Methodology Used:

1. NIA Policy was mapped to ISO 27001:2013 and PCI DSS v3.1 controls.
2. A green blank in the ISO/PCI controls indicate that no direct mapping was found between NIA policy and ISO 27001 / PCI DSS v3.1 controls.
3. A cell highlighted in yellow indicates partial mappings between the standards

Document Control

Author: Cyber Security Policy and Standards Section, Cyber Security Sector, Ministry of Information and Communications Technology
Document Ver: 3.0
Last Updated: 30 November 2015
Document Classification: Public

References

[27001]: ISO/IEC 27001:2013(E): International Standard ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements, Second edition 2013-10-01

Disclaimer

The Ministry of Information and Communications Technology (ictQATAR) in its endeavor to further the adoption of its National Information Assurance Policy (NIAP) V2.0 and simplify compliance to multiple standards has created a mapping to identify common controls across NIAP and other international standards.

Within this document we have mapped the NIAP to ISO 27001:2013 and PCI DSS V3.1

PCI Security Standards Council, LLC with a place of business at 401 Edgewater Place, Suite 600, Wakefield, MA 01880, is the owner of the copyright in each of the standards, specifications produced by PCI Security Standards Council including PCI DSS v3.1. PCI DSS standards are available for download at the PCI website (https://www.pcisecuritystandards.org/security_standards/documents.php).

International Standards Organization (ISO) with a place of business at 1, ch. de la Voie-Creuse, Case postale 56, CH-1211 Geneva 20, is the owner of the copyright in each of the standards, specifications produced by ISO including ISO 27001:2013 and its associated guidelines and standards. ISO Standards are available for purchase at the International Organization for Standardization website: http://www.iso.org/iso/iso_catalogue .

Users of this document are advised that the cross mappings provided in this document are only to help identify overlapping controls within these standards and assist users in building a unified controls framework for their organization. Although the document has gone through an extensive quality review both by internal and external stakeholders, we advise that the organizations conduct the necessary due diligence to ensure compliance with the respective standards and policies.

For any queries regarding compliance to specific controls within a standard or to the complete standard, users are advised to contact the necessary owner of the standard / policy document.

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
	National Information Classification Policy				
3.1	Process Prioritization				
3.2	Compliance Roadmap	6.2	Information Security Objectives and Planning to Achieve Them		
3.3	Application of Controls	A 8.1.1, A 8.2.1	Inventory of assets & Classification Guidelines	2.4, 12.3.4	Maintain an inventory of system components that are in scope for PCI DSS. A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)
	National Information Assurance Manual				
	Section A				
	Section B				
1	Governance Structure				
IG 1	Allocate Program Owner	5.3, A6.1.1	Organizational roles, responsibilities and authorities, Information security roles and responsibilities	12.5	Assign to an individual or team the following information security management responsibilities: 12.5.1 Establish, document, and distribute security policies and procedures. 12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel. 12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. 12.5.4 Administer user accounts, including additions, deletions, and modifications. 12.5.5 Monitor and control all access to data.
IG 2	Allocate appropriate budget and staff	5.1.c, 7.1	Leadership & commitment, Resources		
IG 3	Ensure independence of Program Owner				
IG 4	Continuous Support from Agency's Management for the development, implementation and ongoing maintenance of ICT security processes and infrastructure within their organization	5.1	Leadership and Commitment	12.3.1, 12.5, 12.6, 12.8.3	Explicit approval by authorized parties. Assign to an individual or team the following information security management responsibilities: 12.5.1 Establish, document, and distribute security policies and procedures. 12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel. 12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. 12.5.4 Administer user accounts, including additions, deletions, and modifications. 12.5.5 Monitor and control all access to data. Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. 12.6.1 Educate personnel upon hire and at least annually. 12.6.2 Require personnel to acknowledge at least annually that they have read and understood the

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
IG 5	Delegation of Authority for approval of variation				
IG 6	Define Information Security Responsibilities for ISM, Management, Employees	5.3, A6.1.1, A7.1.2, A15.1.1	Organizational roles, responsibilities and authorities, Information security roles and responsibilities & HR pre Employement Terms and conditions of employment, Information security policy for supplier relationships	3.7, 12.4	Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties. Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
IG 7	Competence of Information Security Manager(ISM)				
IG 8	Define general Information Security management responsibilities for ISM	5.3, A6.1.1	Organizational roles, responsibilities and authorities, Information security roles and responsibilities	12.5	Assign to an individual or team the following information security management responsibilities:Establish, document, and distribute security policies and procedures. , Monitor and analyze security alerts and information, and distribute to appropriate personnel., Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations., Administer user accounts, including additions, deletions, and
IG 9	Define Operational Infomration Security Responsibilities of ISM	5.3, A6.1.2	Organizational roles, responsibilities and authorities, Information security roles and responsibilities		
IG 10	Ensure familiarity of ISM with SOP and roles of IT staff	7.2	Competence		
2	Risk Management				
RM 1	Define a risk assessment process to identify threats and vulnerabilities to critical information assets	6.1.2, 8.2	Define Risk Assessment approach of the organization	12.2 , 6.1	Implement a risk-assessment process , Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities
RM 2	define a risk treatment plan to address threats and vulnerabilities	6.1.3, 8.3	Identify and evaluate options for treatment of risks and select control objectives and controls for treatment of risks , information security risk assessment	12..8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.
RM 3	Ensure that the risk treatment plan and residual risk selected for information assets with an aggregate security level of High are vetted by Senior Management	6.1.3.f	Obtain risk owner approval of the proposed residual risks		
RM 4	Monitor effectiveness of control	6.1.1.e.2, 8.2	evaluate the effectiveness of actions , information security risk assessment		
RM 5	Integration of Risk Assessment with business process	6.1.1.e.1, 8.2	integrate and implement actions into ISM system proccess , information security risk assessment		
3	Third Party Security Management				
TM 1	Ensure outsourced services remain under the governance of the Agency	A14.2.7, A15.2.2	Outsourced software development, Managing changes to supplier services		
TM 2	Understand and acknowledge the risks associated with outsourcing	A 15.1.1, 15.1.2, 15.1.3	Information security policy for supplier relationships, Addresssing security within supplier agreement, Information and Communication Technology Supply Chain		

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
TM 3	Security controls specified in this manual are applicable on outsourced services	A 15.1.1, A 15.2.2	Information Security Policy For Supplier Relationships, Managing Changes to Supplier Services	12..8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.
TM 4	Third party provides regular reporting of services	A 15.2.1	Monitoring and Review of Supplier Services	12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.
TM 5	Reports provided by Third party are monitored, reviewed and audited	A 15.2.1, A 15.2.2	Monitoring and Review of Supplier Services, Managing changes to supplier services	12.8	Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of
4	Data Labeling				
DL 1	Server as a Labeling Authority	A8.2.2	Labeling of information	12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)
DL 2	Rate all information	A8.2.1	Classification of information	12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)
DL 3	Default Classification	A8.2.1, A8.2.3	Classification of information, Handling of information		
DL 4	Establish Data labeling system based on a Need to Know	A8.2.3	Handling of information		
DL 5	Establish Data labeling education and awareness	A8.2.3	Handling of information		
5	Change Management				
CM 1	Define and document a Change Management procedure	A12.1.2, 14.2.2	Change Management, System change control procedures	1.1.1 6.2 6.4.5.1 6.4.5.3 6.4.5.4	A formal process for approving and testing all network connections and changes to the firewall and router configurations Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release Documentation of impact Functionality testing to verify that the change does not adversely impact the security of the system Back-out procedures
CM 2	Establish Change Management Committee				
CM 3	CMC to document and approve proposed changes	8.1	Operational planning and control		
CM 4	Assess system for re-cerification after major changes	8.1, 10.2	Operational planning and control, Continual improvement	6.4.5.2	Documented change approval by authorized parties.
CM 5	Update System Documentation	A5.1.2, A12.1.1, 8.1, 10.2	Review of the policies for information security , Documented operating procedures, Operational planning and control, Continual improvement		
CM 6	Change Management Process to define appropriate action for URGENT Changes				
6	Personnel Security				
PS 1	HR processes integrated with Info Sec Policies	A7	Human resources Security		

