الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

# NATIONAL INFORMATION ASSURANCE STANDARD

[IAS-NAT-INFA]

MAY 2023

VERSION 2.1

**TOWARDS A SECURE**
CYBER SPACE

# "DISCLAIMER LEGAL RIGHTS"

National Cyber Security Agency (NCSA) has designed and created this publication, titled "National Information Assurance Standard" - V 2.1 , primarily as a guidance resource for senior management, IT management, risk management and IT and IT security professionals.

NCSA is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge NCSA as the source and owner of the "National Information Assurance Standard".

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the NCSA. NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

## Document Details

| | |
|---|---|
| ▸ **Document ID** | IAP-NAT-INFA |
| ▸ **Version** | V2.1 |
| ▸ **Classification & Type** | Public |
| ▸ **Abstract** | This document is intended to provide organizations within the State of Qatar with the necessary foundation and the relevant tools to enable the implementation of a full-fledged Information Security Management System within organizations. |

## Review/Approval

| Name | Dept./Role | Reviewed/Approved | Version | Date |
|---|---|---|---|---|
| **Dana Al Abdulla** | National Cyber Governance and Assurance Affairs | | **2.1** | May 2023 |

| Version | Author(s) | Revision Description | Date |
|---|---|---|---|
| **1.0** | ictQATAR | Published | January 2010 |
| **2.0** | MOTC | Published | February 2014 |
| **2.1** | NCSA – National Cyber Governance & Assurance Affairs | Published | May 2023 |

# "LEGAL MANDATE(S)"

Based on Amiri Decree No.1 for 2021 about the establishment of National Cyber Security Agency (NCSA), which aims to maintain and regulate national cyber security and to enhance and protect the vital interests of the state in the face of cyber threats, and according to Article No. (3) of the law, it is concerned with developing and updating policies, governance mechanisms, standards, controls and guidelines necessary to enhance cyber security in coordination with the concerned authorities, and circulating them the relevant authorities and follow-up commitment to them.

And within this context, this National Information Assurance Standard has been developed which aims to regulate and govern the data assurance and security in the organizations of State of Qatar and identify the basic principle in understanding the data governance and covering the important controls of protecting data through its lifecycle.

The adopting and implementation of this standard is the full responsibility of the organization. NCSA does not take any responsibility for to any damages related to un-informed decision of adopting and implementing this standard or out of the scope of this standard.

This standard has been developed based on the responsibilities assigned to NCSA as per Amiri Decree No.1 for 2021. In the event a conflict arises between this document (specific provision or clauses) and the laws of Qatar, the latter (law), SHALL take precedence. Any such term (specific provision or clauses), to that extent SHALL be deemed omitted from this document, without affecting the remaining provisions of this document. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

# TABLE OF CONTENTS

# 1. Introduction

## 1.1. Context

Information security is not only a technical issue, but also a business and governance challenge that involves risk management, reporting, and accountability. It is a top-down process requiring a comprehensive information security strategy that is explicitly linked to the organization's business processes and objectives.

Effective security requires the active engagement of executive management to address emerging threats and provide strong cyber security leadership. The term used to describe executive management's engagement is Information Security Governance. Information Security Governance consists of the set of policies and internal controls by which information security activities within an organization, irrespective of size or form, are directed and managed. Risk management, reporting, and accountability are core focus area of all information security policies and internal controls. Information security governance is a subset of an organization's overall corporate governance program.

For security to be effective, it must be included in all organizational and business processes from end to end - physical, operational, and technical. A formal information security strategy must be implemented by developing comprehensive information security policies consistent with the goals and mission of the organization. To provide effective governance, a set of enterprise standards for each domain must be developed to provide defined boundaries for acceptable processes and procedures. Education, training, and awareness must also be considered to convey information to all personnel as part of an ongoing process to change behaviors not conducive to secure, reliable operations.

The strategy must then be implemented through a comprehensive information security programme that includes well-conceived and complete policies and standards.

# 2. Purpose, Scope, Usage and Authority

## 2.1. Purpose

This standard specifies the security controls and requirements to be implemented by the organizations to comply with the security requirements of the National Data Classification Policy, together the two documents will help organizations in implementing a robust information security management system within their organization.

## 2.2. Scope

This standard applies to all Organizations and their corresponding information assets. Where the Organization has outsourced or subcontracted any processes or activities, they should ensure that the outsourced or sub-contracted processes or activities also comply with this standard and associated controls.

## 2.3. Usage

This NIA Standard is designed to be used in conjunction with the National Data Classification Policy [IAP-NAT-DCLS] and applicable laws and regulations within State of Qatar. The standard provides, baseline controls which an organization should implement at minimum to protect their information system. The controls are grouped in the following security domains:

- Access Control Security [AM]
- Audit & Certification [AC]
- Business Continuity Management [BC]
- Change Management [CM]
- Communications Security [CS]
- Cryptographic Security [CY]
- Data Labeling [DL]
- Data Retention & Archival [DR]
- Documentation [DC]
- Gateway Security [GS]
- Governance Structure [IG]
- Incident Management [IM]
- Information Exchange [IE]
- Logging, Auditing & Security Monitoring [SM]
- Media Security [MS]
- Network Security [NS]
- Personnel Security [PS]
- Physical Security [PH]
- Portable Device & Working Off-Site Security [OS]
- Product Security [PR]
- Risk Management [RM]
- Security Awareness [SA]
- Software Security [SS]
- System Usage Security [SU]
- Third Party Security Management [TM]
- Virtualization [VL]

Within this standard, baseline controls (indicated by '*') are mandatory and must be implemented, additional controls as deemed appropriate based on the security rating of the asset must also be implemented respectively. These form auditable items, against which conformance will be sought. Organizations may implement over and above the controls specified within this standard for added assurance. In case NIAS controls intersect with other Laws and regulations, Organization must consider compliance to both or whichever is providing higher degree of security.

The following steps are required to use this standard:

a. Use the National Data Classification Policy [IAP-NAT-DCLS] to classify all your information assets. This is a mandatory step before attempting to apply the controls outlined in this document.

b. Assets allocated security attributes of I0, A0 and C0 require no baseline controls. Some minimal controls MAY apply.

c. Assets allocated security attributes of I1, A1, C1 or above, require compliance to all control statements that are baseline at minimum; these are indicated by (*). All sections of the standard have positive impact on integrity, availability, and confidentiality of assets (to some degree), hence for each asset, the appropriate baseline controls should be implemented.

d. Assets allocated security attributes of I2, A2, or C2 require additional controls (one or more) per applicable domain based on the results of a Risk Assessment (see section B- 2, Risk Management [RM] for more details). This assessment needs to be undertaken before these additional controls are chosen.

e. Assets allocated security attributes of I3, A3, or C3 and higher require multiple additional controls (two or more) per applicable domain based on the results of a Risk Assessment (see section B- 2, Risk Management [RM] for more details). This assessment needs to be undertaken before these additional controls are chosen.

f. Implementation of the chosen controls needs to be undertaken for each asset. Implementation priority should be based on the aggregate security level (L, M, H), with High (H) assets being the highest priority for implementation.

## 3. Key Definitions

| | |
|---|---|
| ► **Organizations** | Refers to businesses operating within the State of Qatar. |
| ► **Personal Data** | Data that can be used to identify a person directly or indirectly |
| ► **Government Organization** | Organizations that report either to the Emiri Diwan, or the Prime Minister's Office, or the Council of Ministers, or to the Heir Apparent's Office. |
| ► **Hot/Warm/Cold Sites** | Sites used for recovery of enterprise systems and business operations, classified based on their readiness and availability |
| ► **National Classification Markings** | Data Classification Labels used to identify information sensitive from a national perspective. |

## 4. Security Governance & Security Processes

This section provides controls on how Security Governance should be established in an Organization. It also highlights some of the key activities that need to be established to ensure security is maintained to this baseline standard. The activities covered are Risk Management, Third Party Security Management, Data Labelling, Change Management, Personnel Security, Security Awareness, Incident Management, Business Continuity Management, Logging, Auditing & Security Monitoring, Data Retention & Archival, Documentation, and finally Certification.

### 1. Security Governance [IG]

#### 1.1 Objectives

The objective of this domain is to define an Information Security Governance structure for Organizations.

#### 1.2 Control Statements

To comply with this domain, Organizations SHALL:

IG 1. *Appoint a person to own and manage the Information Security programme. This person will be referred to as the 'Security Manager' within this NIA Standard.

IG 2. *Allocate appropriate budget to staff and operate the Information Security Programme.

IG 3. *Ensure the Security Manager has a reporting line to the Organization's senior management such as risk or internal audit function.

IG 4. *Ensure that the Organization head provides documented and continuous support for the development, implementation and ongoing maintenance of ICT security processes and infrastructure within their Organization.

IG 5. Where the Organization head delegates their authority to approve variations from requirements in this standard the delegate must have higher authority than the Security Manager.

IG 6. Define information security responsibilities for the Security Manager, management, employees and/or outsourced/3rd party vendors, suppliers or contractors of the Organization.

IG 7. *Ensure the Security Manager has:

a. ready access to, and full support from, executive management

b. familiarity with information security and/or ICT security

c. a general knowledge of, and experience in, or necessary resources in systems used by the Organization, especially operating systems, access & authorisation control systems/facilities and auditing facilities.

d. a reasonable capacity and competence to support the Security Manager role.

IG 8. Include the following responsibilities within the Security Manager's role:

a. identifying and recommending ICT security improvements to all business systems and business processes.

b. ensuring ICT security aspects are considered as part of the change management process.

c. ensuring the coordinating of development, maintenance and implementation of all ICT security documentation, in conjunction with the business managers.

d. ensuring timely reporting and adequate participation in investigation for ICT security incidents, with NCSA.

IG 9. Ensure the Security Manager is responsible for:

a. ensuring the development, maintenance, updating and implementation of security risk management plans, system security plans and any security procedures used.

b. providing technical security advice involved with system development, acquisition,

c. implementation, modification, operation, support, and architecture

d. assisting the system manager to develop system security standards/policies

e. the certification of systems, when applicable

f. ensuring the Organization has an appropriate ICT security awareness and training program.

g. the regular review of system security, system audit trails and logs and the integrity of system configurations.

IG 10. Ensure the Security Manager is familiar with all security operating procedures relating to systems, including to the roles of system managers, system administrators and system users.

## 2. Risk Management [RM]

### 2.1 Objectives

This domain defines the requirement to conduct risk assessment to devise a suitable risk treatment plan for information assets, which have been classified as having an aggregate security level of Medium or High [IAP-NAT-DCLS] and keep the residual risk to an acceptable level depending on the Organization's risk appetite.

### 2.2 Control Statements

To comply with this domain, Organizations SHALL:

RM 1. *Define a risk assessment process to identify threats and vulnerabilities to critical information assets (identified with an aggregate security level of Medium or High).

RM 2. *Based on the assessment, define a risk treatment plan to address threats and vulnerabilities.

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 in the Organization.

RM 4. Ensure that the controls chosen in RM2 & RM3 are monitored for effectiveness on a periodic basis.

RM 5. Risk assessments should be integrated within the business process and revised whenever there is a change. Changes in the business or legal/regulatory environment may also warrant the need to do risk assessment.

## 3. Third Party Security Management [TM]

### 3.1 Objectives

This domain defines the requirement to maintain security controls specified in this NIA Standard for service(s) that have been outsourced to a third party.

### 3.2 Control Statements

To comply with this domain, Organizations SHALL:

TM 1. *The areas or services being outsourced remain the governance, compliance and risk management accountability of the Organization.

TM 2. *They understand and acknowledge the risks associated with the outsourcing of their services.

TM 3. That the security controls specified in this NIA Standard are included in the third-party service delivery agreement or contract. This SHALL also apply to sub-contractors used by the third party.

TM 4. The third party SHALL be contractually required to regularly report on the outsourced service'(s) security posture, including any incidents.

TM 5. The services, reports and records provided by the third party should be continuously monitored and reviewed, and audits should be conducted on defined periodic intervals.

