Knights Inc.

Statement of Applicability

ISO 27001 : 2013

DOCUMENT CONTROL

Name	Action	Date	Signature
Harold	Prepared by	November 2013	

Revision History

Version	Date	Description
1.0		First Release

ISO 27001 Statement of Applicability (SOA)

Clause	Controls	Applicable Yes/ No	Justification	If yes give Reference Document
A.5	Information security policies			
A.5.1	Management direction for information security			
A.5.1.1	Policies for information security	Yes	As a result of risk assessment	ISMS Policy
A.5.1.2	Review of the policies for information security	Yes	As a result of risk assessment	➢ ISMS Policy ➢ Minutes of Meetings of the SMB Information Security Committee meetings
A.6	Organization of information security			
A.6.1	Internal organization			
A.6.1.1	Information security roles and responsibilities	Yes	To ensure all requirements & controls have owners	ISMS Policy (Roles & Responsibilities)
A.6.1.2	Segregation of duties	Yes	As a result of risk assessment	Policy for segregation of duties
A.6.1.3	Contact with authorities	Yes	As a result of risk assessment	List of Contact details with Administration department
A.6.1.4	Contact with special interest groups	No	As a result of risk assessment	➢ IT team has membership in online ➢ Records
A.6.1.5	Information security in project management	Yes	As a result of risk assessment	Software Project Management Procedure & Infra Project Management Procedure
A.6.2	Mobile devices and teleworking			
A.6.2.1	Mobile device policy	Yes	As a result of risk assessment	➢ Tele-working and mobile Device policy and procedure ➢ Authorization records of users allowed to do mobile computing
A.6.2.2	Teleworking	No	Tele working	All banking and support actives are done in office. Individuals do not connect to systems using teleworking.
A.7	Human resource security			
A.7.1	Prior to employment			
A.7.1.1	Screening	Yes	As a result of risk assessment	➢ Personnel security policy ➢ Screening procedure
A.7.1.2	Terms and conditions of employment	Yes	As a result of risk assessment, Contractual requirement	➢ Personnel security policy ➢ Terms and conditions of employment attached with Appointment Letter
A.7.2	During employment			

Clause	Controls	Applicable Yes/ No	Justification	If yes give Reference Document
A.7.2.1	Management responsibilities	Yes	As a result of risk assessment	Information security roles and responsibilities document
A.7.2.2	Information security awareness, education and training	Yes	As a result of risk assessment	➢ Training schedule ➢ Training material ➢ Training attendance records
A.7.2.3	Disciplinary process	Yes	As a result of risk assessment	➢ Disciplinary procedure ➢ Record of disciplinary actions taken
A.7.3	Termination and change of employment			
A.7.3.1	Termination or change of employment responsibilities	Yes	As a result of risk assessment	➢ Termination or change employment checklist ➢ Records of termination proceedings and correspondences
A.8	Asset management			
A.8.1	Responsibility for assets			
A.8.1.1	Inventory of assets	Yes	As a result of risk assessment	➢ Policy and Procedure for maintaining Asset Inventory for each department ➢ Asset Inventory
A.8.1.2	Ownership of assets	Yes	As a result of risk assessment	Asset Inventory
A.8.1.3	Acceptable use of assets	Yes	As a result of risk assessment	Acceptable use policy
A.8.1.4	Return of assets	No	As a result of risk assessment	Employee clearance forms
A.8.2	Information classification			
A.8.2.1	Classification of information	Yes	As a result of risk assessment	➢ Asset Classification guidelines ➢ All assets are classified as per guidelines
A.8.2.2	Labelling of information	Yes	As a result of risk assessment	Information labelling and handling procedure
A.8.2.3	Handling of assets	Yes	As a result of risk assessment	Information labelling and handling procedure
A.8.3	Media handling			
A.8.3.1	Management of removable media	Yes	As a result of risk assessment	➢
A.8.3.2	Disposal of media	Yes	As a result of risk assessment	➢ Media handling policy and procedure ➢ Logs of disposed media
A.8.3.3	Physical media transfer	No	Bank process does not allow any employee's to use any removable material	NA