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
PS 2	HR manual made available to staff indicating their obligations to the organization	A7.1.2	Terms and Conditions of Employment		
PS 3	Store and Manage Personal information with due diligence in line with state privacy legislations	A18.1.4	Privacy and protection of personally identifiable information		
PS 4	Ensure IS responsibilities are included in Job Responsibilities	A7.1.2	Terms and conditions of employment	12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
PS 5	Pre-Screening of Employees, contractors and third party	A7.1.1	Screening	12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources.
PS 6	Ensure staff on joining sign an agreement outlining their security obligations and responsibilities	A7.1.2	Terms and conditions of employment	12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.
PS 7	Ensure suitable adequate controls in place to prevent personnel from making un-authorized disclousures	A7.2.1, A7.3.1	Management responsibilities, Termination or change of employment responsibilities	9.1 , 9.4	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment , Implement procedures to identify and authorize visitors.
PS 8	User rights are restrictive to information on a Need to Know basis	A9.1.1, A.9.4.1	Access Control Policy, Information access restrictions	7.1.2	Restrict access to privilege user IDs to least privileges necessary to perform job responsibilities.
PS 9	Job Segregation (Split of Responsibilities) is implemented. 4 eye principle.	A6.1.2	Segregation of Duties	6.4.2	Separation of duties between development/test and production environments
PS 10	Define a Disciplinary process and create employee awareness regarding the same.	A7.2.3	Disciplinary process		
PS 11	Physical security for vistors including logs, badges and escorts	A11.1.2	Physical Entry controls	9.2 , 9.4	Develop procedures to easily distinguish between onsite personnel and visitors, to include: Identifying onsite personnel and visitors (for example, assigning badges) Changes to access requirements Revoking or terminating onsite personnel and expired visitor identification (such as ID badges), Implement procedures to identify and authorize visitors.
PS 12	HR integrated with IT for any change in Job responsibilities	A7.3.1	Termination or change of employment responsibilites	9.2	Develop procedures to easily distinguish between onsite personnel and visitors, to include: Changes to access requirements
7	Security Awareness				
SA 1	Define Security Awareness program	A7.2.2	Information Security awareness, education and training	12.6	Implement a formal security awareness
SA 2	Minimum Requirements for SA Program	7.3	Awareness	12.3.5	Acceptable uses of the technology

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
SA 3	Scope of SA Training, (Employees and whre applicable contractors)	7.2, A7.2.2	Competence, Information Security awareness, education and training	4.3 5.4 6.7 8.8 11.6	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties. Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties. Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties. Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.
SA 4	Employees should be trained to recognize social engineering attempts on them and not to disclose any information that could violate Agencie's security policies, such as during social gathering , public events and training events.				
SA 5	Contents of SA Training should be regularly reviewed and updated.				
SA 6	SA Training should be part of Induction training for new emplyees	A7.2.2	Information Security awareness, education and training	12.6.1	Educate personnel upon hire and at least annually.
SA 7	Assess effectiveness of the Training Program. Records of training, tests etc	7.2.c	Competence		
SA 8	Use of indirect media should be effective				
8	Incident Management				
IM 1	Appoint a person to own the Incident Management program and a point of contact	A16.1.1	Responsibilities and procedures	12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.
IM 2	Establish Incident Response Capability	A16.1	Management of Information Security Incidents and Improvements	12.1	Implement an incident response plan. Be prepared to respond immediately to a system breach.
IM 3	Define procedures to detect, evaluate and respond to incidents.	A16.1.2, A16.1.3, A16.1.4, A16.1.5	Reporting information security events, Reporting information security weakness, Assessment of and decision on information security events, Response to information security incidents	12.1	Implement an incident response plan. Be prepared to respond immediately to a system breach.
IM 4	Procedures to report manage and recover from incidents	A6.1.3, A16.1.2, A16.1.4, A16.1.5, A16.1.7	Contact with Authorities, Reporting information security events, Assessment of and decision on information security events, Response to information security incidents, Collection of evidence	12.10.1	Create the incident response plan to be implemented in the event of system breach.
IM 5	Create awareness amongst staff to report incidents	A16.1.2, A.16.1.3	Reporting information security events, Reporting security weaknesses	12.10.4	Provide appropriate training to staff with security breach response responsibilities.
IM 6	Categorise incidents				
IM 7	Co-ordinate with QCERT to create repository of incidents	A6.1.4, A16.1.5	Contact with Special Interest Groups, Response to information security incidents		
IM 8	Report all Criticality Level 1 incidents within 1 hour to QCERT				

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
IM 9	Incident Management coordinator is responsible for developing and executing annual security assurance plan (may include pen test, audit, scenario test)	A16.1.1	Responsibilities and procedures	12.10.2 , 12.10.6	Test the incident response plan at least annually. , Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.
9	Business Continuity Management				
BC 1	Appoint a person to own and manage BC Program	A17.1.2	Implementing information security continuity		
BC 2	Prepapre BC Plan based on RTO	A17.1.1	Planning information security continuity	12.10.1	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: - Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum - Specific incident response procedures - Business recovery and continuity procedures - Data backup processes - Analysis of legal requirements for reporting compromises - Coverage and responses of all critical system components - Reference or inclusion of incident response procedures from the payment brands.
BC 3	BC Plan should include disaster scenarios	A17.1.2	Implementing information security continuity		
BC 4	BC Plan is updated to reflect current status	A17.1.2	Implementing information security continuity		
BC 5	A copy of BC Plan alongwith necessary backup tapes is placed in Fire/ tamper proof safe	A17.2.1	Availability of information processing facilities	9.5.1	Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.
BC 6	Identify alternate DR sites based on RTO	A17.2.1	Availability of information processing facilities		
BC 7	Specifiy strong controls in out-sourcing contracts	A15.1.2	Addressing security within supplier agreements		
BC 8	Regularly test BC Plans	A17.1.3	Verify, review and evaluate information security continuity	12.10.2	Test the plan at least annually.
BC 9	Create awareness about BC Plan	A7.2.2	Information Security awareness, education and training		
10	Logging & Security Management				
SM 1	Adequate set of technical control implementations or proccesses exists for monitoring of access	A12.4.1, A12.4.3	Event logging, Administrator and operator logs	10.1, 10.2	Implement audit trails to link all access to system components to each individual user. Implement automated audit trails for all system components to reconstruct events:
SM 2	Monitoring practices are established in accordance with criticality of infrastructure. Recommend 24x7 for C3 infrastructure	A12.4.1	Event logging	10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.
SM 3	Monitoring activity is in line with regulatory & legal framework	A18.2.2	Compliance with security policies and standards		
SM 4	Enable logging on all infrastructure, data processing equipment and applications equipment processing or protecting info with rating C2 and above	A12.4.1	Event Logging	10.2	Implement automated audit trails for all system components to reconstruct the following events:

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
SM 5	Classify all security log rating of C3 while app and sec log shall be classified in accordance with Confidentiality rating of system	A12.4.2	Protection of log information	10.5.1, 10.5.2, 10.5.5	Limit viewing of audit trails to those with a job-related need. Protect audit trail files from unauthorized modifications. Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).
SM 6	Logs containing personal info should be protected appropriately	A18.1.2	Privacy and Protection of personally identifiable informations		
SM 7	logs retained for minimum 90 days and maximum depending on criticality	A12.4.2	Protection of log information	10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).
SM 8	Relevant event are logged to provide enough information to permit reconstruction of events enable Audit logging or log capture	A 12.4.1	Event logging	10.3	Record at least the following audit trail entries for all system components for each event
SM 9	Exception are identified and reported in accordance with Incident Handling Policy	A12.4.1	Event logging		
11	Data Retention & Archival				
DR 1	Determine retention period of critical assets	A18.1.3	Protection of records	3.1	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements Specific retention requirements for cardholder data Processes for secure deletion of data when no longer needed A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention
DR 2	Data which needs to be retained is stored ensuring CIA and that it can be accessed for defined future purposes	A18.1.3	Protection of records	9.6.1	Classify media so the sensitivity of the data can be determined.
DR 3	Personal information is retained as per proposed information privacy & protection law	A18.1.4	Privacy and Protection of personally identifiable information		
DR 4	Backup, Archival and Recovery processes have defined procedures which ensure CI is retained	A12.3.1	Information Backup		
DR 5	Archived data retains its classification	A12.3.1	Information Backup		
DR 6	Archiving technology is regularly reviewed for obsolence and archived data is maintained in a state that allows successful recovery	A12.3.1	Information Backup		
12	Documentation				
DC 1	Produce a Agency Security Policy incorporating requirements of NIA	A5.1.1	Policies for information security	12.1	Establish, publish, maintain, and disseminate a security policy.

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
DC 2	All systems that is determined as critical should be covered by system security plan/ standards. Necessary SOPs be created and documented.	A12.1.1	Documented Operating Procedure	4.3 5.4 6.7 8.8 11.6	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties. Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties. Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties. Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.
DC 3	System security standards and procedures are aligned and consistent with Agency's security policies and objectives	7.5.2	Creating and updating		
DC 4	ICT security documentation should be classified as C3	7.5.3, A8.2.1	Control of documented information, Classification of information		
DC 5	Ensure documentation is up to date	A12..1.1, 7.5.3	Documented Operating Procedure, Control of documented information	12.1.1	Review the security policy at least annually and update the policy when the environment changes.
13	Accreditation				
AC 1	Ensure establishment of a Governance and SIP in compliance with the National Information Classification Policy [IAP-NAT-DCLS] and this NIA Manual.	4.4	Information security management system		
AC 2	Comply with relevant laws and regulations that exist and those that may be amended or added at a later date.	A18.1	Compliance		
AC 3	Be audited by Certification Body or an independent body designated by ictQATAR	A18.2.1	Independent review of information security		
AC 4	Ensure that an Audit is carried out atleast once every year and whenever it undergoes a change that may impact security of the agency.	A18.2.1, A18.2.3	Independent review of information security, Technical compliance review		
AC 5	Ensure that scope should include all information assets people and processes.	4.3	Determining the scope of the information security management system		
AC 6	Recertification is carried out whenever a major change takes place, or the current accreditation is questioned ..	A18.2.3	Technical compliance review		
AC 7	All non conformances are fixed in a defined timeline	10.1	Non comformity and corrective action		
AC 8	Any exemptions sought by the Agency are approved by the certification body	6.1.3.d	Statement of Applicability		
	Section C				
1	Communication Security				
1.2	***Cabling***				
CS 1	Conduits are used to protect cables from tampering, damage or accidents when carrying data classified at C4 and above and recommended for C2 and above	A11.2.3	Cabling Security Sensitive system isolation		
CS 2	Separate cabling distribution for information classified at C4 and above.	A13.1.3, A11.2.3	Segregation of networks, Cabling security		

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
CS 3	Conduits installed in public / visitor areas should not attract undue attention	A11.2.3	Cabling security	9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks.
CS 4	Documentation on cabling (Cable Register)				
CS 5	Inspect cables for inconsistencies with cable register				
CS 6	Agency's MAY provision for redundant communication pathways to ensure continued connectivity	A 17.2.1	Availability of Information Processing Facilities		
1.3	***Telephone and Faxes***				
CS 7	Advise users of the maximum permitted levels of classifications for both internal and external telephone connections determined by encryption used	A7.2.2, A8.1.3	Information security awareness, education and training, Acceptable use of assets		
CS 8	Speakerphone feature is disabled during telephonic / video conversations where information classified at C3 above is to be discussed and may be overheard	A13.2.1	Information transfer policies and procedures		
CS 9	Remote initiation of conferencing equipment is disabled in sensitive locations	A13.2.1	Information transfer policies and procedures		
CS 10	Rooms designated for communication of sensitive material have appropriate controls to prevent leakage of sound	A11.1.3	Securing offices, rooms and facilities		
CS 11	Fax machines on both ends are secured using encryption devices when sending information classified at C2 and above	A13.2.3	Electronic messaging		
CS 12	Ensure that all of standards are met at both ends before sending a fax. Collect information from fax machine ASAP and inform sender if fax does not arrive within agreed amount of time.	A13.2.1	Information transfer policies and procedures		
2	Network Security	A10.6	Network Security		
2.2	**Network Management**				
NS 1	Details of internal network and system configuration and other sensitive technology are not publicly disclosed or available	A.9.4.1	Information access restriction		
NS 2	remove or disable all default accounts or change their passwords	A9.2.5	Review of user access rights	2.1 2.1.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
NS 3	Network configuration is kept under the control of network manager and all changes are approved through formal CM process, documented and comply with network security policy and regularly reviewed.	A12.1.2	Change management	6.4.5	Change control procedures for the implementation of security patches and software modifications must include the following: 6.4.5.1 Documentation of impact. 6.4.5.2 Documented change approval by authorized parties. 6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system. 6.4.5.4 Back-out procedures.
NS 4	For each managed network maintain high level diagram showing all connections, logical diagrams, include current at date label etc			1.1.2	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks.

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
NS 5	Networks are designed and configured to limit opportunities of unauthorized access	A13.1.2	Security of network services	11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network.
NS 6	Management networks adopt minimum protection measures.	A13.1.3	Segregation in networks	10.5.2	Protect audit trail files from unauthorized modifications.
2.3	**Virtual LANS**				
NS 7	VLANS are used to separate IP telephone traffic	A13.1.3	Segregation of networks		
NS 8	Administrative access is only permitted from the most highly classified VLAN to one at same or lower level of classification.	A.9.2.3	Management of privileged access rights	7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
NS 9	implement all security measures recommended by Agency's Risk Assessment and hardening guidelines published by vendor of switch.	A11.2.1, 6.1.3	Equipment siting and protection, Information security risk treatment		
NS 10	Trunking/port mirroring is not used on switches managing VLAN of different classifications.				
2.4	**Multifunction Devices**				
NS 11	Network connected MFD's are not used to copy documents classified above the level of connected networks				
NS 12	Network connected MFDs capable of transmitting information should have similar controls as normal computers (Access Control, content management etc)	A9.1.1	Access Control Policy		
NS 13	No direct connection from an MFD to a telephone network of lower classification unless specified criterion of NIA is met	A13.1.3	Segregation of networks		
NS 14	deploy MFDs after developing set of policies and procedures governing use of equipment	A.8.3.3, A12.1.1	Phisycal media transfer , Documented Operating Procedure		
NS 15	Info classified at C1 or above is not retained permanently in the MFD				
NS 16	MFDs follow the procedures specified in section C,8.3				
2.5	**Domain Name Servers**				
NS 17	A separate internal DNS is setup and placed on the internal network	A13.1.3	Segregation of networks		
NS 18	DNS information that should be made public either has a locally hosted and secured (bastion server) server.				
NS 19	DNS servers are deployed to ensure there is no single point of failure in their service.	A17.2.1	Availability of information processing facilities		
NS 20	Zone files are digitally signed and crypto authentication and data integrity of zone transfers and dynamic updates is provided.				
NS 21	Cryptographic origin authentication and integrity assurance of DNS data is provided				
NS 22	DNS services including zone transfers to authorized users only				
NS 23	Cryptographic functions related to NS 20 and 21 use a hardware security module for both key management and processing	A10.1	Cryptographic controls		
2.6	**Internet Security**				
NS 24	All s/w and files downloaded are screened & verified against malicious traffic	A12.2.1	Controls against malware		
NS 25	internet gateway denies all traffic unless specifically enabled.			1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.
NS 26	web browsers running on users workstations are properly configured and updated				
NS 27	have capabilities to monitor the traffic and deduce traffic pattern and usage				
2.7	**Email Security**				
NS 28	Email servers are hardened as per best practices and configured as bastion servers.	A13.2.3	Electronic messaging		