## 4. Data Classification Label [DL]

### 4.1 Objectives

This domain provides a high-level data labelling methodology for all Organizations for the purpose of understanding and managing data and information assets about their level of classification. The domain explains the methodology and the processes for effective data labelling.

The rationale for labelling information assets per their classification levels is to ensure the Organization and the designated users of the information assets will be able to correctly identify and adequately allocate resources for the protection of the information assets.

### 4.2 Control Statements

Although this document provides an overall standard to achieve consistent data labelling, the Organization MAY be expected to extend these concepts to fit the needs of National Classification Markings.

To meet the requirements of this domain Organizations MUST:

DL 1. *Serve as a labelling authority for the data and information that it collects or maintains.

DL 2. *Rate all information assets in accordance with [IAP-NAT-DCLS]. All assets rated with a Confidentiality rating of C1, C2, C3, or C4 SHALL be suitably marked the data label of Internal, Restricted, Secret or Top Secret respectively.

DL 3. *By default, label information assets as 'Internal' unless they are specifically for public release or consumption or rated to a higher confidentiality level.

DL 4. Establish the data labelling system to support the "Need-To-Know" requirement, so that information will be protected from unauthorized disclosure and use.

DL 5. Establish data labelling education and awareness for its staff, employees, and contractors.

## 5. Change Management [CM]

### 5.1 Objectives

The purpose of the Change Management domain is ensuring no unauthorized changes are made to information systems to which may otherwise expose, disclose or threaten CIA of information. It is necessary to document, review, approve and implement changes in a formal process-oriented mechanism to minimize security or business risks and to derive maximum value from information resources.

### 5.2 Control Statements

To comply with this domain, Organizations SHALL:

CM 1. *Define and adhere to a documented change management process which may include

the following or similar change categories:

a. Planned Major Change. Examples of planned major changes are:

- Changes that result in business interruption during regular business hours
- Changes that result in business or operational practice change
- Changes in any system that affects disaster recovery or business continuity
- Introduction or discontinuance of an information technology service

b. Maintenance and Minor Changes. Examples of this type of change are:

- Application-level security changes/patches
- Operating system patches (critical, hotfixes, and service packs)
- Regularly scheduled maintenance
- Changes that are not likely to cause a service outage

c. Emergency and Unplanned Outage Changes. Examples of this type of change are:

- A severe degradation of service needing immediate action

- A system/application/component failure causing a negative impact on business operations
- A response to a natural disaster
- A response to an emergency business need
- A change requested by emergency responder personnel

CM 2. Establish a cross functional Change Management Committee which must include representation from security and risk divisions

CM 3. Document and approve all proposed changes through the relevant Change Management Committee.

CM 4. *Ensure that upon implementing any proposed change that may impact the security of the ICT system assess whether the system will require re-certification. The system MUST comply with baseline requirements at minimum even after change implementation. Risk analysis may be required to ensure residual risk at acceptable level. the

CM 5. All associated system documentation is updated to reflect the change.

CM 6. Emergency changes may be carried out based on a verbal/informed approval from the Change management committee Head and the Business process owner. However, post emergency, the standard procedure for documenting and risk analysis is to be applied.

## 6. Personnel Security [PS]

### 6.1 Objectives

The objective of this domain is to ensure that personnel (staff, vendors, contractors, and others) deployed with the Organizations are aware of their security responsibilities and that suitable controls are in place to mitigate risks arising out of human element.

### 6.2 Control Statements

To comply with this domain, Organizations SHALL:

PS 1. Ensure that the Human Resources (HR) processes are aligned with information security policies and initiatives of the organization.

PS 2. *Ensure the HR department documents security requirements and obligations and ways of working in HR standard, which is read, understood and available to all staff to ensure.

PS 3. *Obtain, manage, and retain information related to personnel with due care and due diligence, in line with the requirements for handling Personal Information as specified in the Personal Data Privacy and Protection Law.

PS 4. Ensure information security responsibilities are included as part of the employees' job responsibilities and job descriptions and are applied throughout an individual's employment within the organization.

PS 5. *Conduct adequate screening to ascertain the integrity of prospective candidates for employment and contractors (including sub-contracted workers). The Organization may further extend this exercise to existing employees as deemed necessary to satisfy conditions arising out of factors such as but not limited to "Change of employee responsibilities" or "Suspicion raised on the conduct of an employee".

PS 6. *Ensure that staff sign an agreement, on joining the Organization or when there is a change in job profile or duties, which outlines their security obligations and responsibilities. This SHALL include:

a. Confidentiality and non-disclosure obligations.

PS 7. Ensure that adequate controls are in place to prevent personnel (employees, vendors, contractors, and visitors) from making unauthorized disclosures, misusing or corrupting information as per Organization security policies.

PS 8. Ensure that users access rights are restrictive to the information they need to fulfill their job requirements as per least privilege and need to have principles.

PS 9. Implement a split of responsibilities over sensitive security processes and tasks, using the 'four eyes' principles to ensure knowledge sharing and to avoid a single individual having full control over critical processes or tasks.

PS 10. *Define, communicate, and enforce a disciplinary process and ensure that employees are made aware of the process. Disciplinary processes SHOULD be documented in the employee or HR standard.

PS 11. *Ensure that vendors, contractors, delegates, or guests visiting Organization premises are:

a. Logged with unique identifiable information including date, time and purpose of admittance.

b. Provided with a visitor badge or identification tag.

c. Wearing a noticeable sign displaying their status as "visitor" at all times.

d. Made aware of their obligations in complying with the security policies of the Organization.

e. Escorted by Organization employees while accessing secure areas.

PS 12. *Ensure that a change request from the HR department is generated when a change of duties or termination of contract of an employee, contractor or third party occurs. This ensures that employees, contractors and third parties return Organization assets and physical & logical access are amended/removed as appropriate.

## → 7. Security Awareness [SA] ▼

### 7.1 Objectives

The purpose of this domain is to define criteria for a security training and awareness program conducted by the Organization for its employees, contractors, temporary personnel, and other entities who may use or administer the Organization's Information System assets.

### 7.2 Control Statements

To meet the requirements of this domain Organizations MUST:

SA 1. *A security awareness programme is defined and adequate budgets are allocated for its implementation.

SA 2. *As a minimum, such training includes

a. Baseline requirements specified in this NIA Standard
b. Organization's security requirements
c. Legal and regulatory responsibilities
d. Business specific processes and controls
e. Acceptable use of information processing facilities, (e.g., log-on procedures, use of software packages, etc.)
f. Information on the enforcement and disciplinary process
g. Information on who to contact for further security advice and the proper channels for reporting information security incidents

SA 3. *All employees of the Organization and, where relevant, contractors and third-party users receive appropriate security awareness training regarding the Organization's policies and procedures, as relevant for their job function, roles, responsibilities and skills.

SA 4. Employees should be trained to recognize social engineering attempts on them and not disclose any information that could violate the Organization's security policies, such as during social gatherings, public events, and training events.

SA 5. Contents of the security training and awareness are reviewed and updated regularly to reflect new trends, new threats, and changes to the Organization's information technology infrastructure or applicable laws and regulations.

SA 6. New employees are provided information security awareness training as part of the employee induction process and refresher training must be conducted on periodic basis.

SA 7. Training is followed up with an assessment, to ascertain the effectiveness of the programme, including maintaining of records of attendance of security awareness programmes.

SA 8. Indirect media such as posters, intranet, email, etc. may be used effectively to support the awareness programme.

## 8. Incidents Management [IM]

### 8.1 Objectives

An information security incident is an event that impacts on the confidentiality, integrity or availability of an information system or network, through an act that contravenes prescribed security policy and or applicable laws or regulations.

For the purposes of this standard, an incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

This standard intends to provide a reference for the Organization's management, administration, and other technical and operational staff to facilitate the development of information security incident management capability, and to be used for preparation for, detection of and response to information security incidents.

### 8.2 Control Statements

To meet the requirements of this domain Organizations MUST:

IM 1. *Appoint a person to own and manage the Incident Management programme, including a point of contact for all information security communications.

IM 2. Establish an information security incident response capability, based on the [IAP-NAT-DCLS] which can make a periodic risk assessment (from threat, vulnerability, and asset value) of data, processes, systems and networks in accordance with this Information Assurance Standard.

IM 3. *Define procedures to detect, evaluate and respond to incidents.

IM4. Define procedures to report, manage and recover from information security incidents, internally, with NCSA and with other support organizations including Law Enforcement Agencies.

IM 5. *Create awareness amongst its staff to report incidents.

IM 6. Categories and prioritize all incidents based on the type of attack and the criticality of the impacted systems.

IM 7. Co-ordinate with NCSA to create a repository of incidents in the Organization.

IM 8. *Report all Critical incidents to NCSA within two (2) hour of incident identification.

IM 9. The Incident Management coordinator is responsible for developing and executing an annual Security Assurance Plan. This may include activities such as penetration testing, audit of security procedures, and incident scenario testing.

## 9. Business Continuity Management [BC]

### 9.1 Objectives

This document provides Organizations with guidance in the development and implementation of a comprehensive Business Continuity (BC) plan to enable organizations to recover, operate and deliver essential business processes and services including information technology services.

### 9.2 Control Statements

To meet the requirements of this domain Organizations MUST:

BC 1. *A person is appointed to own and manage the Business Continuity Program.

BC 2. *A Business Continuity (BC) Plan is prepared to ensure continuance of critical processes and the delivery of essential services to an acceptable level. This plan SHALL include and be based on Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each Organization process.

BC 3. The BC Plan covers disaster scenarios possible and adequate and includes disaster recovery provisions.

BC 4. *The BC Plan is maintained and updated to reflect the current status and requirements and relevant information is made available for all team members, employees and service providers.

BC 5. A copy of the up-to-date BC Plan along with the necessary backup data tapes media and information is stored in a fire/tamper proof safe, along with an additional copy stored in an off-site location. Best practices state that offsite location must be in a geographically different zone than the primary data centre.

BC 6. They identify alternate disaster recovery sites, whose readiness is determined by the RTO requirements. These sites may be Hot/Warm/Cold Sites depending upon the Organization's requirements.

BC 7. They specify strong controls in contracts that involve outsourcing a portion of their business or information technology functions or business continuity services.

BC 8. The BC Plan is periodically tested at least on an annual basis or when significant changes take place in the business or legal/regulatory requirements.

BC 9. *Awareness about the BC plan is created amongst its employees.

## 10. Logging and Security Monitoring [SM]

### 10.1 Objectives

This The aim of this domain is to provide requirements for logging and monitoring to identify unauthorized data, application and resource access and to detect unauthorized changes or access privileges abuse.

### 10.2 Control Statements

To meet the requirements of this domain Organizations MUST:

SM 1. *Adequate set of technical control implementations, or processes exist for logging, identification and continuous monitoring of access, changes, command execution to, any/all information assets for protection of business sensitive information.

SM 2. *Monitoring practices are established in accordance with criticality of the infrastructure, data, and applications. It is RECOMMENDED to provide a 7/24 monitoring for C3, I3 and A3 classified infrastructures and ensure that monitoring responsibilities are allocated as specified in clause PS9, section B- 6, Personnel Security [PS].

SM 3. Monitoring activity is in line with regulatory and legal frameworks such as the proposed Information Privacy & Protection Law and SHALL cover use or access to systems.

SM 4. *They enable logging on all infrastructure and data processing equipment, and applications that are associated with the access, transmission, processing, security, storage, and/or handing of information classified with a confidentiality rating of C2 and above.

SM 5. They classify all security logs with a confidentiality rating of C3, while application and system logs SHALL be classified in accordance with the confidentiality rating of the system.

SM 6. Logs containing Personal Information have appropriate privacy protection measures in place, in accordance with the Proposed Information Privacy & Protection Legislation.

SM 7. *These logs are retained for a minimum of hundred and twenty (120) days and a maximum depending on criticality assessments and sector specific laws and regulations.

SM 8. Organization's MUST enable audit logging or log capture, to record date, time, authentication activity with unique user and system identifiers, including all failure or change actions, further including commands issued and output generated to provide enough information to permit reconstruction of incidents and move system to its original state.