Clause	Controls	Applicable Yes/ No	Justification	If yes give Reference Document
A.9	Access control			
A.9.1	Business requirements of access control			
A.9.1.1	Access control policy	Yes	As a result of risk assessment	➢ Network and Application access control policy and procedure ➢ Logical access control matrix ➢ Record of periodic review of the access control matrix
A.9.1.2	Access to networks and network services	Yes	Logical Segregation of projects and IT services	LAN management Process
A.9.2	User access management			
A.9.2.1	User registration and de-registration	Yes		➢ User access management policy and procedure ➢ Record of all persons registered to use the service ➢ Record for removal or addition of users ➢ Record of periodic review of registered users
A.9.2.2	User access provisioning	Yes	To ensure a process for assigning and revoking of access rights to end users for log on their desktops and laptops	Access Control Process
A.9.2.3	Management of privileged access rights	No	There are no privileged accounts	➢ Authorization records for allocation of privileges
A.9.2.4	Management of secret authentication information of users	Yes	As a result of risk assessment	➢ Process for issue and control of RAS tokens ➢ Process for password management
A.9.2.5	Review of user access rights	Yes	As a result of risk assessment	➢ User access management policy and procedure ➢ Information security audit procedure ➢ Records of reviews
A.9.2.6	Removal or adjustment of access rights	Yes		Termination checklist
A.9.3	User responsibilities			
A.9.3.1	Use of secret authentication information	Yes	As a result of risk assessment	Process for issue , control & use of RAS tokens
A.9.4	System and application access control			
A.9.4.1	Information access restriction	Yes	As a result of risk assessment	➢ Logical access control policy ➢ Logical access control matrix
A.9.4.2	Secure log-on procedures	Yes	As a result of risk assessment	➢ Operating system security policy and procedure ➢ Security message displayed at logon ➢ Security policies defined on Domain Controller
A.9.4.3	Password management system	Yes	As a result of risk assessment	➢ Operating system security procedure

Clause	Controls	Applicable Yes/ No	Justification	If yes give Reference Document
				➢ Password security procedure
A.9.4.4	Use of privileged utility programs	Yes	Access to use of privileged utility programs (system utilities) are strictly controlled based on needs of systems and application	➢ Access control policy
A.9.4.5	Access control to program source code	Yes	As a result of risk assessment	➢ Software development and testing policy ➢ Audit logs of all accesses to program source libraries ➢ Authorization records for personnel having access to program source code ➢ Change control records ➢ Logical access control list of personnel authorized to access source code
A.10	Cryptography			
A.10.1	Cryptographic controls			
A.10.1.1	Policy on the use of cryptographic controls	Yes	Encryption done for backups, Hard disks of laptops	Encryption Policy
A.10.1.2	Key management	Yes	Keys for encryption are controlled	
A.11	Physical and environmental security			
A.11.1	Secure areas			
A.11.1.1	Physical security perimeter	Yes	As a result of risk assessment	Physical and environmental security Policy and Procedure
A.11.1.2	Physical entry controls	Yes	To ensure levels of security depending on physical access rights (e.g. Treasury, Data centre etc.)	➢ Physical and environmental security Policy and Procedure ➢ Visitors' Register
A.11.1.3	Securing offices, rooms and facilities	Yes	As a result of risk assessment	➢ Physical and environmental security Policy and Procedure ➢ Swipe card system logs
A.11.1.4	Protection against external and environmental threats	Yes	As a result of risk assessment	➢ Physical and environmental security Policy and Procedure ➢ Environmental System documents ➢ Risk Assessment
A.11.1.5	Working in secure areas	Yes	As a result of risk assessment	Physical and environmental security Policy and Procedure
A.11.1.6	Delivery and loading areas	Yes	As a result of risk assessment	➢ Physical and environmental security Policy and Procedure ➢ Incoming and Outgoing Materials Register
A.11.2	Equipment			

Clause	Controls	Applicable Yes/ No	Justification	If yes give Reference Document
A.11.2.1	Equipment siting and protection	Yes	As a result of risk assessment	Physical and environmental security Policy and Procedure
A.11.2.2	Supporting utilities	Yes	As a result of risk assessment	Physical and environmental security Policy and Procedure
A.11.2.3	Cabling security	Yes	As a result of risk assessment	➢ Physical and environmental security Policy and Procedure ➢ Cabling security procedure and patch list
A.11.2.4	Equipment maintenance	Yes	Need to ensure availability of all information processing equipment.	➢ Physical and environmental security Policy and Procedure ➢ Daily equipment monitoring records and maintenance records ➢ Equipment repair / servicing records ➢ Equipment Insurance documents
A.11.2.5	Removal of assets	Yes	Protection of all information processing assets to safeguard infomraiton.	➢ Physical and environmental security Policy and Procedure ➢ Gate pass
A.11.2.6	Security of equipment and assets off-premises	Yes	As a result of risk assessment	➢ Physical and environmental security Policy and Procedure ➢ Equipment Insurance documents
A.11.2.7	Secure disposal or re-use of equipment	Yes	As a result of risk assessment	Physical and environmental security Policy and Procedure
A.11.2.8	Unattended user equipment	Yes	As a result of risk assessment	Physical and environmental security policy
A.11.2.9	Clear desk and clear screen policy	Yes	As a result of risk assessment	Physical and environmental security policy
A.12	Operations security			
A.12.1	Operational procedures and responsibilities			
A.12.1.1	Documented operating procedures	Yes	As a result of risk assessment	Documented operating procedures
A.12.1.2	Change management	Yes	As a result of risk assessment	➢ Operations management and Change control policy and procedure ➢ Change management records
A.12.1.3	Capacity management	Yes	As a result of risk assessment	➢ Physical security procedure ➢ Record of capacity planning
A.12.1.4	Separation of development, testing and operational environments	No	As all developers ensure compliance to change management policy to upgrade changes to the operational environments	NA
A.12.2	Protection from malware			
A.12.2.1	Controls against malware	Yes	As a result of risk assessment	➢ Policy and procedure for protection against malicious and mobile