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
NS 29	TLS protection is used with SMTP Server			2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP,
NS 30	implement email sender policy framework (SPF). Undeliverable or bounce emails to senders that can be verified via SPF				
NS 31	Internal email distribution lists are secured to prevent access from external parties				
NS 32	Email gateways scan all incoming and outgoing emails to ensure it complies with State Agency's security policy	A12.2.1	Controls against malware		
2.8	**Wireless Security**				
NS 33	Where wireless LANS are used, they are used with sufficient authentication, transmission encryption measures in place	A9.4.2	Secure Log-on procedures		
NS 34	use stronger wireless security protocols such as WPA2 EAP-TLS. Use of VPN over WLANS if classified info is being used.			4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.
NS 35	Good inventory of wireless devidec is maintained	A8.1.1	Inventory of Assets	11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.
NS 36	Scan regulalrly for rogue or unauthorized wireless access points			11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.
NS 37	access points are located to minimize network tapping from publicly accessible areas				
NS 38	The client side settings for 802.1x MUST be secured				
NS 39	network default name, SSID, SNMP strings do not reflect name of agency's department, system etc				
NS 40	For non public wireless AP, encryption keys are regularly changed and SSID disabled				
NS 41	firewall / router is in place between the AP and agency's network			1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
NS 42	WIPS/WIDS installation for C3+ networks				
NS 43	Use multiple SSIDs with different configurations for different VLANs				
2.9	**Clock Synchronization**				
NS 44	NTP servers MUST be secured			10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.
NS 45	Computer or Comms device shall be synchronised to an agreed standard with procedures to address drift.	A12.4.4	Clock Synchronization	10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
NS 46	State Agency's MAY use the authorized Qatari Government time server (a part of the Government Network) as the primary NTP server				
NS 47	All servers and network devices are synchronized with local Agency NTP	A12.4.4	Clock Synchronization	10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.
2.10	**Virtual Private Networks**				
NS 48	VPNs authenticate using either one-time password such as token device, public-private key system with strong paraphrase	A.9.4.2	Secure Log-on procedures		
NS 49	VPNs disconnect automatically after a pre-defined inactivity period			12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity
NS 50	Dual tunnelling is not permitted unless suitable controls are in place.				
NS 51	All computers connected to Agency network via VPN are equipped with personal security software. SW shall be activated at all times	A12.2.1	Controls against malware		
NS 52	Gateway level firewalls are installed to control network trafic from VPN clients.	A13.1.1	Network controls		
2.11	**Voice Over IP**				
NS 53	Voice and data are separate networks. Should be physical but Vlan is permitted.	A13.1.3	Segregation of networks		
NS 54	VoIP capable gateways and other appropriate security mechanism are employed	A13.1.2	Security of network services		
NS 55	evaluate and use security enabled protocols such as SRTP				
NS 56	Proper physical counter measures are in place to protect the VoIP infrastructure	A11.1.2	Physical Entry controls	9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.
NS 57	Adequate call log monitoring is implemented	A14.1.3	Protecting application services transactions		
NS 58	Soft phones if permitted is through secure connection				
NS 59	Backup power is provided to VoIP in case of failure of power				
NS 60	Strong authentication and access controls are implemented to protect voice gateway	A.9.4.2	Secure Log-on procedures		
NS 61	IPSEC or secure shell is used for all remote management and auditing access	A.9.4.2	Secure Log-on procedures	2.2.3 4.1	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: Only trusted keys and certificates are accepted. The protocol in use only supports secure versions or configurations. The encryption strength is appropriate for the encryption methodology in use.
NS 62	Contingency plans for making voice calls are developed if VoIP system becomes unavailable	A17.2	Redundancies		
NS 63	Port security features are enabled on network lan switches that connect VoIP devices				
2.12	**IP V6**				

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
NS 64	A proper risk assessment is conducted prior to transitioning from IPv4 to IPv6	6.1.2	Information security risk assessment		
NS 65	A proper risk assessment is conducted prior to implementing a dual stack environment	6.1.2	Information security risk assessment		
NS 66	Re-accreditation is requested where State Agencies deploy IPv6 in their gateways.	A12.1.2	Change management		
3	Information Exchange				
IE 1	Prior to establishing cross-domain connectivity, the Agency evaluates, understands and accepts the structure, security and risks of other domains. This risk review SHALL be documented for compliance requirements.	6.1, A13.2.1	Actions to address risks and opportunities, Information transfer policies and procedures		
IE 2	When intending to connect an agency network to another secured network, they should comply with the listed baseline controls	A 13.2.1	Information transfer policies and procedures		
IE 3	Ensure necessary agreements (confidentiality agreements) between entities exchanging information have been established prior to information exchange.	A 13.2.2, A 13.2.4	Agreements on information transfer, Confidentiality or nondisclosure agreements	12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.
IE 4	Ensure media which is used to exchange information is protected against unauthorized access, manipulation or misuse within or outside the Agency environment.	A8.2.3	Handling of assets		
IE 5	Maintain the classification and protection of information that has been obtained from another Agency.				
IE 6	Maintain appropriate levels of physical protection for media in transit and store in packaging that protects it against any hazards that would render it unreadable	A 8.3.3	Physical Media transfer	9.5	Physically secure all media.
IE 7	Ensure only reliable and trusted courier service or transport organization shall be used based on a list of known and authorized couriers	A 8.3.3	Physical Media transfer	9.6.2	Send the media by secured courier or other delivery method that can be accurately tracked.
IE 8	Protect information exchanged via electronic messaging from unauthorized access, change or interruption of service.	A13.2.3	Electronic Messaging	4.2	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).
IE 9	Ensure secure messaging is used for all information classified at C3 or above			4.2	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).
IE 10	Attach specified disclaimer	A 13.2.4	Confidentiality or non disclosure agreements		
IE 11	Ensure due diligence to ensure information transmitted if free of viruses and trojans or malicious code	A 12.2.1	Controls against malware		
IE 12	Ensure information exchanged between systems is secured against misuse, unauthorized access or data corruption. For information classsified as C2, I2 or above authenticated and encrypted channels shall be used	A 13.2.3	Electronic Messaging		
IE 13	Limit information provided to general public to sanitized and approved information through a designated and trained media related spokesperson	7.4	Communication		
4	Gateway Security				
4.2	**General**				
GS 1	Networks are protected from other networks by gateways and data flows are properly controlled	A 13.1.1, A 13.1.3	Network Controls, Segregation in networks	1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
GS 2	Gateways connecting Agency networks to other networks shall use appropriate network device to control data flow, control the data flow, use gateway components	A 13.1.1, A13.1.2	Network Contorls, Security of network services	1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.
GS 3	Only authorized and trained staff manage gateways	A7.2.2	Information security awareness, education and training	1.1.5	Description of groups, roles, and responsibilities for management of network components
GS 4	Administrative or management access to gateways processing or transmiting information classified at C3 or above is provided based on dual control- 4 eyes principle.	A 9.4.2	Secure logon procedure		
GS 5	Information exchanged through gateway is labelled as per Data Classification Policy and protected as specified in this document.	A13.2.1, A 13.2.3	Information transfer policies and procedures, Electronic Messaging		
GS 6	DMZs are used to separate externally accessible systems from uncontrolled public neworks	A 13.1.3	Segregation in networks	1.1.4 1.3.1	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
GS 7	Configuration recommendation for Gateways			1.2.2	Secure and synchronize router configuration files.
GS 8	Hardenining guide for Gateways				
GS 9	Monitoring and supervision of gateways is in place and include threat prevention meachanisms and logging.	A 12.4	Logging & Monitoring	12.10.5	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.
GS 10	Gateways block or drop any data identified by the content filter as suspicious	A12.2.1	Documented Operating Procedures		
4.3	**Data Export**				
GS 11	System users are held accountable for data they export and instructed to perform checks on data exported.				
GS 12	Data exports performed should be in accordance to approved procedures or specifically approved by the ISM	A 12.1.1	Documented Operating Procedures		
GS 13	Export of data to a less classified system is restricted by filtering data using atleast checks on classification lables	A 13.2.1	Information transfer policies & procedures		
GS 14	Data exports are checked ensuring keywords searches are performed. Any unidentified data is quarantined until reviewed and approved for release by a trusted source other then the originator				
4.4	**Data Import**				
GS 15	System users are held accountable for data theyimport and instructed to perform checks on data imported.				
GS 16	Data imports performed should be in accordance to approved procedures or specifically approved by the ISM	A 12.1.1	Documented Operating Procedures		
GS 17	Data imported is scanned for malicious and active content	A 12.2.1	Controls against malware		
5	Product Security				
PR 1	Process for product selection is carried out with due diligence and ensures product and vendor independence				
PR 2	Products are classified and labelled as per Classification Policy	A14.1.1	Information security requirement analysis and specification		
PR 3	Selection process includes proper identification of vendor, screening of vendors and defines eval criterion			12.3.7	List of company-approved products
PR 4	Proper testing and effective matching between vendors claim and functionality is carried out.	A 14.2.9	System Acceptance Testing		