SM 9. Exceptions are identified and reported in accordance with the Incident Handling policy, as defined in section B- 8, Incident Management [IM].

## 11. Data Retention and Archival [DR]

### 11.1 Objectives

The objective of the domain is to provide direction on setting up the retention period for information and the necessary security controls to protect information in its lifetime.

### 11.2 Control Statements

To meet the requirements of this domain Organizations MUST:

DR 1. *They determine and document the retention periods of suitable information assets including but not limited to the critical information assets that they hold. Data retention periods SHALL, at a minimum, be governed by:

a. Organization policies & needs

b. Regulatory requirements

c. Legal requirements

DR 2. *Data, which needs to be retained, is stored ensuring confidentiality, integrity and availability and that it can be accessed for defined future purposes.

DR 3. Personal and sensitive Information is not retained for longer than it is necessary as per the Proposed Information Privacy & Protection Legislation.

DR 4. Processes for backup, archival and recovery of data have corresponding procedures which ensure that the integrity and confidentiality of the data is retained.

DR 5. *Archived data retains it classification markings and is secured accordingly.

DR 6. The archiving technology deployed is regularly reviewed to ensure that it does not suffer from obsolescence and archived data is maintained in a state that allows successful recovery.

## 12. Documentation [DC]

### 12.1 Objectives

The objective of this domain is to define the minimum set of security documentations that an organization needs to produce, as well as how these documents should be protected and maintained.

### 12.2 Control Statements

To meet the requirements of this domain Organizations MUST:

DC 1. *Produce an organization security policy, incorporating the requirements of this NIA Standard.

DC 2. Ensure that every system that is determined to be critical to the Organization is covered by a system security plan/standard. Organizations SHOULD ensure that, where necessary, security operating procedures are created and documented.

DC 3. Ensure system security standards and procedures are aligned and consistent with the Organization's security policies and objectives.

DC 4. *By default, classify ICT security documentation as a minimum of C3/RESTRICTED

DC 5. *Review and update documentation periodically to ensure that they are up to date and current.

## 13. Audit & Certification [AC]

### 13.1 Objectives

The objective of this domain is to ensure that an adequate governance and security improvement program is established and managed by the organization, which is in compliance with the National Data Classification Policy [IAP-NAT-DCLS] and this National Information Assurance Standard

### 13.2 Control Statements

To meet the requirements of this domain Organizations MUST:

AC 1. *Ensure the establishment of a governance and security improvement programme in compliance with the National Data Classification Policy [IAP-NAT-DCLS] and this NIA Standard.

AC 2. *Comply with relevant provisions of Government Laws and regulations that exist at the time and those, which may be amended and / or added later in time.

AC 3. *Be audited by the Accredited audit organization, designated by NCSA.

AC 4. *Ensure that an audit of its Information System (infrastructure, people, and processes) is carried out at least once every year or whenever it undergoes a change that may impact the security of the Organization.

AC 5. *Ensure that the identified scope of the audit process is approved by the NCSA, and includes all information assets, people, and processes.

AC 6. *Ensure that recertification is carried out where any change or new finding invalidates or calls into question the current accreditation. Full certification is required for major changes affecting the basic security design of a system and a partial process is needed where the change is moderate or affects two or more security requirements.

AC 7. *Ensure that all non-conformance is fixed in a defined timeline.

AC 8. *Ensure that any exemptions are approved by the competent department within the NCSA.

# 5. SECURITY CONTROLS

This section of the NIA Standard covers mainly technical control areas that a Organization needs to implement as baseline security to be compliant to this NIA Standard. The areas covered are Communications Security, Information Exchange, Gateway Security, Product Security, Software Security, System Usage, Media Security, Access Control, Cryptographic Security, portable devices, working off-site and Virtualization.

## 1. Communication Security [CS]

### 1.1 Objectives

The objective of the domain is to ensure Organizations take the necessary measures to ensure potential emanation security and physical security weaknesses associated with cabling is minimized.

### 1.2 Control Statements - Cabling

To meet the requirements of this domain Organizations MUST:

CS 1. Advise users of the maximum permitted classification level for conversations of both internal and external telephone connections, as determined by the examination of the internal telephone system and the level of the encryption, if any, on external connections.

CS 2. *Separate cabling distribution is used for systems dealing with information classified at C4 and above

CS 3. Conduits installed in public, or visitor areas are not labelled in a manner that attract undue attention by people who may not have the appropriate security clearances or a need-to-know of the existence of such cabling

CS 4. *They maintain a register of cables. The register SHOULD record at least the following:

a. cable identification number,

b. classification,

c. source,

d. destination, and

e. floor plan diagram.

CS 5. *Inspect cables for inconsistencies with the cable register on a regular basis

CS 6. Organization's MAY provision for redundant communication pathways to ensure continued connectivity.

### 1.3 Control Statements – Telephones and Faxes

To meet the requirements of this domain Organizations MUST:

CS 7. Advise users of the maximum permitted classification level for conversations of both internal and external telephone connections, as determined by the examination of the internal telephone system and the level of the encryption, if any, on external connections

CS 8. *Ensure that the speakerphone feature is disabled during telephonic/video conversations where information classified at C3 or above is likely to be discussed and where it may be overheard.

CS 9. *Ensure that remote initiation of conferencing equipment is not enabled where it is installed in a sensitive location.

CS 10. *Ensure that rooms designated for communication of sensitive material or information, or meetings have appropriate controls for preventing the leakage of sound.

CS 11. *Ensure that fax machines on both ends are secured using encryption devices, while sending information classified as C2 and above.

CS 12. Ensure that all of the standards for the use of fax machines are met at both ends for the level of classification to be sent, and the sender makes arrangements for the receiver to:

a. collect the information from the fax machine as soon as possible after it is received, and

b. notify the sender if the fax does not arrive within an agreed amount of time, e.g., 10 minutes.

## 2. Network Security [NS]

### 2.1 Objectives

This domain establishes the baseline for the general use and connection of IT networks. Networks have opened the doors to unlimited processing by sharing and inter connection of devices and given birth to concepts like distributed applications, GRID systems etc. However, the introduction of networks has posed a slew of concerns, the security of multiple systems as well as the security of the interconnecting network is equally important, especially if public access wide area networks are used.

The risks of connecting to outside networks must be weighed against the benefits. It may be desirable to limit connection to outside networks to those hosts that do not store sensitive material and keep vital machines isolated.

### 2.2 Control Statements – Network Management

To meet the requirements of this domain Organizations MUST:

NS 1. *Details of internal network and system configuration, employee or device related directory services and other sensitive technology are not publicly disclosed or enumerable by unauthorized personnel.

NS 2. They remove or disable all the default accounts e.g., root, administrator, etc. or change the password as specified in section C6-, Software Security [SS].

NS 3. Network configuration is kept under the control of the network manager or similar and all changes to the configurations are:

a. approved through a formal change control process as defined in section B- 5, Change Management [CM]

b. documented, and comply with the network security policy and security plan as defined in section B- 12, Documentation [DC].

c. regularly reviewed. Old configurations as mandated by the Organization's procedures are maintained as part of change revision. The frequency of reviewing configuration shall depend on the Organization risk and processes.

NS 4. *For each managed network the Organization has:

a high level diagram showing all connections into the network, and a logical network diagram showing all network devices. processes to update NS4 (a) & (b), as network changes occur include a "Current at <date>" label on each page.

NS 5. *Networks are designed and configured to limit opportunities of unauthorized access to information transiting the network infrastructure. Organizations SHOULD use the following technologies to meet this requirement:

a. switches instead of hubs,

b. port security on switches to limit access and disable all unused ports

c. routers and firewalls segregating parts of the network on a need-to-know basis,

d. IPSEC/IP Version 6

e. application-level encryption

f. an automated tool that compares the running configuration of network devices against the documented configuration

g. network edge authentication

h. Restrict and manage end-user devices communicating to Organization network through techniques such as MAC address filtering.

i. IPS/IDS to detect/prevent malicious activity within the network

j. Time and day restriction.

NS 6. *Management networks adopt the following protection measures:

a. dedicated networks are used for management devices, i.e. implement a separate management VLAN, or physically separate infrastructure,

b. secure channels e.g., by using VPNs, SSH, etc.

### 2.3 Control Statements – Virtual LANs (VLANs)

To meet the requirements of this domain Organizations MUST:

NS 7. VLANs are used to separate IP telephone traffic, in business critical networks.

NS 8. *Administrative access is only permitted from the most highly classified VLAN to one at the same level of classification or of lower classification.

NS 9. *They implement all security measures recommended by the Organization's risk assessment and the hardening guidelines by the vendor of the switch.

NS 10. *Trunking/port mirroring SHALL not be used on switches managing VLANs of differing classifications.

### 2.4 Control Statements – Multifunction Devices (MDFs)

To meet the requirements of this domain Organizations MUST:

NS 11. *Network-connected MFDs are not used to copy documents classified above the level of the connected network

NS 12. Where network connected MFDs have the ability to transmit information via a gateway to another network, Organizations MUST ensure that:

a. each MFD applies user identification, authentication and audit functions for all information transmitted by users from that MFD,

b. these mechanisms are of similar strength to those required for workstations on that network, and

c. *the gateway can identify and filter the information in accordance with the requirements for the export of data.

NS 13. *There is no direct connection from an MFD to a telephone network of a lower classification unless the MFD has been evaluated, and the scope of the evaluation includes:

a. information flow control functions to prevent unintended and unauthorized data flows,

b. data export controls capable of blocking information based on information classification,

c. authentication, and audit data generation and protection

NS 14. They deploy MFDs after developing a set of policies, plans and procedures governing the use of the equipment.

NS 15. Information classified at C1 or above is not retained permanently in the MFD. Where the MFD has features to schedule jobs, sufficient standard/automatic controls or configurations SHALL exist to

remove the information from its memory once the job is complete.

NS 16. MFDs follow the procedures specified in section C, 8.3, Media Sanitization.

### 2.5 Control Statements – Domain Name Service (DNS) Servers

To meet the requirements of this domain Organizations MUST:

NS 17. A separate internal DNS server is set up and placed in the internal network for internal domain information that is not disclosed to the Internet.

NS 18. DNS information that should be made public either has a locally hosted and secured (bastion server) server. Government Organizations may also use the Government DNS which is part of the Government Network as the Primary DNS.

NS 19. DNS servers are deployed to ensure there is no single points of failure in their service, they are security-hardened, and security is proactively maintained.

NS 20. *Zones files are digitally signed, and cryptographic mutual 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 are provided to authorized users only.

NS 23. *Cryptographic functions related to NS 20 and NS 21 above, use a hardware security module for both key management and cryptographic processing as specified in section C- 10, Cryptographic Security [CY].

### 2.6 Control Statements – Internet Security

To meet the requirements of this domain Organizations MUST:

NS 24. All software and files downloaded from the Internet are screened and verified against malicious software, including mechanisms to scan HTTP traffic.

NS 25. *The Internet gateway denies all Internet services unless specifically enabled.

NS 26. Web browsers running on user's workstation are properly configured and updated. Organizations SHOULD reference the following guidelines when configuring web browsers:

a. Disable any active content options, e.g. Java, JavaScript and ActiveX, in the email application/ browser, except when communicating with a trusted source

b. Use up-to-date browser versions and apply latest security patches

c. Disable password auto-complete/password remembering features

d. Enable pop-up blocking features, except when communicating with trusted sites

e. Regularly remove cache files or temporary files of the browsers to protect data privacy

f. Disable automatic installation of plug-ins, add-ons, or software

NS 27. *They have the capability needed to monitor the traffic, deduce traffic patterns, usage etc. See section B- 10, Logging & Security Monitoring [SM] for more information.

### 2.7 Control Statements – EMail Security

To meet the requirements of this domain Organizations MUST:

NS 28. E-mail servers are hardened as per best practices and configured as a bastion server. If technically and operationally feasible, information revealing the specific details of internal systems or configurations MUST be avoided in email headers to avoid the disclosure of system information to external parties.

