets (ports/services) for communications. The application ports/services should be reviewed against commonly-identified vulnerable ports/services. (Please specify the proposed TCP or UDP ports/services used)

[30] Encryption is required for confidential information transfer between the client and server. (example of confidential information such as business dealing, monetary transaction etc)

[31] [Please provide a supporting document to indicate the encryption level (base on OSI e.g. network level or application level), type of encryption (e.g. SSL, SSH, IPsec, VPN) and the encryption algorithm used (e.g. 3DES, AES)]

[32] The system must be designed to handle the segregation of duties. (e.g.; Admin functions, Business functions and operation functions etc). The UI for these functions must also be configured to run on different ports. (e.g.; port 80/tcp for user UI, and port 8081/TCP for admin UI).

[33] The application must be designed to enforce idle session timeout. (I.e. when no user activity for certain period of time, the session will be terminated. User has to re-logon after timeout termination) the timeout period will be 30 minutes.

[34] The application system must prohibit simultaneous logon sessions from more than 1 workstation/browser/user ID. In case of exception must need justification.

[35] The application must be able to provide the following audit logs on OS level:-

a. system and application log
b. user activity
c. exception log

[36] The application must be able to provide the following audit logs on Application level:-

a. system and application log
b. user activity
c. exception log

[37] The application must be able to provide the following audit logs on Database level:-

a. system and application log
b. database and file accesses log
c. user activity
d. exception log

[38] If the application is in-house developed, the application developer should practice secure programming or coding. (Please specify which secure programming or coding guideline does the application developer practices. E.g. Security code guideline from Java Sun, Code Access Security in Practice or Building Secure Assemblies from Microsoft etc.)

[39] If the application is in-house developed, the source code must be fully documented.

[40] The application should be reviewed against commonly-identified vulnerabilities such as below:-

a. Invalidated Input
b. Broken Access Control
c. Broken Authentication and Session Management
d. Cross-Site Scripting (XSS) Flaws

e. Buffer Overflows
f. Injection Flaws
g. Improper Error Handling
h. Insecure Storage
i. Denial of Service
j. Insecure Configuration Management

[41] Application penetration testing is required for INTERNET FACING APPLICATION. Vendor will do this penetration test and it must be approved by Securitysense Network Security & Audit. Application Penetration Testing report must be submitted to Securitysense Network Security and Audit prior to going live.

[42] The application must be able to provide controls to protect unauthorized changes and operational problem with the logging facilities as follow:

a. Alterations to the log are to be recorded.
b. Log files being edited or deleted.
c. Storage capacity of the log files media being exceeded.

[43] Vendor shall provide detailed documentation on all communication (including protocols & rule sets) required through a firewall, whether inbound or outbound.

[44] Vendor shall provide documentation and/or notification on:

a. Problem reporting.
b. Known vulnerability.
c. Remediation process to test, validate and apply updates and/or workarounds on a baseline reference system before distribution.

[45] Vendor to provide the following documentation, where applicable:

a. Solution system design
b. Technical specification
c. Access matrix
d. Highlight solution dependencies
e. Solution Interfaces
f. Implementation strategy
g. Project timeline
h. Operating procedures – startup & shut down procedure, instruction for handling errors, support contact, system restart, back-up and recovery, other related procedures
i. Business impact analysis and risk assessment
j. UAT plan

5.4 Database Security

[46] The Database has to be configured or harden to meet Robi's Database security guideline.

[47] Database software should be protected from unauthorized modification.

[48] Unnecessary & risky privileges/roles (e.g. DBA/SYSDBA etc.) must not be used by the Application and there must not be any database user password within the OS scripts.

[49] Configuration Management policies should be developed and implemented for database applications.

[50] DDL (Data Definition Language) statements that alter data objects should not be used in a production environment.

[51] Unused database components that may contain vulnerabilities must be removed. Remove all test database and user IDs. The default admin password must be changed and not used.

[52] System must be equipped/installed with latest patches available.

[53] Production and development database components and resources should be separated, easily identified, and protected.

[54] ODBC (Open Database Connectivity) tracing should be removed from an Oracle Windows host system to prevent the creation of unprotected sensitive information.

[55] Database application software should be owned by a single, protected account.

[56] A database software baseline should be created to allow determination of unauthorized modifications.

[57] Audit trail data should be maintained for 12 year. It can be archived and kept separately.

[58] Database object baselines should be established and maintained to help detection of unauthorized modification.

[59] Temporary passwords should be assigned to newly created database accounts. Change password will be requested upon first logon.

[60] Client should be configured to prevent random port assignment to remote database connections.

[61] The connection timeout parameter should be set to prevent denial of service attacks on the listener port.

[62] The expiry time parameter should be set to prevent inactive remote connections to the database

[63] Trust relationships can be set up between systems.

[64] Access control policies are in place for data access privileges.

[65] A documented information classification scheme must be in place. Database schema should be separated according to its classification.

5.5 System Security

[66] The Operating System (OS) has to be configured or harden to meet Robi's OS security guideline.

[67] By default all unwanted services must be closed. Only required services such as the client-server services, application services and system requirement services are allowed.

[68] Disable all unneeded communication ports/services, program, removable media drive.

[69] Warning statement on misuse of the system information and facility should be placed upon successful log-in or before log-in to the system.