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
PR 5	Security evaluation is carried out on a dedicated evaluation configuration including functionality tests, security tests and patching to protect against potential threats and vulnerabilities.	A 14.2.8	System security testing		
PR 6	Delivery of security products is consistent with Agency's security practice of secure delivery	A 12.1.1	Documented Operating Procedures		
PR 7	Secure delivery procedures shall include measures to detect tampering or masquerading	A 14.2.9	System Acceptance Testing		
PR 8	Products have been purchased from developers that have made commitment to ongoing maintenance and assurance of their product.	A15.1.3	Information and communication technology supply chain		
PR 9	Product patching and updating processes are in place.	A12.6.1	Management of Technical Vulnerabilities		
6	Software Security				
6.2	**Software Development and Acquisition**				
SS 1	Security is considered in all phases of SDLC and that it is an integral part of all sys development or implementation project	A 14.1.1, A 14.2.1	Information Security Requirement Analysis & Specification, Secure Development Policy		
SS 2	All applications are classified using Classification Policy and accorded appropriate security	A8.2.1, A 14.1.1, A 14.1.2	Classification of information, Information security requirements analysis and specifications, Securing Application Services on Public Networks		
SS 3	Security requirements (functional, technical and assurance requirements) are developed and implemented as part of system requirements	A 14.1.1, A 14.2.1, A14.2.5	Information security requirements analysis and specifications, Secure development policy, Secure system engineering principles	6.3	Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: In accordance with PCI DSS (for example, secure authentication and logging) Based on industry standards and/or best practices. Incorporating information security throughout the software-development life cycle
SS 4	Dedicated test and development infrastructure are available and is separate from prod systems. Information flow between diff environments shall be strictly according to defined and cocumented policy. Write access to the authoritative source of the software shall be disabled	A 12.1.4, A14.2.6	Separation of Development, Testing and Operational Environments, Secure development environments	6.3.1 6.4.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers. Separate development/test environments from production environments, and enforce the separation with access controls
SS 5	All applications (acquired / developed) are available for production use only after appropriate Quality and sec assurance tests	A14.2.8, A 14.2.9	System security testing, System Acceptance Testing		

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
SS 6	SW developers use secure programming practices	A14.2.1, A 14.2.5, A14.2.6	Secure development policy, Secure System Engineering Principles, Secure development environment	6.3 6.5	Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle Address common coding vulnerabilities in software-development processes as follows: - Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. - Develop applications based on secure coding guidelines
SS 7	SW should be reviewed and tested for vulnerabilities before it is used in a prod environment. SW should be tested by an independent party and not by developer.	A 14.2.8	System security testing	6.3.2	Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: - Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. - Code reviews ensure code is developed according to secure coding guidelines - Appropriate corrections are implemented prior to release. - Code-review results are reviewed and approved by management prior to release.
SS 8	System (acquired / developed) complies with all legal requirements including license, IPR, copyrights etc	A 18.1, A18.2.1, A18.2.3	Compliance with legal and contractual requirements, Independent review of information security, Technical compliance review		
SS 9	All System (acquired / developed) are adequately documented				
SS 10	Source code of custom developed critical application is available and in case of commercial applications, State Agencies should look into options of escrow	A 9.4.5	Access control to program source code		
SS 11	Prior to commissioning of applications they are accredited.	A 18.2.2, A 18.2.3	Compliance with security policies and standards, Technical compliance review	6.4	Follow change control processes and procedures for all changes to system components. The processes must include the following:
6.3	**Software Applications**				
SS 12	All server and workstation security objectives and mechanisms are documented in the relevant system security plan	A 12.1.1	Documented Operating Procedures	1.1.6	Documentation and Business justification for use of all services, protocols and ports allowed including documentation of security features implemented for those protocols considered to be secure.
SS 13	Wkstn use a hardened Standard Operating environment	A 12.1.1	Documented Operating Procedures		

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
SS 14	Vulnerabilities are reduced by adhering to recommendations in NIA Manual	A12.6.1	Management of technical vulnerabilities	6.5	Address common coding vulnerabilities in software-development processes as follows: Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. Develop applications based on secure coding guidelines
SS 15	High risk server e.g. Web server maintain effective functional separation, minimize communication and limit system users access to a minimum	A13.1.3	Segregation of networks		
SS 16	Check integrity of all servers whose functions are critical to agency or those identified as being as High risk			11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.
SS 17	Store the integrity information securely off the server in a manner that maintains integrity				
SS 18	Update integrity information after every legitamate change to system				
SS 19	As part of agency's ongoing audit schedule compare the stored integrity information against current integrity information	A12.7.1	Information System Audit Controls		
SS 20	Resolve any detected changes in accordance to Incident Handling Procedure	A16.1.4	Assessment of and decision on information security events	11.5.1	Implement a process to respond to any alerts generated by the change-detection solution.
SS 21	All SW applications are reviewed to determine wheter they attempt to establish any external connection.				
6.4	**Web Applications**				
SS 22	All active content is reviewed for sec issues. Adhere to OWASP guidelines	A14.2.1	Secure development policy	6.5 6.6	Address common coding vulnerabilities in software-development processes as follows: Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory. Develop applications based on secure coding guidelines For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks
SS 23	Connectivity and access between each web app component is minimized				
SS 24	Personal information and sensitive data is protected whilst in storage and in transmission using crypto controls	A 18.1.4	Privacy and Protection of Personally Identifiable Information		
SS 25	Critical sector websites that need to be strongly authenticated, use SSL certificates provided from a Certificate Service Provider (CSP) licensed in the State of Qatar.				
SS 26	Web application firewall (WAF) MUST be used for applications with MEDIUM or higher risk rating.			2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure
6.5	**Databases**				