NS 29. TLS protection is used with the SMTP Mail server in line with section C10-, Cryptographic Security [CY].

NS 30. *They implement the email Sender Policy Framework (SPF) [RFC4408]. Organizations SHOULD only send 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 to reduce the risk of unsolicited email.

NS 32. Email gateways are employed to scan all incoming and outgoing emails to ensure it complies with the Organization's security policy and that it is free of any malicious code.

### 2.8 Control Statements – Wireless Security

To meet the requirements of this domain Organizations MUST:

NS 33. *Where wireless LANs (WLANs) are used, they are used with sufficient authentication and transmission encryption measures in place, complemented by proper security management processes and practices.

NS 34. *Strong wireless security protocols such as WPA2 and EAP-TLS are used. However, such wireless security protocol should not be solely relied upon to protect data confidentiality and integrity. Organization SHALL deploy dynamic key exchange mechanisms, secure Virtual Private Network (VPN) on top of wireless network if classified data, C3 and above, is to be communicated over wireless networks. WEP SHALL NOT be implemented within any network.

NS 35. *A good inventory of all devices with wireless interface cards is maintained. Once a device is reported missing, consider modifying the encryption keys and SSID.

NS 36. *Network administrators regularly scan for "rouge" or "unauthorized" wireless access points.

NS 37. Access points are located to minimize network tapping from publicly accessible area.

NS 38. The client-side settings for 802.1x MUST be secured. Some of the techniques are server certificate validation by selecting the CA certificate, specify the server address and disable it from prompting users to trust new certificates or servers.

NS 39. *The network default name, encryption keys and Simple Network Management Protocol (SNMP) community strings (and any insecure configuration) is changed at installation. SSID SHALL NOT reflect the name of any Organization's departments, system name or product name.

NS 40. For non-public wireless access points, encryption keys are regularly changed and SSID broadcasting is disabled. Where applicable MAC address filtering SHOULD also be considered.

NS 41. *A firewall or router is in place between the access point and the Organization's network to filter connections. Restricted firewall rules MUST be applied to allow only needed ports to pass from the wireless segment.

NS 42. WIPS/WIDS installation is recommended for networks with C+3 to monitor threats from wireless installations like rouge Aps, DOS attacks, etc.

NS 43. Use multiple SSIDs with different configurations for different VLANs, client authentication methods, etc. For example, contract staff or guest may use a different WIFI connections. Guest WIFI may have lower security and may only allow for connecting to the internet.

### 2.9 Control Statements – Clock Synchronization

To meet the requirements of this domain Organizations MUST:

NS 44. NTP servers MUST be secured as per best practices.

NS 45. *Where a computer or communications device has the capability to operate a real-time clock, it shall be set to an agreed standard, e.g., Universal Coordinated Time (UTC) or local standard time. As some clocks are known to drift with time, there shall be a procedure that checks for and corrects any significant variation.

NS 46. Government Organization'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 the local Organization NTP server which is synchronized as specified in NS45 and NS46.

### 2.10 Control Statements – Virtual Private Network (VPNs)

To meet the requirements of this domain Organizations MUST:

NS 48. VPNs carrying classified data at C3 or above, SHALL authenticate using two-factor authentication:

- First one a one-time password authentication such as a token device or a public/private key system with a strong passphrase
- Second username and password using external authentication server (LDAP, Radius, TACACS .etc.)

NS 49. VPNs disconnect automatically from Organization's network after a pre-defined period of inactivity. The user SHALL be required to logon again to reconnect to the network.

NS 50. *Dual (split) tunnelling is not permitted unless suitable controls are in place. Organizations SHOULD only permit one network connection at a time.

NS 51. All computers connected to a Organization's networks via VPN are equipped with personal security software, latest security patches, anti-virus software and malicious code detection and repair software. This security software SHALL be activated at all times and with the latest virus signatures and malicious code definitions.

NS 52. Gateway-level firewalls are installed to control network traffic from VPN clients to authorized information systems or servers.

### 2.11 Control Statements – Voice over IP Security (VoIP)

To meet the requirements of this domain Organizations MUST:

NS 53. Voice and data are separate networks. The separation SHOULD be physical, but use of Virtual LANS is permitted. The voice gateway, which interfaces with the PSTN segregates H.323, SIP, or other VoIP protocols from the data network.

NS 54. VoIP capable gateways and other appropriate security mechanisms are employed.

NS 55. *They evaluate and use security enabled protocols such as Secure Real Time Protocol (SRTP) and disable unnecessary voice protocols.

NS 56. *Proper physical counter measures are in place to protect the VoIP infrastructure.

NS 57. *Adequate call log monitoring is implemented.

NS 58. *Soft phones, if permitted are through a secure connection. e.g. secure VPN.

NS 59. Backup power is provided to POE VoIP phone devices in case of failure of power.

NS 60. Strong authentication and access controls are implemented to protect the voice gateway system.

NS 61. IPSEC or Secure Shell (SSH) is used for all remote management and auditing access.

NS 62. Contingency plans for making voice calls are developed if VoIP systems become unavailable.

NS 63. *Port security features are enabled on the network LAN switches that connect VoIP devices.

### 2.12 Control Statements – Internet protocol Version 6 (IPv6)

To meet the requirements of this domain Organizations MUST:

NS 64. *A proper risk assessment is conducted by the Organization to assess the security merits and demerits of IPv4 and IPv6 technology. Organizations SHOULD start considering IPv6 deployment.

NS 65. A proper risk assessment is conducted if the Organization decided to implement a dual-stack environment.

NS 66. Recertification is requested where Organizations deploy IPv6 in their network.

## → 3. Information Exchange [IE] ▼

### 3.1 Objectives

The purpose of this domain is to provide baseline security requirements when an organization is exchanging confidential information with other government Organizations or with other third parties.

### 3.2 Control Statements

To meet the requirements of this domain Organizations MUST:

IE 1. Prior to establishing cross-domain connectivity, the Organization evaluates, understands, and accepts the structure, security, and risks of other domains. This risk review SHALL be documented for compliance requirements.

IE 2. *When intending to connect an organization network to another secured network, they:

a. obtain a list of networks to which the other network is connected from the other network's Accreditation, Authority and System Manager,

b. examine the information from both sources to determine if any unintended cascaded connections exist, and

c. consider the risks associated with any identified cascaded connections prior to connecting the Organization network to the other network, particularly where a connection to an un-trusted network such as the internet may exist.

IE 3. Ensure that necessary agreements (specifically confidentiality agreements) between the entities exchanging information have been established prior to information exchange. Agreements SHALL provide information on responsibilities, information exchange notification procedure, technical standards for transmission, identification of couriers, liabilities, ownership, and controls. For vendors and 3rd parties a formal Non-Disclosure Agreement (NDA) SHALL be used. Appendix D provides an NDA template.

IE 4. Ensure media which is used to exchange information is protected against unauthorized access, manipulation, or misuse within or outside the Organization environment.

IE 5. Maintain the classification and protection of information that has been obtained from another Organization.

IE 6. Maintain appropriate levels of physical protection for media in transit and store in packaging that protects it against any hazard that would render the content unreadable.

IE 7. *Ensure only reliable and trusted courier service or transport organization SHALL be used based on a list of known and authorized couriers.

IE 8. *Protect information exchanged via electronic messaging from unauthorized access, change or interruption of service.

IE 9. Ensure secure messaging (information is digitally signed and/or encrypted) is used for all information classified at C3 or above. Organizations SHALL use Secure Multipurpose Internet Mail Extension (S/MIME), equivalent or better protocol for secure messaging as specified in clause CY5, section C- 10, Cryptographic Security [CY].

IE 10. *Attach the following email disclaimer, or similar, to all outgoing email:

"The information in this email, including attachments, may contain information that is confidential, protected by intellectual property rights, or may be legally privileged. It is intended solely for the addressee(s). Access to this email by anyone else is unauthorized. Any use, disclosure, copying, or distribution of this email by persons other than the designated addressee is prohibited. If you are not the intended recipient, you should delete this message immediately from your system. If you believe that you have received this email in error, please contact the sender or < Organization's name & contact information>. Any views expressed in this email, or its attachments are those of the individual sender except where the sender, expressly and with authority, states them to be the views of < Organization>."

IE 11. Exercise due diligence to ensure that any information sent/received is free of viruses, trojans and other malicious code

IE 12. Ensure information exchanged between systems is secured against misuse, unauthorized access, or data corruption. For transmitting information classified at C2, I2 or above, authenticated, and encrypted channels SHALL be used as specified in CY5, section C- 10, Cryptographic Security [CY].

IE 13. *Limit the information provided to the general public (via media outlets), to sanitized and approved information, through a designated and trained media relation spokesperson.

## 4. Gateway Security [GS]

### 4.1 Objectives

The main purpose of this domain is to provide minimum security requirement for securing gateways used for inter Organization communications as well as for external link communications.

The deployment of a controlled gateway can be used to ensure that only allowable information is transferred between the gateway and the connected networks. This can be used to preserve need-to-know requirements and to prevent malicious activities propagating from one network connected to another. Gateways include routers, firewalls, content filtering solutions and proxies.

### 4.2 Control Statements – General

To meet the requirements of this domain Organizations MUST:

GS 1. Networks are protected from other networks by gateways and data flows are properly controlled

GS 2. Gateways connecting Organization networks to other Organization networks, or to uncontrolled public networks, are implemented:

a. with an appropriate network device to control data flow

b. with all data flows appropriately controlled

c. with gateway components physically located within an appropriately secured server room.

GS 3. Only authorized and trained staff manage and maintain gateways

GS 4. *Administrative or management access to gateways processing or transmitting information classified at C3 or above is only provided based on dual control and the 'four eyes' principles.

GS 5. Information exchanged through gateways is labelled as per the National Information Classification policy [IAP-NAT-DCLS] and protected as specified in this document. Gateways SHALL be classified in line with the information they are transmitting.

GS 6. Demilitarized zones (DMZs) are used to separate externally accessible systems from uncontrolled public networks and internal networks via usage of firewalls and other network security capable equipment.

GS 7. Gateways:

a. are the only communications paths into and out of internal networks

b. by default, deny all connections into and out of the network

c. allow only explicitly authorised connections

d. are managed via a secure path isolated from all connected networks

e. provide sufficient audit capability to detect gateway security breaches and attempted network intrusions

f. provide real-time alarms.

GS 8. *Gateways are hardened prior to any implementation on production site and are protected against:

a. Malicious code and vulnerabilities

b. Wrong or poor configurations

c. Account compromise and privilege escalation

d. Rogue network monitoring

e. Denial of service (DoS) attacks

f. Information/data leakage

GS 9. *Monitoring and supervision of gateways is in place and include threat prevention mechanisms, logging, alerts, and surveillance of equipment. Section B- 10, Logging & Security Monitoring [SM].

GS 10. Gateways block or drop any data identified by a content filter as suspicious, including at least the following:

a. *Offensive language or attachments

b. Malware infected content

c. DoS attacks

d. *Categories of website/content defined as inappropriate in the proposed Cyber Crime Law including sites hosting obscene material, gambling sites, etc.

### 4.3 Control Statements – Data Export

To meet the requirements of this domain Organizations MUST:

GS 11. System users:

a. are held accountable for the data they export

b. are instructed to perform a protective marking check, a visual inspection and a metadata check if relevant on whether the information can be exported

GS 12. Data exports are either:

a. performed in accordance with processes and/or procedures approved by the Organization; or

b. individually approved by the information security manager.

GS 13. *Export of data to a less classified system is restricted by filtering data using at least checks on classification labels.

GS 14. *Data exports are checked, ensuring:

a. keyword searches are performed on all textual data

b. any unidentified data is quarantined until reviewed and approved for release by a trusted source other than the originator.

### 4.4 Control Statements – Data Import

To meet the requirements of this domain Organizations MUST:

GS 15. System users:

a. are held accountable for the data they import

b. are instructed to perform a protective marking check, a visual inspection and a metadata check if relevant.