Clause	Controls	Applicable Yes/ No	Justification	If yes give Reference Document
				code ➢ Logs of scans by the antivirus software
A.12.3 Backup				
A.12.3.1	Information backup	Yes	As a result of risk assessment	➢ Backup Procedure (including procedure for backup testing) ➢ Record of backups taken ➢ Logs of backup testing
A.12.4	Logging and monitoring			
A.12.4.1	Event logging	Yes	Enabled to track to activities. Most default settings retained or increased as per RA	Event Log policy & Process
A.12.4.2	Protection of log information	Yes	As a result of risk assessment	➢ Event Log policy & Process ➢ Logging and log monitoring procedure ➢ Logical access control list of personnel authorized to maintain and access logs
A.12.4.3	Administrator and operator logs	Yes	As a result of risk assessment	System administrator and operator logs
A.12.4.4	Clock synchronisation	Yes	As a result of risk assessment, Legal requirement	Procedure for clock synchronization
A.12.5	Control of operational software			
A.12.5.1	Installation of software on operational systems	Yes	As a result of risk assessment	➢ Software development and testing policy ➢ Record of Acceptance Testing carried out before new applications or OS versions are deployed ➢ Audit logs of all updates to operational program libraries ➢ Logical access control list of personnel authorized to access internal applications
A.12.6	Technical vulnerability management			
A.12.6.1	Management of technical vulnerabilities	Yes	As a result of risk assessment	➢ Software development and testing policy ➢ Patch management procedure ➢ Bug Fix procedure related to OS, Application and Network ➢ Version control procedure
A.12.6.2	Restrictions on software installation			
A.12.7	Information systems audit considerations			
A.12.7.1	Information systems audit con-	Yes	As a result of risk assess-	Information security audit procedure

Clause	Controls	Applicable Yes/ No	Justification	If yes give Reference Document
	trols		ment	
A.13	Communications security			
A.13.1	Network security management			
A.13.1.1	Network controls	Yes	As a result of risk assess-ment	➢ Network security policy ➢ Router and Switch and Firewall logs ➢ Log monitoring records
A.13.1.2	Security of network services	Yes	As a result of risk assess-ment	➢ Network security procedure ➢ Email policy and procedure
A.13.1.3	Segregation in networks	Yes	As a result of risk assess-ment	Network security procedure
A.13.2	Information transfer			
A.13.2.1	Information transfer policies and procedures	Yes	As a result of risk assess-ment	Email policy and procedure
A.13.2.2	Agreements on information transfer	Yes	Contractual requirement	Third party agreements
A.13.2.3	Electronic messaging	Yes	As a result of risk assess-ment	Email policy and procedure
A.13.2.4	Confidentiality or nondisclosure agreements	Yes	As a result of risk assess-ment	➢ Terms and conditions of employ-ment attached with Appointment Letter ➢ Non-Disclosure Agreements signed with personnel handling very sensitive information
A.14	System acquisition, development and maintenance			
A.14.1	Security requirements of infor-mation systems			
A.14.1.1	Information security require-ments analysis and specification	Yes	As a result of risk assess-ment	➢ Software development and testing policy ➢ Security requirements specification document for systems ➢ Record of testing carried out before purchase of products
A. 14.1.2	Securing application services on public networks	Yes	Online banking service and ATM services use applications with other service providers	ODBC connectivity security process
A. 14.1.3	Protecting application services transactions	Yes	Online banking service and ATM services use applications with other service providers	ODBC connectivity security process
A.14.2	Security in development and support processes			