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
SS 27	All info stored within database is associated with appropriate classification if the info could be exported to a diff system or contains different classification of info	A8.2.1, A 8.2.2, A 8.2.3	Classification of information, Labelling of Information, Handling of Assets		
SS 28	Classification is applied with a level of granularity sufficient to define handling requirement for any information retrieved or exported from database	A8.2.1, A 8.2.2	Classification of information, Labelling of Information		
SS 29	DB files are protected from access that bypasses the DBs normal access control	A 9.4.1	Information Access restriction	8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: All user access to, user queries of, and user actions on databases are through programmatic methods. Only database administrators have the ability to directly access or query databases. Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).
SS 30	DB provide functionality to allow for auditing of system users action	A 12.7.1	Information System Audit Controls		
SS 31	System users who do not have sufficient privilige to view DBs content should not see associated meta data in search engine queries.	A9.2.3	Management of priviledged access rights		
SS 32	Sensitive data in database shall be masked using data masking technology for C3 & above.				
7	System Usage Security				
SU1	System users SHALL be responsible for the information assets provided to them to carry out their official responsibilities. They SHALL handle the information assets with due care and operate them in line with the vendor / Agency's Acceptable usage policy.	A 8.1.2, A8.1.3	Ownership of assets, Acceptable use of assets	12.3	Develop usage policies for critical technologies and define proper use of these technologies.
SU2	System users will conduct due diligence when accessing the web and shall strictly follow agencies guidelines. Agencies shall decide on usage of social forums	A8.1.3	Acceptable use of assets		
SU3	ICT assets are protected against web based threats by implementing measures that will prevent downloading sw programs, active content and non biz web sites	A 12.2.1	Controls Against Malware		
SU4	Web Access is provided through secure proxies and filtering gateways	A13.1.2	Security of network services	1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
SU5	Staff are aware of the types of content permitted and restricted within State Agency. State Agencies should consider an effective solution for monitoring content of encrypted channels	A 8.1.3, A13.1.2	Acceptable usage of assets, Security of network services		
SU6	Staff should use email with due diligence and include necessary classification labelling depending upon content and attachment	A8.1.3, A8.2.2	Acceptable use of assets, Labelling of information		
SU7	App measures are taken to protect email against potential threats as viruses, trojans, spam etc	A 12.2.1, A13.2.3	Controls Against Malware, Electronic messaging	5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
SU8	staff are aware that web based public emails are not allowed to be used to send receive emails from state agency systems	A 8.1.3	Acceptable use of assets (Also throughout the manual, baseline controls provided)		
SU9	Staff are aware that emails used to exchange confidential information is to be sent to only named recipients and not distribution lists	A 8.1.3	Acceptable use of assets (Also throughout the manual, baseline controls provided)		

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
SU10	Staff are aware that the use of automatic forwarding is dependent on the sensitivity of their normal emails. Email classified at C2 and above shall not be automatically forwarded.	A 8.1.3, A13.2.1	Acceptable use of assets, Information transfer policies and procedures		
SU11	When dealing with external parties Agencies ensure that external recipients understand and agree on the usage of classified data	A 13.2.2	Agreements on information transfer		
8	Media Security				
8.2	**Media Classification and Labeling**				
MS 1	HW containing media is classified at or above the classification of information contained in media	A8.2.2, A8.2.3	Labelling of information, Handling of assets	9.6.1	Classify media so the sensitivity of the data can be determined.
MS 2	Non Volatile media is classified to the highest classification of information stored on it.	A8.2.2	Labelling of information	9.6.1	Classify media so the sensitivity of the data can be determined.
MS 3	Volatile media is classifed to highest classification of info stored on it while powered ON and at other times as C1	A8.2.2	Labelling of information	9.6.1	Classify media so the sensitivity of the data can be determined.
MS 4	Storage media is reclassified if info copied onto that media is high classification or if info contained on that media is subject to classification upgrade	A8.2.2	Labelling of information	9.6.1	Classify media so the sensitivity of the data can be determined.
MS 5	Media holding classified info may be de-classified after the info on the media has been de-classified or if the media has been sanitized	A8.3.1, A8.3.2	Management of removable media, Physical media transfer	9.6.1	Classify media so the sensitivity of the data can be determined.
MS 6	If the media cannot be sanitized then it cannot be declassified and must be destroyed.	A8.3.1, A8.3.2	Management of removable media, Physical media transfer	9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
MS 7	The classification of all media is readily visually identifiable Agencies should label media with protective marking that states the maximum classification	A8.2.2	Labelling of information	9.6.1	Classify media so the sensitivity of the data can be determined.
MS 8	Classification of media is visually identifiable, when using non textual representation for classification markings due to opn sec, staff should be trained appropriately.	A8.2.2	Labelling of information	9.6.1	Classify media so the sensitivity of the data can be determined.
8.3	**Media Sanitization**				
MS 9	Document procedures for sanitization and test it regularly	A 8.3.1	Management of removable media		
MS 10	Media types like micro fiche, optical disks etc containing info classified as C1 or above shall be destroyed prior to disposal	A 8.3.1, A11.2.7	Management of removable media, Secure disposal or reuse of equipment	9.8.1, 9.8.2	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
MS 11	Volatile media is sanitised by removing power from media for at least 10 minutes or over writing all locations of media with arbitrary pattern.	A 8.3.1, A11.2.7	Management of removable media, Secure disposal or reuse of equipment	9.8.1, 9.8.2	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
MS 12	Non volatile magnetic media is sanitised by over writing media or using de guasser	A 8.3.1, A11.2.7	Management of removable media, Secure disposal or reuse of equipment	9.8.1, 9.8.2	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
MS 13	Non volatile EPROM is sanitized by erasing as per manufacturers specification	A 8.3.1, A11.2.7	Management of removable media, Secure disposal or reuse of equipment	9.8.1, 9.8.2	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
MS 14	Flash memory media is sanitized by over writing the media twice in its entirety with a pseudo random pattern	A 8.3.1, A11.2.7	Management of removable media, Secure disposal or reuse of equipment	9.8.1, 9.8.2	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
8.4	**Media Repairing and Maintenance**				
MS 15	Appropriately vetted and briefed personnel carry out repairs and maintenance for HW containing classified info	A11.2.4	Equipment maintenance		
MS 16	Repairs on systems containing classified info rated C3 or above is carried out under supervision	A11.2.4	Equipment maintenance		
8.5	**Media Destruction and Disposal**				
MS 17	Document procedures for destruction and disposal of media	A 8.3.2	Disposal of Media		
MS 18	Media is destroyed by breaking or heating the media until it has either burnt to ash or melted	A 8.3.2	Disposal of Media	9.8.1, 9.8.2	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed. Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
MS 19	Staff members supervise the destruction of media ensuring that it is completed successfully	A 8.3.2	Disposal of Media		
MS 20	Media including faulty media, containing classified info is santized before disposal	A 8.3.2	Disposal of Media		
MS 21	Disposal of media and media waste does not attract undue attention	A 8.3.2	Disposal of Media	9.8.1	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that
9	Access Control Security				
9.2	**General**				
AM 1	Users will be provided access based on concept of least privilege and governed by need to know	A 9.1.1, A 9.1.2	Access control policy, Access to Networks and Network Services	7.1, 7.1.2	Limit access to system components and cardholder data to only those individuals whose job requires such access , Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
AM 2	Access will be managed and controlled through system access controls, identification and authenticationand audit trails based on sensitivity of info. Request shall be authorized by staff supervisor	A 9.2.1, A9.2.2, A9.4.1, A 12.4.1	User registration and deregistration, User access provisioning, Information access restriction, Event Logging	7.2, 8.1.2, 12.3.1	Establish an access control system for systems components that restricts access based on a user's need to know Control addition, deletion and modification of user IDs, credentials and other identifier objects. Explicit approval by authorized parties
AM 3	Access rights of user shall be based on a matrix model of rights defined by business rules established by owners of information	A 9.1.1, A9.4.1	Access Control Policy, Information access restriction	7.1.1, 7.1.3 , 1.1.5	Define access needs for each role, Assign access based on individual personnel's job classification and function., Description of groups, roles, and responsibilities for management of network components