GS 16. *Data imports are either:

a. performed in accordance with processes and/or procedures approved by the Organization; or

b. individually approved by the information security manager.

GS 17. *Data imported to a Organization system is scanned for malicious and active content.

## 5. Product Security [PR]

### 5.1 Objectives

This domain establishes the minimum security for selecting and acquiring information products through a proper selection and acquisition process. Organizations MUST ensure that selected products are chosen after an independent evaluation process that meets the security requirements listed in this domain.

### 5.2 Control Statements

To meet the requirements of this domain Organizations MUST:

PR 1. The 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 National Data Classification policy [IAP-NAT-DCLS].

PR 3. *The selection process includes proper identification of vendor, screening of vendors and evaluation criteria definition which should include as a minimum:

a. Vendor status and identification, including location and ownership

b. Financial situation

c. References from previous successful engagements

d. The ability of the vendor to build and/or maintain appropriate controls as determined by a risk assessment

PR 4. Proper testing and effective matching between vendor's claim and functionality are carried out, to avoid loss of confidentiality, integrity and/or availability.

PR 5. *Security evaluation of the product is done on a dedicated evaluation configuration including functionality tests, security tests and patching to protect against potential threats and vulnerabilities.

PR 6. Delivery of products is consistent with the Organization's security practice for secure delivery.

PR 7. Secure delivery procedures SHALL include measures to detect tampering or masquerading.

PR 8. *Products have been purchased from developers that have made a commitment to the ongoing maintenance of the assurance of their product.

PR 9. Product patching and updating processes are in place. Updates to of products SHALL follow the change management policies specified in section B- 5, Change Management [CM].

# 6. Software Security [SS]

## 6.1 Objectives

The purpose of this domain is to define the importance of including security in the process of software development and acquisition, rather than adding it as an add-on. This domain defines security as it applies to the various phases of the Software / System Development Life Cycle (SDLC). This domain also covers security controls for commercial applications deployed within an organization.

## 6.2 Control Statements – Software Development & Acquisition

To meet the requirements of this domain Organizations MUST:

SS 1. Security is considered in all phases of the SDLC and that it is an integral part of all system development or implementation project.

SS 2. *All applications (including new and developed) are classified using the National Data Classification Policy [IAP-NAT-DCLS] and accorded security protection appropriate to its Confidentiality, Integrity, and Availability ratings.

SS 3. Security requirements (functional, technical and assurance requirements) are developed and implemented as part of system requirements.

SS 4. *Dedicated test and development infrastructure (systems and data) are available and is separate from production systems. Furthermore, information flow between the environments SHALL be strictly limited according to a defined and documented policy, with access granted only to system users with a clear business requirement and write access to the authoritative source for the software SHALL be disabled.

SS 5. All applications (acquired and/or developed) are available for production use only after appropriate quality and security assurance tests and checks to ensure that the system confirms and complies with the intended security requirements.

SS 6. *Software developers use secure programming practices when writing code, including:

a. complying with best practices, for example the Mitre top 25 most dangerous programming errors [Mitre]

b. designing software to use the lowest privilege level needed to achieve its task

c. denying access by default

d. checking return values of all system calls

e. validating all inputs.

SS 7. Software should be reviewed and/or tested for vulnerabilities before it is used in a production environment. Software SHOULD be reviewed and/or tested by an independent party and not by the developer.

SS 8. System (acquired and/or developed) complies with all legal requirements including license, copyrights, IPR etc.

SS 9. All systems (acquired and/or developed) are adequately documented.

SS 10. *Source code of custom developed critical applications is available and in the case of commercial applications (serving critical applications / processes) a Organization SHOULD investigate options of arranging an escrow for the source code.

SS 11. Prior to commissioning of applications, they are certified as specified in section B- 13, Audit & Certification [AC].

### 6.3 Control Statements – Software Applications

To meet the requirements of this domain Organizations MUST:

SS 12. All server and workstation security objectives and mechanisms are documented in the relevant system security plan.

SS 13. *Workstations use a hardened standard operating environment (SOE) covering:

a. removal of unwanted software
b. disabling of unused or undesired functionality in installed software and operating systems
c. implementation of access controls on relevant objects to limit system users and programs to the minimum access needed to perform their duties
d. installation of software-based firewalls limiting inbound and outbound network connections
e. configuration of either remote logging or the transfer of local event logs to a central server.

SS 14. *Potential vulnerabilities in their SOEs and systems are reduced by:

a. removing unnecessary file shares
b. ensuring patching is up to date
c. disabling access to all unnecessary input/output functionality.
d. removing unused accounts
e. renaming default accounts
f. replacing default passwords.

SS 15. High risk servers e.g., Web, email, file and Internet Protocol telephony servers, etc. having connectivity to uncontrolled public networks:

a. maintain effective functional separation between servers allowing them to operate independently
b. minimise communications between servers at both the network and file system level, as appropriate
c. limit system users and programs to the minimum access needed to perform their duties.

SS 16. Check the integrity of all servers whose functions are critical to the Organization, and those identified as being at a high risk of compromise. Wherever possible these checks SHOULD be performed from a trusted environment rather than the system itself.

SS 17. Store the integrity information securely off the server in a manner that maintains integrity

SS 18. Update the integrity information after every legitimate change to a system

SS 19. *As part of the Organization's ongoing audit schedule, compare the stored integrity information against current integrity information to determine whether a compromise, or a legitimate but incorrectly completed system modification, has occurred.

SS 20. Resolve any detected changes in accordance with the Organization's information and communications technology (ICT) security incident management procedures.

SS 21. *All software applications are reviewed to determine whether they attempt to establish any external connections. If automated outbound connection functionality is included, Organizations SHOULD make a business decision to determine whether to permit or deny these connections, including an assessment of the risks involved in doing so.

### 6.4 Control Statements – Web Applications

To meet the requirements of this domain Organizations MUST:

SS 22. *All active content on their Web servers is reviewed for security issues. Organizations SHOULD follow the documentation provided in the Open Web Application Security Project (OWASP) guide to building secure Web applications and Web services.

SS 23. Connectivity and access between each Web application component is minimised.

SS 24. That Personal Information and sensitive data is protected whilst in storage and in transmission using appropriate cryptographic controls.

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.

### 6.5 Control Statements – Database

To meet the requirements of this domain Organizations MUST:

SS 27. All information stored within a database is associated with an appropriate classification if the information:

a. could be exported to a different system, or

b. contains differing classifications and/or different handling requirements.

SS 28. Organizations should ensure that classifications are applied with a level of granularity sufficient to clearly define the handling requirements for any information retrieved or exported from a database.

SS 29. *Database files are protected from access that bypasses the database's normal access controls.

SS 30. Databases provide functionality to allow for auditing of system users' actions.

SS 31. *System users who do not have sufficient privilege to view database contents cannot see associated metadata in a list of results from a search engine query. If results from database queries cannot be appropriately filtered, Organizations MUST ensure that all query results are appropriately sanitized to meet the minimum-security privilege of system users.

SS 32. Sensitive data in database shall be masked using data masking technology for C3 & above.

## 7. System Usage Security [SU]

### 7.1 Objectives

This domain establishes the need for Organizations to clearly define what behaviors and actions are permitted on their systems, and what is unacceptable. Organizations MUST ensure that system users have awareness training to ensure they understand their obligations.

### 7.2 Control Statements

To meet the requirements of this domain Organizations MUST:

SU 1. System users SHALL be responsible for the information assets (systems / infrastructure) 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 / Organization's Acceptable usage policy.

SU 2. System users will conduct due diligence when accessing the web and browsing the web SHALL strictly follow Organization principles and guidelines on accessing the internet. Organizations SHOULD consider whether usage of forums, social networks, etc is permitted or not.

SU 3. ICT assets are protected against web-based threats by implementing measures that will prevent downloading software programs, active content and non- business-related websites.

SU 4. Web access is provided through secure proxies and filtering gateways as defined in section C 4, Gateway Security [GS].

SU 5. *Staff is aware of the types of content permitted and restricted within the Organization, as specified in section B- 4, Gateway Security [GS]. Organizations SHOULD consider an effective solution for monitoring content of encrypted channels.

SU 6. Staff use e-mail with due diligence and include necessary classification labelling depending upon the content/attachments according to National Data Classification Policy [IAP-NAT-DCLS].

SU 7. Appropriate measures are taken that e-mail is protected against potential threats as viruses, trojans, spam mails, forgery and social engineering.

SU 8. *Staff is aware that web based public e-mail services are not allowed to be used to send and receive e-mails from Organization systems.

SU 9. Staff is aware that e-mails used to exchange confidential information SHOULD only be sent to named recipients and not to a group or distribution list.

SU 10. Staff is aware that the use of automatic forwarding of e-mails is dependent upon the sensitivity of their normal e-mails. Emails carrying information classified at C2 and above SHALL NOT be automatically forwarded outside to the Organization's systems.

SU 11. *When dealing with external parties, Organizations ensure that external recipients/originators understand and agree on the usage of classified data as defined in section C- 3, Information Exchange [IE].

## 8. Media Security [MS]

### 8.1 Objectives

The objective of this domain is to help Organizations to define how media can be classified, labelled, and registered to assist in properly identifying and accounting for it. The domain considers the whole lifecycle of the media from usage, repair, sanitization, and destruction to disposal.

### 8.2 Control Statements – Media Classification and Labelling

To meet the requirements of this domain Organizations MUST:

MS 1. Hardware containing media is classified at or above the classification of the information contained on the media

MS 2. Non-volatile media is classified to the highest classification of information stored on it

MS 3. *Volatile media that has a continuous power supply is classified to the highest classification of information stored on it while the power is on. Volatile media may be treated as classified C1 information once the power is removed from the media.

MS 4. Storage media is reclassified if:

a. information copied onto that media is of a high classification,

b. information contained on that media is subject to a classification upgrade

MS 5. Media holding classified information may be declassified after:

a. the information on the media has been declassified by the originator, or

b. the media has been sanitized in accordance with section C- 8.3, Policy & Baseline Controls - Media Sanitization

MS 6. If the storage media cannot be sanitized, then it cannot be declassified and MUST be destroyed.

MS 7. *The classification of all media is readily visually identifiable. Organizations SHOULD achieve this by labelling media with a protective marking that states the maximum classification as specified in section B4-, Data Labelling [DL]

MS 8. Classification of all media is easily visually identifiable. When using non-textual representations for classification markings due to operational security, Organizations SHALL document the labelling scheme and train staff members appropriately.

### 8.3 Control Statements – Media Sanitization

To meet the requirements of this domain Organizations MUST:

MS 9. *They document procedures for the sanitisation of media, which are regularly tested.

MS 10. All media types which contain information classified as C1 or above are destroyed prior to disposal:

a. microfiche & microfilm
b. optical discs
c. printer ribbons and the impact surface facing the platen
d. programmable read-only memory
e. read-only memory
f. faulty media that cannot be successfully sanitised.

MS 11. Volatile media is sanitised by:

a. removing power from the media for at least 10 minutes, or
b. overwriting all locations of the media with an arbitrary pattern followed by a read back for verification.

MS 12. *Non-volatile magnetic media is sanitised by:

a. overwriting the media, if pre2001- or under 15GB, in its entirety, with an arbitrary pattern followed by a read back for verification three times
b. overwriting the media, if post2001- or over 15GB, in its entirety, with an arbitrary pattern followed by a read back for verification one time; or
c. using a degausser with sufficient field strength for the coercivity of the media (NOTE: Degaussing may render some modern media unusable)

MS 13. Non-volatile EPROM media is sanitised by erasing as per the manufacturer's specification, increasing the specified ultraviolet erasure time by a factor of three, then overwriting the media once in its entirety with a pseudo random pattern. Sanitization of media with rating C3 & above SHOULD be documented.

MS 14. Flash memory media is sanitized by overwriting the media twice in its entirety with a pseudo random pattern, followed by a read back for verification.

### 8.4 Control Statements – Media Repairing & Maintenance

To meet the requirements of this domain Organizations MUST:

MS 15. *Appropriately vetted and briefed personnel carry out repairs and maintenance for hardware containing classified information.