[70] Data dictionary should be used to document, standardize and control the naming convention and usage of data

[71] The development, DR and production environment should be separated

5.6 System Partitioning

[72] Does the solution use system partition where it allows scalable-processing or multi-processor and more than one application reside & share the firmware in a same physical box?

[73] If partitioning of the applications is at the data-storage (LPARS), partitioning segregation or control mechanism must be in-place.

[74] If partitioning takes place at the physical-memory (memory addressing stack), control mechanism against risk of cross-addressing (e.g. in a memory-overflow) must be addressed.

[75] System must be equipped / installed with latest patches available.

[76] Vendor shall provide documentation detailing all applications, utilities, system, services, script, configuration files, databases, and all other software required and appropriate configuration, including revisions and/or patch levels.

5.7 ID Security (OS, Application & Database)

[77] Ensure the password related controls must be inbuilt in all systems (OS, Application, Database and network level)

a. Each user must have individual username and password. Password cannot be shared with others in any instance.

b. Minimum password length is 8 characters.

c. Force users to change temporary password at the first log-on.

d. Passwords contain combination of minimum three out of these four: one numbers, one capital character, one small letter, one special character (e.g.,!,?, #, %, *).

e. User cannot use the same password after next two times. (System will remember last two passwords).

f. Passwords are displayed on the screen in asterisk (*) form when being entered.

g. In network environment, users need to change password after 45 days interval.

h. Allow users to change their own passwords and include a confirmation procedure to allow for input error.

[78] For secure authentication practice, the following security measures must be inbuilt in all systems (OS, Application, Database and network level)

a. Systems or database or applications do not display the contents until the log-on process has been successfully completed.

b. System or database or applications authentication is transferred in encrypted from rather that clear text.

c. Upon completion of all input of log-in requirements, system validates the logon information. If errors arise, the system does not indicate which part of the data is correct or incorrect. Unsuccessful log-on attempts is allowed only to three attempts.

d. Limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on.

e. Display date and time of previous successful log-on and display details of any unsuccessful log-on attempts since the last successful log-on.

f. As a security measure, after 30 minutes of no activity, log-on session automatically expires

[79] Application, OS, and Database must ensure that the password MUST NOT be same as the user id or “PASSWORD” upon creation of the new user id.

[80] Vendor cannot have administrative password to work in the system/servers either locally or remotely after project go-live. If they require administrative password, that must be entertained and shall be attendant by a Securitysense system Administrator. In case of requirement to work from remotely a secured method shall be applied in this case (e.g. WebEx Session, Secured Shared Shell session etc).

[81] The input field for password MUST NOT be visible while the users type in their passwords.

[82] Password MUST NOT be stored in clear text. It must be encrypted or masked.

[83] User id/Password repository (e.g. a file, database-table) MUST NOT be allowed to be copied out or must be secured against password-cracking.

[84] Password must never be hard-coded into software developed.

[85] System is able to generate alerts for failed login attempts (configurable)

[86] Account lockout must be configured. After 5 times of unsuccessful attempt, the user id will be locked.

[87] Changing of password can be done without administrator assistance.

[88] IDs that have been dormant or inactive for 120 days must be revoked. Dormant period can be configured.

[89] Inactive ID for more than 120 days must be highlighted.

[90] Vendor supplied default passwords for the system should be changed immediately upon installation.

[91] Application provider will assist Securitysenseto establish user access matrix.

5.8 Operational Management

[92] System/Application/Database must have a backup mechanism to comply Securitysense Standard backup and disaster recovery procedure to satisfy business continuity requirements.

[93] Project Manager to need consider redundant system for service availability

[94] Project Manager must ensure system must be compatible with Securitysense existing and future planned backup system .Also ensure system must be capable to backup from the 1st operation day

[95] New system must have tape backup facilities and must compatible with EMC, VERITAS, SAN or other renowned backup application.

[96] The system has the backup/restore capability for

a. Full systems backup such (application, production data, configuration, parameters and definitions etc) into removable media for offsite storage.

b. Backup files can be restored for business continuity.

c. Backed-up files recoverable instantaneously whenever required for forensic/ investigation purposes.

[97] The vendor is to provide a documented steps & procedures for the backup and restore process.

[98] Vendors sign individual NDA's to preserve the confidentiality of any proprietary information made available to them by Robi.

7. RESPONSIBILITY

Compliance with this guideline is the responsibility of Project Manager, Application/OS/Database owner/ Infrastructure Management team, Vendor and others who is associated with project or project relevant work.

Project Manager will ensure the overall security controls are in place. System / Database / OS / Application / Network Infrastructure and other associate team will be responsible to see the security control of their respective area.

8. ENFORCEMENT

This has been made for protection of company assets and employees. Employees have gone through, understood and acknowledged the guideline. All heads of departments will be responsible to enforce this guideline at their level.

9. DISCIPLINARY PROCESS

Any employee or personal found to have violated this guideline may be subject to disciplinary action that will be handled via existing organization governing rules regulation and procedures.

10. GUIDELINE REVIEW

Network Security and Audit Team will review this guideline as per need basis in conjunction with major changes to the infrastructure, as part of Securitysense.org's participation in system security audits, after each breach in system security, or any time if business need.

11. CONCLUSION

Information is critical to the operation and perhaps even the survival of organization. Being compliance to this guideline will help to manage and protect valuable information assets.

12. REFERENCES

1. Information Security Checklist
2. Exception & Justification Template

3. Risk assessment Template
4. Baseline security guide for windows, LINUX/UNIX and Database etc.