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
AM 4	A process is established which upon any employee role or status change ensures that information system access is updated to refelect new role or status	A 9.2.1, A 9.2.5	User Registration and de-registration, Review of user access rights	8.1.3	Immediately revoke access for any terminated users.
AM 5	System users that need additional access to bypass security mechansims for any reasons shall be formally authroised by ISM	A 9.2.3	Management of Privileged Access Rights	7.1.4	Require documented approval by authorized parties specifying required privileges.
AM 6	Any unauthorized attempt to circumvent Agencys information security shall be perceived as security incident and shall be handled according to incident handling procedure	A 16.1.2	Reporting Information Security events		
AM 7	Audit logs shall be enabled and maintained in such a manner as to allow compliance monitoring with govt policy and incident handling	A 12.7.1	Information Systems Audit Controls	10.1	Implement audit trails to link all access to system components to each individual user.
AM 8	logical access to Agencys network is technically controlled.	A 9.4.2	Secure logon procedures	12.3.2	Authentication for use of the technology
AM 9	Secure records are maintained of all authorised users, user identification, who provided the authorisation, when the auth was granted.	A9.2.2, A 9.4.2	User access provisioning, Secure logon procedures		
AM 10	A logon banner is displayed and requires system users response as acknowkledgement.				
AM 11	Centralized authentication repositories to be protected againt DoS				
9.3	**Identification and Authentication**				
AM 12	Develop and maintain a set of policies and procedures derived from National Classification Policy covering sys users identification, authentication and authorization	A 9.1.1	Access control policy	7.3, 8.1, 8.8	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties, Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components, Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.
AM 13	Educate system users of the Agenc policies and procedures.	A 7.2.2	Information security awareness, education and training	7.3	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.
AM 14	All system user are uniqely identifiable and authenticated on each occasion access is granted			8.1.1, 8.5	Assign all users a unique ID before allowing them to access system components or cardholder data. Do not use group, shared, or generic IDs, passwords or other authentication methods as follows: -Generic user IDs are disabled or removed. -Shared user IDs do not exist for system administration and other critical functions. -Shared and generic user IDs are not used to administer any system components.
AM 15	Individuals who are not employees, contractors or consultants are not granted a user account or given privileges to use Agencies information resources or comm systems unless explicitly approved by the ISM who shall check appropriate agreements, clearances and access forms have been completed	A 9.1.1, A9.4.1	Access Control Policy, Information access restriction	8.1.5	Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: - Enabled only during the time period needed and disabled when not in use. - Monitored when in use.

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
AM 16	Alternate methods of determining the identification of system user are in place when shared / non-specific accounts are used			8.5, 8.6	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: - Generic user IDs are disabled or removed. - Shared user IDs do not exist for system administration and other critical functions. - Shared and generic user IDs are not used to administer any system components. Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc), use of these mechanisms must be assigned as follows: -Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. -physical and/or logical controls must be in place to ensure only yhe intended account can use that mechanism to gain access.
AM 17	Unprotected authentication info that grants system access or decrypts an encrypted device is located on or with the system or device to which authentication information grants access to.				
AM 18	System authentication data whilst in use is not susceptible to attacks including but not limited to replay MITM and session hijacking				
AM 19	A password policy enforcing either a minimum password length of 12 characters with no complexity or 7 characters with complexity as per defined rules	A 9.4.3	Password Management System	8.2.3	Passwords/phrases must meet the following: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.
AM 20	passwords are changed atleast every 90 days	A 9.4.3	Password Management System	8.2.4	Change user passwords/passphrases at least once every 90 days.
AM 21	System users cannot change their password more than once a day and the system forces the user to change an expired password on initial logon or reset	A 9.4.3	Password Management System		
AM 22	Chosen passwords are checked to prevent password predictability as per NIA	A 9.4.3	Password Management System	8.2.5	Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.
AM 23	Screen / Session lockouts to be configured as per NIA	A 11.2.8, A11.2.9	Unattended user equipment, Clear desk and clear screen policy	8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
AM 24	Access to system is suspended after specified nos of logon attempts and as soon as the staff member does not need access due to changing roles	A9.1.1, A9.4.1, A9.2.6	Access Control Policy, Information access restriction, Removal or adjustment of access rights	8.1.6 , 8.1.3	Limit repeated access attempts by locking out the user ID after not more than six attempts, Immediately revoke access for any terminated users.
AM 25	Lost, stolen , compromised passwords are immediately reported to ISM and changed upon identity verification	A16.1.2	Reporting Information Security events		
AM 26	Accounts that are inactive for more then 3 months are suspended	A 9.2.6	Removal or adjustment of access rights	8.1.4	Remove/disable inactive user accounts within 90 days.
AM 27	Accounts on system processing information rated C2 I2 A2 or above are audited for currency on a 6 monthly basis	A 9.2.5	Review of User access rights		
9.4	**System Access**				

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
AM 28	Security policies document any access requirement, sec clearances and briefings necessary for system access	A 9.1.1, A9.4.1	Access control policy, Information access restriction	7.3	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.
AM 29	System users have been vetted before being granted access to system	A 7.1.1, A9.2.1	Screening, User registration and deregistration		
AM 30	System users have received necessary briefings before being granted access to system	A 7.2.2, A9.3.1	Information security awareness, education and training , Use of secret authentication information		
9.5	**Privileged Access**				
AM 31	Use of privileged account is documented, controlled and accountable and kept to a minimum.	A 12.4.3, A 9.2.3	Administrator and Operator logs, Management of Privileged Access Rights	7.1.4, 7.2.2	Require documented approval by authorized parties specifying required privileges. Assignment of privileges to individuals based on job classification and function.
AM 32	System administrators are assigned an individual account for undertaking admin tasks	A9.2.3	Management of Privileged Access Rights		
AM 33	Only Qatari nationals have privileged access to systems processing information classified at C4 and above unless explicit authorization for exemption is given	A9.2.3	Management of Privileged Access Rights		
AM 34	System management log is updated to record mandated fields	A 12.4.1	Event Logging	10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges
9.6	**Remote Access**				
AM 35	Remote Access shall not be provided unless authorized explicitly by the dept head and only if warranted by biz requirements and only after due diligence has been performed to analyze associated risks	A6.2.2	Teleworking	12.3.9 , 12.3.10	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use, For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.
AM 36	2 factor authentication using a HW token, biometric control or similar is used when accessing systems processing data classified at C3 or above.			8.3	Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).
AM 37	Remote access sessions are secured by using suitable end-end encryption as specified in section C10	A6.2.2	Teleworking		
AM 38	Remote Access computers are equipped with a minimum protection (personal FW and AV) and activated at all times	A6.2.2	Teleworking		
AM 39	SW including security SW on these computers shall be patched and kept up to date				
AM 40	Users do not access Agency internal systems from public computers	A 6.2.1	Mobile device policy		
AM 41	Vendors remote access is limited to situations where there are no other alternatives. Such connections shall be controlled and monitored by State Agency and will be for defined period.			12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use
10	Cryptographic Security				

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
CY 1	Crypto Algorithms, encryption, encryption, HW/SW key management system, life times etc to meet the requirements specified in Appendix B of NIAM	A10.1	Cryptographic controls		
CY 2	Lifetime of the key SHALL be determined by the primarily by the application and the information infrastructure it is used in. Keys SHALL be immediately revoked and replaced if it has been or suspected of being compromised.				
CY 3	Info assets classified at C3 and above are encrypted and protected against unauthorized disclosures when stored and in transit.				
CY 4	Information assets classifed as I3 have ensured integrity by the use of hashing in line with approved algorithims				
CY 5	Transport protocols with approved algorithims in Appendix A			3.6.4 3.6.5	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.
CY 6	Passwords must always be encrypted/hashed and protected against un authorized disclosure when they are stored or in transit			8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.
CY 7	Only S/MIMEv3 or better used for securing emails				
CY 8	HSM are certified to at least FIPS 140-2 level 2 or Common Criterion CC3.1	A10.1.2	Key Management		
CY 9	Crypto keys are only physically moved in HSMs meeting CY7	A10.1.2	Key Management		
CY 10	Suitable key management processes are defined as per ISO11770-1 and used to manage the life cycle of crypto keys covering identified functions	A10.1.2	Key Management	3.6.1 3.6.2 3.6.3	Generation of strong cryptographic keys Secure cryptographic key distribution Secure cryptographic key storage
CY 11	Agency's SHALL ensure the digital certificates are compliant to standards in use by the CSP-PMA, MICT. Agencies SHALL use online revocation systems to minimize the risk of fraudulent use of digital certificates.	A18.1.5	Regulation of cryptographic controls		
CY 12	Security token/smartcard provisioning systems of CSPs meet requirements for Subject Device Provision Service specified in CWA14167-1	A18.1.5	Regulation of cryptographic controls		
CY 13	Any Digital certificate used in production system to be issued by Govt certified CSP	A18.1.5	Regulation of cryptographic controls		
11	Portable Devices & Working Off Site Security				
OS 1	Develop policies governing how Mobile Devices and Laptops can be used in the organization	A6.2.1	Mobile device Policy		
OS 2	Do not conduct classified conversation using MDs and laptops capable of conducting phone conversation while BlueTooth is enabled	A6.2.1	Mobile device Policy		

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
OS 3	MDs and Laptops with Bluetooth serial port connection do not have the port enabled if the device is to hold classified info	A6.2.1	Mobile device Policy		
OS 4	MDs with recording facilities are not allowed in controlled areas without prior approval from the SM	A6.2.1	Mobile device Policy		
OS 5	All laptops and MDs (where possible) encrypt information	A6.2.1	Mobile device Policy		
OS 6	MDs and Laptops should be kept under continual direct supervision when is use or kept secured when not in use	A6.2.1	Mobile device Policy	9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.
OS 7	MDs and Laptops not directly owned or controlled by Agencies shall not be used with Agency systems. MDs and Laptops not owned or controlled by Agency shall be managed and accounted for and accredited in the same manner as the Agency owned device. Agency laptops and MDs may be connected to non Agency network provide a suitable firewall is used to protect it against potential threats emanating from the host network	A8.1.3 A13.1.1	Acceptable use of assets, Network Controls	1.4	Install personal firewall software on any mobile and / or employee owned devices that connect to the internet when outside the network and which are used to access the network
OS 8	Unaccredited MDs and Laptops do not connect to Agency systems or store Agency's information. Temp connection is permitted as long as they are segregated from the main networks by firewalls	A6.2.1, A8.1.3 A13.1.1	Mobile device policy, Acceptable use of assets, Network Controls		
OS 9	In case of loss or theft of the MDs or laptops, the incident should be immediately reported	A6.2.1, A11.2.7	Mobile device policy, Secure disposal or reuse of equipment		
OS10	Emergency destruction / locking plan is in place for any MDs and laptops in situations where there is high probability of loss or compromise. For MDs this should be a remote capability	A8.3.2	Disposal of Media		
12	Physical Security				
PH 1	Appropriate protection for Physical space is determined based on assessment of risk. Assessment shall occur during the design phase of new construction or for existing work places as part of an on-going risk management process	A11.1	Secure area	9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
PH 2	Physical spaces are zoned depending upon the security requirement. Each zone is designated a physical security level.	A11.1.1	Physical security perimeter	9.1.1 , 9.3	Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law ,Control physical access for onsite personnel to sensitive areas as follows: Access must be authorized and based on individual job function. Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.
PH 3	Each physical zone has appropriate Physical controls implemented. Appendix A provides minimal baseline controls	A11.1.2	Physical entry contorls	9.2, 10.1	Develop procedures to easily distinguish between onsite personnel and visitors, to include: Identifying onsite personnel and visitors (for example, assigning badges) Changes to access requirements Revoking or terminating onsite personnel and expired visitor identification (such as ID badges). Implement audit trails to link all access to system components to each individual user.
PH 4	Implement clean desk and clean screen policy	A11.2.9	Clear desk and clear screen policy		

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
PH 5	SERver / Data rooms meet atlest the medium protection requirement	A11.1.3, A11.2.1	Secure offices, rooms and facilities, Equipment sitting and protection	9.3	Control physical access for onsite personnel to sensitive areas as follows: - Access must be authorized and based on individual job function. - Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.
PH 6	Cable carrying information upto level C3 is physically separate from those carrying Nationally classified info	A11.2.3	Cabling security		
PH 7	A site security plan and where necessary SOP for each server room are developed and implemented. SOP should follow the recommended guidelines	A11	Physical and environmental security	9.3 9.10	Control physical access for onsite personnel to sensitive areas as follows: -Access must be authorized and based on individual job function. -Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled. Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.
13	Virtualization				
VL 1	Evaluate the risks associated with the virtual technologies.	6.1.2, 6.1.3	Infromation security risk assessment, Information security risk treatment		
VL 2	Harden the hypervisor and related components as per the industry accepted best practices			2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.
VL 3	Enforce least privilege and separation of duties for managing the virtual environment.	A6.1.2, A9.1.1	Segregation of Duties, Access control policy		
VL 4	Ensure adequate physical security	A11.1.3	Securing offices, rooms and facilities	9.1, 9.1.2, 9.3, 9.4	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. Implement physical and/or logical controls to restrict access to publicly accessible network jacks. Control physical access for onsite personnel to sensitive areas as follows: -Access must be authorized and based on individual job function. -Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled. Implement procedures to identify and authorize visitors.
VL 5	augmentation by third party security technology				
VL 6	Segregate the Virtual Machines based on the classification of their data	A8.2	Information classification		
VL 7	A change management process encompasses the virtual technology environment.	A.12.1.2	Change management		

Mapping of NIA Policy Ver 2.0 to ISO 27001:2013 & PCI DSS v3.1

Ref Nos	Description	ISO 27001 Clause	ISO 27001 Clause Description	PCI DSS v3.1 clause	PCI clause description
VL 8	Monitor Logs from the virtual technology environment along with other IT infrastructure.	A.12.4.1	Event logging	10	Track and monitor all access to network resources and cardholder data