MS 16. Repairs on systems containing classified information rated C3 or above are carried out under supervision.

### 8.5 Control Statements – Media Destruction & Disposal

To meet the requirements of this domain Organizations MUST:

MS 17. *They document procedures for the sanitisation of media, which are regularly tested.

MS 18. *Media is destroyed by:

a. Degaussing non-volatile magnetic media
b. breaking up the media
c. heating the media until it has either burnt to ash or melted.

MS 19. *Staff members supervise the destruction of media:

a. handling the media to the point of destruction
b. ensuring that the destruction is completed successfully.
c. C3 & above media destruction must be documented.

MS 20. Media, including faulty media, containing classified information is sanitised to the extent possible prior to disposal.

MS 21. *The disposal of media and media waste does not attract undue attention.

## 9. Access Control Security [AM]

### 9.1 Objectives

The objective of this domain is to establish the use and deployment of a variety of access control solutions to ensure the confidentiality, integrity, and availability of the Organization's information assets. This domain defines the rules necessary to achieve this protection, and to ensure secure and reliable operation of the Organization's information systems.

### 9.2 Control Statements – General

To meet the requirements of this domain Organizations MUST:

AM 1. Users will be provided access based on the concept of "least privilege" and governed by a "Need to Know" or a "Need to Have" basis.

AM 2. Access will be managed and controlled through system access controls, identification and authentication, and audit trails based on the sensitivity of the information. These request s for access SHALL be authorized by a staff member's supervisor or manager.

AM 3. *Access rights of a user or entity to create, read, update, delete or transmit a Organization's information assets SHALL be based on a matrix (hierarchical) model of rights defined by business rules established by the owners of that information.

AM 4. A process is established which, upon any employee role or status change (including termination), ensures that information system access is updated to reflect the employee's new role

AM 5. System users that need additional access to bypass security mechanisms for any reason seek formal authorisation from the Security Manager

AM 6. *Any unauthorized effort to circumvent the Organization's access control SHALL be perceived as a security incident and SHALL be handled in accordance with established incident handling procedure and/or appropriate human resources policies and procedures.

AM 7. Audit logs SHALL be enabled and maintained in such a manner as to allow compliance monitoring with government policy and to assist in Incident Management.

AM 8. *Logical access to Organization Networks is technically controlled. This MAY be by using Network Admission Control (NAC) services/devices.

AM 9. *Secure records are maintained of:

a. all authorised system users
b. their user identification
c. who provided the authorisation to access the system
d. when the authorisation was granted
e. maintain the record for the life of the system to which access is granted.

AM 10. *A logon banner is displayed before access to the system is granted. These banners SHOULD cover:

a. access is only permitted to authorised system users
b. the system user's agreement to abide by relevant security policies
c. he system user's awareness of the possibility that system usage is being monitored
d. the definition of acceptable use for the system
e. legal ramifications of violating the relevant policies.
f. Wherever possible requires a system user response, as acknowledgement

AM 11. *Centralised authentication repositories such as LDAP, authentication databases, etc. are protected from denial-of-service attacks and use secure and authenticated channels for retrieval of authentication data. Such repositories SHALL log the following events:

a. Unauthorized update/access
b. Start and end date and time of activity, together with system identifier
c. User identification (for illegal logon)
d. Sign-on and sign-off activity (for illegal logon)
e. Session/terminal or remote connection

### 9.3 Control Statements – Identification & Authentication

To meet the requirements of this domain Organizations MUST:

AM 12. They develop and maintain a set of policies, plans and procedures, derived from the National Data Classification Policy [IAP-NAT-DCLS], covering system users':

a. identification
b. authentication
c. authorisation

AM 13. They educate their system users of the Organization's policies and procedures.

AM 14. All system users are:

a. uniquely identifiable
b. authenticated on each occasion that access is granted to a system.

AM 15. *Individuals who are not employees, contractors, or consultants are not granted a user account or be given privileges to use the Organization's information resources or communications systems unless explicitly approved by the Security Manager who SHALL check that appropriate agreements, clearance and access forms have been completed.

AM 16. *That alternate methods of determining the identification of the system user are in place when shared/non-specific accounts are used.

AM 17. *Unprotected authentication information that grants system access, or decrypts an encrypted device is located on, or with the system or device, to which the authentication information grants access to.

AM 18. *System authentication data whilst in use is not susceptible to attacks including, but not limited to, replay, man-in-the-middle and session hijacking

AM 19. *A password policy enforcing either a minimum password length of 12 characters with no complexity requirement or a minimum password length of seven characters, consisting of at least three of the following character sets:

a. lowercase characters (a-z)
b. uppercase characters (A-Z)
c. digits (9-0)
d. punctuation and special characters

AM 20. *Passwords are changed at least every 90 days

AM 21. *System users cannot change their password more than once a day and the system force the user to change an expired password on initial logon or if reset.

AM 22. *Chosen passwords are checked to prevent:

a. predictable reset passwords
b. reuse of passwords when resetting multiple accounts
c. passwords to be reused within eight password changes
d. users to use sequential passwords

AM 23. *Screen and/or session locks configured to:

a. activate after a maximum of 15 minutes of system user inactivity
b. activate standardly by the system user, if desired
c. lock to completely conceal all information on the screen
d. ensure the screen does not appear to be turned off while in the locked state
e. have the system user re-authenticate to unlock the system
f. deny system users the ability to disable the locking mechanism.

AM 24. Access to a system is suspended after a specified number of failed logon attempts or as soon as possible after the staff member no longer needs access, due to changing roles or leaving the Organization.

AM 25. Lost, stolen, compromised passwords are immediately:

a. reported, to the Security Manager who SHALL ensure the corresponding account is suspended
b. changed upon user identity verification

AM 26. *Accounts that are inactive for more than three (3) months are suspended.

AM 27. *Accounts on systems processing information rated C2, I2, A2 or above are audited for currency on a six (6) monthly basis.

### 9.4 Control Statements – System Access

To meet the requirements of this domain Organizations MUST:

AM 28. Security policies document any access requirements, security clearances and briefings necessary for system access.

AM 29. *System users have been vetted as specified in section B- 6, Personnel Security [PS], before being granted access to a system.

AM 30. *System users have received any necessary briefings before being granted access to a system.

### 9.5 Control Statements – Privileged Access

To meet the requirements of this domain Organizations MUST:

AM 31. The use of privileged accounts is documented, controlled and accountable and kept to a minimum. Privileged accounts SHALL only be used for administrative work

AM 32. System administrators are assigned an individual account for undertaking their administration tasks

AM 33. *Only Qatari nationals have privileged access to systems processing information classified at C4 and above unless explicit authorisation for exemption to this policy is given.

AM 34. *System management log is updated to record the following information:

a. sanitisation activities
b. system start-up and shutdown
c. component or system failures
d. maintenance activities
e. backup and archival activities
f. system recovery activities
g. special or out of hours activities.

### 9.6 Control Statements – Remote Access

To meet the requirements of this domain Organizations MUST:

AM 35. Remote access SHALL NOT be provided unless authorized explicitly by the department head and only if it is warranted by business requirements and only after due diligence has been performed to analyse associated risks and suitable controls are implemented to mitigate the identified risks.

AM 36. *Two factor authentication, using a hardware token, biometric control or similar is used when accessing systems processing data classified at C3 or above.

AM 37. *Remote access sessions are secured by using suitable end-to-end encryption as specified in section C- 10, Cryptographic Security [CY].

AM 38. Remote access computers are equipped with at a minimum, a personal firewall and anti-malware software. These security controls SHALL be activated at all times.

AM 39. Software, including security software on these computers SHALL be patched and kept up to date.

AM 40. *Users do not access Organization internal systems from public computers e.g., Cyber Cafes etc. or print material to any public computer.

AM 41. Vendor remote access is limited to situations where there are no other alternatives. In this case, initiation of the connection SHALL be controlled and monitored by the Organization. Vendor remote access SHALL only be for a defined period of time, dictated by the duration of the task being undertaken.

## → 10. Cryptographic Security [CY] ▼

### 10.1 Objectives

This domain establishes the baseline for the use of encryption technologies for keeping information assets confidential and/or integral. As a custodian of public and confidential information, Organizations must further protect private and sensitive data/information from all cyber threats and vulnerabilities whether external or internal to the Organization.

### 10.2 Control Statements

To meet the requirements of this domain Organizations MUST:

CY 1. Cryptographic algorithms, encryption hardware/software, key management systems and digital signatures shall demonstrate compliance with the Approved Encryption/ Cryptographic Algorithms and Systems as specified by the competent authority within the Law No. (16) of 2010 on the Promulgation of the Electronic Commerce and Transactions Law.

CY 2. The 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. *Information assets classified as C3 [IAP-NAT-DCLS] are encrypted and protected against unauthorized disclosure when stored and/or in transit regardless of the storing format or media. Organizations MAY apply these cryptographic controls to assets with lower confidentiality requirements, if determined necessary by their risk assessment.

CY 4. Information assets classified as I3 [IAP-NAT-DCLS] have assured integrity using cryptographic hashing. Organizations MAY apply these cryptographic controls to assets with lower integrity requirements, if determined necessary by their risk assessment.

CY 5. *The following protocols or better, with approved algorithms outlined in "Qatar National Cryptographic Standard - English v1.0 (or higher)" issued by the competent authority, are used for securing data classified as C3 when in transit:

a. For securing web traffic: TLS (+128 bits) [RFC4346]

b. For securing file transfers: SFTP [SFTP]

c. For secure remote access: SSH v2 [RFC4253] or IPSEC [RFC 4301]

d. Only S/MIME v3 [RFC3851] or better are used for securing emails. See CY11 for associated requirement.

CY 6. *Passwords must always be encrypted/hashed and protected against unauthorized disclosure when they are stored and/or in transit regardless of the storing format or media. Privileged passwords SHALL be encrypted and stored off-site with backup files each time the password is changed to ensure complete recovery.

CY 7. *Where Hardware Security Modules (HSMs) are used, they are certified to at least FIPS 2-140 Level 2 [FIPS2-140-] or Common Criteria [CC3.1] EAL4.

CY 8. Cryptographic keys are only physically moved in HSMs meeting CY5

CY 9. Suitable key management processes are defined, as per [ISO1-11770] and used to manage the lifecycle of cryptographic keys, covering the following functions:

- Key Custodians Roles and Responsibilities
- Key Generation
- Dual Control and Split Knowledge
- Secure Key Storage
- Key Usage
- Secure Key Distribution and in Transit
- Key Backup and Recovery
- Periodic Key Status Checking
- Key Compromise
- Key Revocation and Destruction
- Audit Trails and Documentation

CY 10. Organization's SHALL ensure the digital certificates are compliant to standards in use by the CSP-PMA, MCIT. Organizations SHALL use online revocation systems to minimize the risk of fraudulent use of digital certificates.

CY 11. Security token/smartcard provisioning systems of CSPs meet the requirements for Subject Device Provision Services as specified in [CWA1-14167].

CY 12. *Any digital certificates used in a production system SHALL be issued by a CSP licensed in Qatar.

## → 11. Portable Devices & Working Off-Site Security [OS] ▼

### 11.1 Objectives

The main purpose of this domain is to specify the minimum requirements for mobile equipment (Mobile Devices (MDs) and laptops) when they are used within the vicinity of an Organization or when used in other uncontrolled environments.

### 11.2 Control Statements

To meet the requirements of this domain Organizations MUST:

OS 1. *They develop policies governing if, and how, Mobile Devices (MDs) and laptops can be used in their organisation.

OS 2. They do not conduct classified conversations using MDs and laptops capable of conducting phone conversations while using Bluetooth-enabled peripherals.

OS 3. MDs and laptops with Bluetooth serial port connections do not have the port enabled if the device is to hold classified information.

OS 4. MDs with recording facilities are not allowed into high-risk areas without prior approval from the Security Manager.

OS 5. *All laptops and MDs SHALL encrypt the information they carry and be password protected.