Clause	Controls	Applicable Yes/ No	Justification	If yes give Reference Document
A. 14.2.1	Secure development policy	Yes	Core Banking application & enhancements require secure development	Coding Guidelines, Code review process, Vendor software development process and Software OEM NDA for secure development
A. 14.2.2	System change control procedures	Yes	As a result of risk assessment	➢ Operations management and Change control policy and procedure ➢ Change management records
A. 14.2.3	Technical review of applications after operating platform changes	Yes	As a result of risk assessment	➢ Operations management and Change control policy and procedure ➢ Change management records
A.14.2.4	Restrictions on software installation packages	Yes	As a result of risk assessment	-Operations management and Change control policy and procedure -Version control procedure
A. 14.2.5	Secure system engineering principles	Yes	To ensure security in application development and testing	Security in application development and testing process
A. 14.2.6	Secure development environment	Yes	To ensure security in application development and testing and use of cloned data for testing	Security in application development and testing process
A. 14.2.7	Outsourced development	Yes	For vendors developing non core banking application.	Vendor management process for software development, testing and enhancement.
A. 14.2.8	System security testing			
A. 14.2.9	System acceptance testing	Yes	As a result of risk assessment	Acceptance criteria mentioned in the Software development and testing policy
A.14.3	Test data			
A. 14.3.1	Protection of test data	Yes	Production data cloned to test environment	Security in application development and testing process
A.15	Supplier relationships			
A.15.1	Information security in supplier relationships			
A.15.1.1	Information security policy for supplier relationships	Yes	As a result of risk assessment	Vendor management process
A.15.1.2	Addressing security within supplier agreements	Yes	Contractual requirement	➢ Security clause present in Supplier agreements ➢ Confidentiality or Non-disclosure agreements with certain Supplier
A.15.1.3	Information and communication technology supply chain	No	There are no suppliers using banking application. Other banks are addressed through Banking regulation	Not applicable
A.15.2	Supplier service delivery management			
A.15.2.1	Monitoring and review of supplier services	Yes	Contractual requirement	➢ Third party security procedure ➢ Record of management reviews of third party services

Clause	Controls	Applicable Yes/ No	Justification	If yes give Reference Document
A.15.2.2	Managing changes to supplier services	Yes	Contractual requirement	➢ Pertaining clause in agreements with Third parties ➢ Change management records
A.16	Information security incident management			
A.16.1	Management of information security incidents and improvements			
A.16.1.1	Responsibilities and procedures	Yes	As a result of risk assessment	Security incident management reports
A.16.1.2	Reporting information security events	Yes	As a result of risk assessment	➢ Incident detection and response policy and procedure ➢ Security incident reporting forms
A.16.1.3	Reporting information security weakness	Yes	As a result of risk assessment	➢ Incident detection and response policy and procedure ➢ Security incident reporting forms ➢ Complaints logs
A.16.1.4	Assessment of and decision on information security events	Yes	Events of system auto alerts are to be managed for performance	Events and Incident Management process
A. 16.1.5	Response to information security incidents	Yes	As a result of risk assessment	Events and Incident Management process
A.16.1.6	Learning from information security incidents	Yes	As a result of risk assessment	➢ Incident detection and response policy and procedure ➢ Incident register
A.16.1.7	Collection of evidence	Yes	Legal requirement	➢ Incident detection and response policy and procedure ➢ Security incident reporting forms ➢ Security incident management reports
A.17	Information security aspects of business continuity management			
A.17.1	Information security continuity			
A.17.1.1	Planning information security continuity	Yes	As a result of risk assessment	➢ Business continuity plans ➢ Contingency policy
A.17.1.2	Implementing information security continuity	Yes	As a result of risk assessment	➢ Business continuity plans ➢ Contingency policy
A.17.1.3	Verify, review and evaluate information security continuity	Yes	As a result of risk assessment	➢ Business continuity plans ➢ Contingency policy ➢ Record of testing and maintaining BCPs
A.17.2	Redundancies			
A.17.2.1	Availability of information processing facilities	Yes	<BLANK – NO JUSTIFICATION>	<BLANK – NO JUSTIFICATION>
A.18	Compliance			
A.18.1	Compliance with legal and contractual requirements			
A.18.1.1	Identification of applicable legislation and contractual require-	Yes	Legal requirement	List of applicable legislations

Clause	Controls	Applicable Yes/ No	Justification	If yes give Reference Document
	ments			
A.18.1.2	Intellectual property rights	Yes	Legal requirement	➢ IPR and Data protection policy ➢ Software licenses ➢ Audit reports
A.18.1.3	Protection of records	Yes	Statutory requirement	➢ Information classification procedure ➢ Information labelling and handling procedure ➢ List of record categories, retention periods etc.
A.18.1.4	Privacy and protection of personally identifiable information	Yes	Legal requirement as per Data Protection Law and SOX	IPR and Data protection policy
A.18.1.5	Regulation of cryptographic controls	Yes	Standard SSL certificates used	Cryptographic controls process
A.18.2	Information security reviews			
A.18.2.1	Independent review of information security	Yes	As a result of risk assessment	➢ Information Security audit reports by External auditors ➢ Agreement with external auditors
A.18.2.2	Compliance with security policies and standards	Yes	As a result of risk assessment	➢ Information security audit procedure ➢ Internal and external audit reports ➢ Management review and Follow-up reports
A.18.2.3	Technical compliance review	Yes	As a result of risk assessment	➢ Information security audit procedure ➢ Internal and external technical audit reports ➢ Penetration test / Vulnerability assessment reports by external auditors