OS 6. *MDs and laptops SHALL be kept under continual direct supervision when in use or kept secured when not in use.

OS 7. *MDs and laptops not directly owned or controlled by the Organization are not used with the Organization's systems. MDs and laptops not owned or controlled by the Organization SHALL be managed, accounted for and accredited in the same manner as Organization owned devices. Organization MD's and laptops MAY be temporary connected to a non- Organization network provided a suitable firewall is used to protect the device from any potential threats originating from the non- Organization controlled network.

OS 8. Unaccredited MDs and laptops do not connect to the Organization's systems or store Organization information. However, temporary connected MDs and laptops are permitted provided they are segregated from the main networks by a firewall.

OS 9. *In case of loss or theft of the MDs or laptops, the incident should be immediately reported to the Information Security Manager / Office and the concerned Law enforcement Organizations. The loss / theft SHALL be handled as per the B8- Incident Management [IM]

OS 10. *Emergency destruction/locking plan /remote wipe/auto destruct is in place for any MDs and laptops.

## 12. Physical Security [PH]

### 12.1 Objectives

The objective of the domain is to ensure prevention of unauthorized physical access, damage, and interference to an Organization's premises and information. Organizations need to ensure that appropriate physical security measures and controls are adopted to meet the baseline requirements of this domain.

### 12.2 Control Statements

To meet the requirements of this domain Organizations MUST:

PH 2. Appropriate protection for physical space is determined based on an assessment of risk. This assessment SHALL occur during the design phase of a new construction or, for existing workplaces, as part of an on-going risk management process.

PH 2. Physical spaces are zoned depending upon their security requirement. Each zone is designated a physical security level. The table below specifies the levels:

**Minimal Protection**
This provides a level of security designed to control assets with no classification (e.g. C0I0A0). It is generally unsuitable for (non-public) government operations.

**Baseline Protection**
This provides a level of security designed to control assets of moderate value or classified as 'Low'. It is generally used as the baseline for government operations.

**Medium Protection**
This provides a level of security designed to control assets of medium value or classified as 'Medium'.

High Protection This provides a level of security designed to control assets of high value or classified as 'High'.

PH 3. Each zone has the appropriate physical security controls implemented. Appendix A provides details of these minimal and baseline protection controls, together with recommendations for additional controls. Medium protection requires one additional class of control, whereas High protection requires two additional class of control. An Organization MAY incorporate additional controls in addition to those mandated by this standard

PH 4. Implementation of a "clean desk" and "clean screen" policy.

PH 5. Server/Data rooms meet at least the medium protection requirement

PH 6. *Cabling carrying information at levels C-1C3 is physically separate (including for fibre optic cabling) and is in separate ducting to that carrying Nationally Classified information

PH 7. A site security plan and where necessary standard operating procedures (SOPs) for each secure area are developed and implemented. Information to be covered includes, but is not limited to:

a. a summary of the protective security risk assessment
b. roles and responsibilities of facility or ICT security officer and staff members.
c. the administration, operation, and maintenance of the electronic access control system and/or security alarm system
d. key management, the enrolment and removal of system users and issuing of personal identification
e. staff member clearances, security awareness training and regular briefings
f. inspection of the generated audit trails and logs
g. end of day checks and lockup
h. reporting of ICT security incidents and breaches.

## 13. Virtualization [VL]

### 13.1 Objectives

The main purpose of this domain is to specify controls to secure the virialized IT infrastructure at the agency. Organizations need to ensure that such virtualized environments are adequately secured.

For virtual environment hosted outside by 3rd parties, agencies should also refer to Cloud Security Policy.

### 13.2 Control Statements

To meet the requirements of this domain Organizations MUST:

VL 1. *Evaluate the risks associated with the virtual technologies.

a. Evaluate the risks in context of relevant legal, regulatory policies and legislations.

b. Evaluate how the introduction of virtual technology will change your existing IT infrastructure and the related risk posture.

VL 2. *Harden the hypervisor, administrative layer, the virtual machine and related components as per the industry accepted best practices and security guidelines and the vendor recommendations.

VL 3. Enforce least privilege and separation of duties [Refer to section C9- Access Management] for managing the virtual environment.

a. Define specific roles and granular privileges for each administrator in the central virtualization management software.

b. Limit direct administrative access to the hypervisor to the extent possible

c. Depending on the risk and the classification of the information processed, Organizations should consider the use of multi factor authentication or dual or split control of administrative passwords between multiple administrators.

VL 4. *Ensure adequate physical security to prevent unauthorized access to the virtual technology environment.

VL 5. Virtualized technology environment should be augmented by third party security technology to provide layered security controls (defence in depth approach) to complement the controls provided by the vendor and technology itself.

VL 6. Segregate the Virtual Machines based on the classification of data they process and / or store.

VL 7. *A change management [Refer to Section B6- Change Management] process encompasses the virtual technology environment.

a. Ensure that virtual machine profile is updated, and the integrity of the Virtual Machine image is maintained at all times.

b. Care should be taken to maintain and update VM's which are not in active state (dormant or no longer used).

VL 8. *Logs from the virtual technology environment SHALL be logged and monitored along with other IT infrastructure. [Refer to Section B10- Logging and Security Monitoring].

# 6. Compliance and Enforcement

## 6.1. Compliance and Enforcement

The standard provides the security requirements and controls necessary for implementing an Information Security Management System within the organization based on the National Data Classification Policy V3.0.

## 6.2. Transitioning and effective date

### 6.2.1. Effective date

The standard will be effective upon the approval of National Data Classification Policy V3.0 Transition period

Organizations impacted by this standard will be provided a window of six (6) months effective the date of publication.

### 6.3. Exceptions and deviations

The standard mandates that organizations within the scope of the National Data Classification Policy, classify their data and implement the relevant security controls specified within this standard to secure the data

Any deviations to this standard shall be communicated to the National Cyber Security Agency by the organization, through an official correspondence explaining the justifications and rational, along with a risk management plan identifying the risks, assessment of the risk, mitigating controls, and communication and acceptance of the risk by senior management. Based on this, the NCSA will provide an assessment of the exception request in coordination with sector regulator (where applicable).

# 7. Appendices

## APPENDIX A (NORMATIVE) PHYSICAL CONTROLS

| | | Minimal (All Mandatory) | |
|---|---|---|---|
| Control Class | Physical security perimeter | • Fire doors are alarmed. Monitored and tested<br>• Perimeter walls, floors, and ceiling must be permanently constructed and attached to each other.<br>• Number of entrances and exits to the facility should be minimized | |
| | Physical entry controls | • Locks | |
| | Securing offices, rooms and facilities | • Directories and internal telephone books should not be accessible by the public | |
| | Protecting against external and environmental threats | • Firefighting equipment to be provided and suitably placed. | |

## PROTECTION LEVEL

| | Baseline (All Mandatory) | Medium & High Controls |
|---|---|---|
| | • All Minimal Controls<br>• Physically sound walls with no gaps in the perimeter.<br>• Manned reception area or other means to control physical access<br>• Information Processing Facilities are physically separated from those managed by third parties | • All Baseline Controls<br>• Slab-to-slab wall construction to separate zones; Metal or solid wood core, minimum of 44.45 mm thick<br>• Visual evidence of unauthorized penetration<br>• Floor to ceiling wall construction<br>• External protection for Windows<br>• Intruder Detection System installed to cover all external doors and accessible windows |
| | • • All Minimal Controls<br>• Electronic locks on zone entrances (card/token only)<br>• Audit trail (date & time) records for access points only<br>• Perimeter doors resistant to forced entry<br>• All visitors supervised; access for specific purpose<br>• Visible identification for all employees, contractors, and third parties including visitors<br>• Third party/contactors granted restricted access to secure areas or sensitive processing facilities<br>Locks that resist easy picking or prying open | • All Baseline Controls<br>• Electronic locks on zone entrances (token and PIN or biometric)<br>• Audit trail (date & time) records for all access (including access to safes, etc.)<br>• Primary entrance and access controlled interior doors must be equipped with an automatic door closer<br>• Metal detectors<br>• X-ray examination<br>• Additional physically controlled barriers<br>• Barriers to prevent access if opening of ducts, vents, pipes, etc. is > 619 square centimetres<br>• Use of safes/vaults |
| | • All Minimal Controls<br>• Facilities should be sited to avoid public access<br>• Buildings should not give obvious signs of their purpose or identify the presence of information processing facilities<br>Clean desk policy | • All Baseline Controls<br>• Windows that might reasonably afford visual surveillance should be made opaque or equipped with coverings<br>• Facilities should not be accessible by the public |
| | • All Minimal Controls<br>• Fallback equipment and back-up data are outside of zone<br>• Hazardous or combustible materials stored at a safe distance from zone | • All Baseline Controls<br>• Sound Transmission Class (STC) rating of 45 or better between zones |
| | | |

| | | | |
|---|---|---|---|
| | | Minimal (All Mandatory) | |
| Control Class | Working in secure areas | | |
| | Public access, delivery and loading areas | • Access to delivery and loading area from outside of zone restricted to authorised & identified personnel<br>• External doors to delivery/loading area secured when any internal door is open<br>• Incoming material is registered and inspected for potential threats | |
| | Equipment siting and protection | • Guidelines for eating, drinking and smoking in proximity to information processing facilities should be established<br>• Lightening/spike protection should be applied to all buildings to all incoming power and<br>• communications lines | |
| | Supporting utilities | • Firefighting equipment to be provided and suitably placed. | |
| | Cabling security | • Power and telecommunications lines into information processing facilities should be underground or subject to adequate alternative protection<br>• Network cabling should be protected from unauthorised interception or damage | |

## PROTECTION LEVEL

| | Baseline (All Mandatory) | Medium & High Controls |
|---|---|---|
| | • Unsupervised working should be avoided | • All Baseline Controls<br>• Vacant secure areas are physically locked and periodically checked<br>• Photographic, video, audio or other recording equipment not allowed, unless explicitly authorised.<br>• Visual indication when visitors are present in any secure zone. |
| | • All Minimal Controls<br>• Incoming and outgoing shipments are physically segregated. | • All Baseline Controls<br>• Access restricted to people / vehicles whose identification papers have been verified.<br>• Access restricted to personnel / vehicles by prior appointment.<br>• Vehicles are checked for suspect devices. |
| | • All Minimal Controls<br>• Controls to minimise risk of potential physical threats e.g. theft, fire, explosives, smoke, water, dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism<br>• Temperature & humidity should be monitored in all Information Processing facilities (e.g. server rooms, etc.) | • All Baseline Controls<br>• Items requiring special protection should be isolated and appropriately protected<br>• Equipment processing sensitive information should be protected to minimise the risk of information leakage due to emanation. |
| | • All Minimal Controls<br>• An Uninterruptible Power Supply (UPS) for all critical systems should be installed and regularly tested.<br>• Water supply failure should generate an alarm. | • All Baseline Controls<br>• A backup generator for all critical systems should be installed and regularly tested.<br>• Telecoms equipment should be connected by at least two diverse routes to prevent single points of failure. |
| | • All Minimal Controls<br>• Power cables should be segregated from communications cables<br>• Clearly identifiable cable and equipment markings should be used.<br>• A documented patch list should be maintained<br>• Access to patch panels and cable rooms must be restricted to authorised personnel | • All Baseline Controls<br>• Armoured conduit and locked rooms or boxes at inspection/termination points.<br>• Use fibre optic cabling<br>• Use electromagnetic shielding to protect cables<br>• Initiate technical sweeps and physical inspections for detecting unauthorised devices |

| | | | |
|---|---|---|---|
| | | Minimal (All Mandatory) | |
| Control Class | Equipment maintenance | • Only authorised personnel should carry out repairs and service equipment<br>• Records should be kept of all suspected or actual faults, and all preventive/corrective maintenance | |
| | Security of equipment off-Premises | • Equipment/media taken off site should not be left unattended<br>• Portable computers should be carried as hand luggage<br>• Adequate insurance cover should be in place | |
| | Secure disposal or re-use of equipment | | |
| | Removal of property | • Equipment, information or software should not be taken off-site without prior authorization<br>• Equipment should be recorded as being removed off-site and recorded when returned | |
| | Monitoring | • Physical guard at entrance during the business hours. | |

## PROTECTION LEVEL

| | Baseline (All Mandatory) | Medium & High Controls |
|---|---|---|
| | • All Minimal Controls<br>• Only authorised and certified personnel should carry out repairs and service equipment<br>• Information should be cleared from equipment when sent for 3rd party repair/ maintenance | • All Baseline Controls<br>• Maintenance should preferably be carried within the premises of Agency or in a security-controlled environment.<br>• Only authorized and certified personnel, whose identification papers have been verified by the Agency, shall carry out repairs and service equipment |
| | • All Minimal Controls<br>• Home working controls should be determined (e.g. use of lockable cabinets, secure communications etc.)<br>• Portable computers with sensitive data should employ media encryption | • All Baseline Controls<br>• Portable computers with sensitive data should not be taken out of the zone |
| | • Devices containing sensitive information (including media, firmware passwords, etc.) should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable | • All Baseline Controls<br>• Damaged devices containing sensitive information should be physically destroyed<br>• Media containing sensitive information should be physically destroyed. |
| | • All Minimal Controls<br>• Employees, contractors and third party users who have authority to permit off-site removal of assets should be clearly identified; | • All Baseline Controls<br>• Time limits for equipment removal should be set and returns checked for compliance<br>• Removal of "C3" classified information, shall require the authorization of "Information Security Manager" |
| | • 24 x 7 guard at entrance<br>• Perimeter video monitoring<br>• Video monitoring entrance to security zone | • Guard patrolling zone, in addition to guard at entrance<br>• Security control centre<br>• Intrusion detection (ex: motion detection & alarm) within zone |

# APPENDIX B (INFORMATIVE)
## SAMPLE NON-DISCLOSURE AGREEMENT (NDA)

This Agreement dated, <INSERT DATE> between <CLIENT ORGANISATION> (hereinafter called "the Owner") and Agency.

WHEREAS the Owner is in ownership and possession of certain Confidential Information (hereinafter called "the Confidential Information").

AND WHEREAS Agency has requested the Owner to provide the said Confidential Information in order to provide services or undertake certain projects which may include legal obligations.

NOW THEREFORE THIS AGREEMENT WITNESSETH that in consideration of the Owner disclosing the Confidential Information to Agency and the mutual agreements and other good, valuable or nominal consideration, the receipt and sufficiency of which is hereby acknowledged, Agency hereto undertakes and agrees with the Owner as follows:

### 1. Definition

#### a. Agreement

Any reference herein to an Agreement, means this Agreement which represents the entire understanding between the parties and supersedes all other agreements express or implied between the parties regarding disclosure of the confidential information.

#### b. The Confidential Information

In this Agreement, "the Confidential Information" means information relating to the products, services, ideas, business, personnel, trademarks, copyrights, intellectual property or commercial activities of the Owner, including but not limited to formulae, systems, presentations, compilations, devices, concepts, techniques, marketing and commercial strategies, processes, data which individually may, or may not be confidential, which information is generally not known to the public and either derives economic value, actual or potential, from not being generally known, or has character such that the Owner has legitimate interest in maintaining its secrecy. In addition, all documents given by the Owner to Agency will be considered the Confidential Information, whether or not marked with any proprietary notice or legend when the disclosure takes place. Confidential Information does not include any pre-existing intellectual property owned by Agency and any knowledge and expertise gained by Agency in the process of providing services or undertaking activities for the Owner.

### 2. Third parties

#### a. Agreement

Agency shall not disclose the Confidential Information to third parties. If such third party disclosure is necessary, or about to be made for whatever reason, Agency shall seek prior written permission of the Owner, and allow the Owner the opportunity to enter into a non-disclosure agreement, substantially identical to this Agreement with the third party.

Agency shall not disclose the confidential information, except in the following:

a. The owner has authorized disclosure in writing
b. Disclosure is required by a legal or judicial process,
c. Disclosure is required by law, or
d. The information is in the public domain.

## 3. Acknowledgement of Ownership and Confidentiality

Agency acknowledges and agrees that the Confidential Information disclosed to it by the Owner, or that it requires, sees, or learns of as a direct or indirect consequence of the discussions contemplated herein, and all dealings and transactions that follow or result from such discussion/s, are the exclusive property of the Owner, and Agency will keep that information strictly confidential.

## 4. No Transfer of Rights

Agency acknowledges and agrees that it shall not acquire any right or interest in the Confidential Information and that the Owner shall remain the sole owner of the Confidential Information, including but not limited to all patent, copyright, trademark, trade secret, trade name and other property rights pertaining thereto, anywhere in the world.

Receiver shall not manufacture, use, sell, or distribute the Confidential Information without the written permission of the Owner.

## 5. No Offer for Sale

The parties acknowledge and agree that the disclosure of the Confidential Information by the Owner to Agency does not constitute an offer by the Owner for the sale, license, or other transfer of the Confidential Information. Except as may be expressly set forth herein, neither party shall have any financial or other obligation to each other respecting the Confidential Information. Any offer for sale, license, or other transfer of the Confidential Information shall be made pursuant to a separate agreement.

## 6. Remedies

Each party agrees that in the event of any such breach of this Agreement by it, that, in addition to all other remedies available to the other party by law, the other party shall be entitled as a matter of right to apply to a court of competent jurisdiction for such relief by way of restraining order compliant with the provisions of this Agreement.

## 7. Modification

The parties can modify any term or condition of this Agreement only by mutual consent and by reducing such modifications to writing, signed by both parties.

## 8. Successors

This Agreement shall be binding upon and inure to the benefit of both parties and their respective heirs, successors, assigns and representatives.

## 9. Waiver

No waiver, delay, indulgence or failure to act by either party regarding any particular default or omission by the other party shall affect or impair any rights or remedies regarding that or any subsequent default or omission that are expressly waived in writing.

## 10. Governing Law

This Agreement shall be construed and interpreted in accordance with the laws of the State of Qatar. Disputes arising out of non-compliance with any of the terms in this Agreement shall be subject to the jurisdiction of the Courts of the State of Qatar.

## 11. Commencing Proceedings

The parties to this Agreement agree that the process of any suit, action, or proceeding before any court sitting in the State of Qatar, may be commenced by service delivered personally to the opposing party to this Agreement or to an appropriate agent for service.

## 12. Continuing Obligation

Any rights and obligations under this Agreement that by their nature extend beyond the terms of this Agreement shall survive any expiration or termination of this Agreement and shall remain in effect for a period of two (2) years following such expiration or termination. However, either party may require a longer confidentiality term for specific information that should be marked and identified to the other party.

## 13. Attorney Fees

If any litigation arises out of this Agreement, the prevailing party shall be entitled to reasonable attorney's fees, costs and expenses in addition to any other relief to which that party may be entitled

## 14. Captions

All indexes, titles, subject headings, section titles, and similar terms are provided for the purpose of reference and convenience and are not intended to be inclusive, definitive or to affect the meaning or scope of this agreement.

## 15. Execution Authority

The persons whose signatures appear below certify that they are authorized to enter into this agreement on behalf of the party for whom they sign.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement.

## OWNER ►

- Signed:
- Name:
- Title:
- Date:

## AGENCY ►

- Signed:
- Name:
- Title:
- Date:

# APPENDIX B (INFORMATIVE)
## SAMPLE NON-DISCLOSURE AGREEMENT (NDA)

| Service | Competent Authority | Competent Department | Contact Details |
|---|---|---|---|
| Administration of Personal Data Privacy Protection Law | National Cyber Security Agency (NCSA) | Office of Data Privacy | privacy@ncsa.gov.qa |
| Personal Data Breach Notification | National Cyber Security Agency (NCSA) | Office of Data Privacy | privacy@ncsa.gov.qa |
| Reporting Cyber Incidents | National Cyber Security Agency (NCSA) | Cyber Fusion Affairs | ncsoc@ncsa.gov.qa |
| Administration of Cyber Crime Law and Reporting Cyber Incidents to Law Enforcement Agency | Ministry of Interior (MoI) | ECCC Department | |
| Queries about this Standard | National Cyber Security Agency (NCSA) | National Cyber Governance & Assurance Affairs | csps@ncsa.gov.qa |
| Accreditation and Certification against National Standards | National Cyber Security Agency (NCSA) | National Cyber Governance & Assurance Affairs | assurance@ncsa.gov.qa |
| Administration of E-Signature and E-Commerce Law | Ministry of Communication and Information Technology (MCIT) | | cspma@mcit.gov.qa |

## 8. Annexes

### a. Agreement

### 8.1. Acronyms

| | |
|---|---|
| **BCP** | Business Continuity Plan |
| **DNS** | Domain Name Server |
| **ICT** | Information Communication Technology |
| **NCSA** | National Cyber Security Agency |
| **NDA** | Non-Disclosure Agreement |
| **VLAN** | Virtual Local Area Network |

### 8.2. References


- Emiri Decree No 1 of year 2021
- President of National Cyber Security Organization (NCSA) Decision No 3 of year 2022
- [IAP-NAT-DCLS] National Information Classification Policy, 2014

- [IAP-NAT-IAFW] Information Assurance Framework, 2008
- [AES] NIST FIPS PUB 197 "Advanced Encryption Standard (AES)," November 2001.
- [CC3.1] Common Criteria for Information Technology Security Evaluation (CC), Version 2006) 2.0)
- [CWA1-14167] Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements, CEN Workshop Agreement, CWA 1-14167, June 2003
- [FIP2-186] NIST FIPS PUB 2-186 "Digital Signature Standard (DSS)," with Change Notice 1, October 2001.
- [FIPS2-140-] National Institute of Standards and Technology, FIPS 2-140, Security Requirements for Cryptographic Modules, January 2007 ,24
- [Mitre] Mitre, 2009 CWE/SANS Top 25 Most Dangerous Programming Errors, http://cwe.mitre.org/top25/ , January 2009.
- [RFC 4301] Kent & Seo, Security Architecture for IP, RFC 4301, December 2005
- [RFC3851] Ramsdell, S/MIME 3.1 Message Specification, RFC 3851, July 2004
- [RFC4346] Dierks & Rescorla, The TLS Protocol, RFC4301, April 2006
- [RSA] RSA Laboratories, "PKCS1# v2.1: RSA Cryptography Standard," June 2002.
- [SFTP] Galbraith & Saarenmaa, SSH File Transfer Protocol, draft-ietf-secsh-filexfer, June 2005
- [SHA] NIST FIPS PUB 2-180, "Secure Hash Standard," National Institute of Standards and Technology, U.S. Department of Commerce., August 2001.
- [SP67-800] NIST SP 67-800 "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher," May 2004.
- [ISO1-11770] Information technology – Security Techniques, Key Management, ISO/IEC -11770 1:2006(E) Part 1: Key Management-Framework, International Organization for Standardization & International
- Electrotechnical Commission, 2006
- [RFC4408] M. Wong, W. Schlitt, on Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, Internet Engineering Task Force (IETF), RFC 4408, April 2006


## 8.3. Major Change Tracker

- **Section 4:** Information Security Governance: Control on reporting of Security Manager is updated
- **Section 4:** Data Classification Label: Classification Labels have been changed
- **Section 4:** Incident Management: Controls updated in the domain and the associated Appendix related to "Incident Management Criticality Classification" has been removed.
- **Section 4:** Logging and Security Monitoring: Control related to Log retention udated.
- **Section 4:** Audit & Certification: Controls have been updated to align with the Certification scheme.
- **Section 5:** Cryptography: Controls have been updated and the associated Appendix related to "Approved Cryptographic Algorithms and Protocols" has been removed
- **Section 6:** Compliance & Enforcement: New section to clarify enforcement of this document

Appendix C: List of Competent Departments

www.ncsa.gov.qa

Tel: 16555 | Fax: 2362080

Email: info@ncsa.gov.qa | P.O. Box: 24100 Doha - Qatar

Follow us: