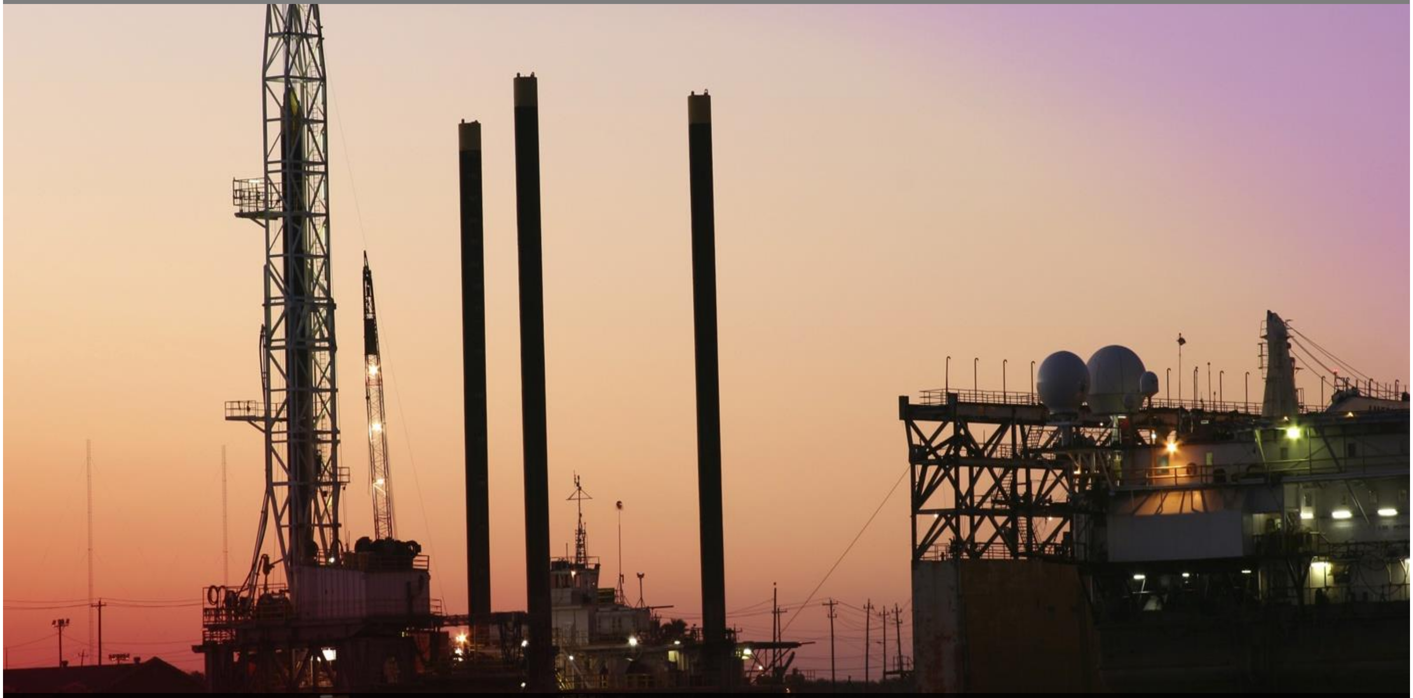
National Information Assurance Policy



Guidance For Assurance Manual [IAG-NAT-GFAM]

Author:	**MOTC**
Version:	2.0
Classification:	PUBLIC
Date of Issue:	**2018-04-29**

Table of Contents

Section A

1. Overview

This document forms a set of the NIA Policy and has been written with the sole objective of providing guidance to the readers in being able to understand and implement the NIA Manual.

The document is focussed on providing an objective assessment and the expectations from the various controls specified in the NIA Manual.

The document shall be read along with the NIA manual as a reference and not independently.

2. Ownership & Maintenance

The manual is owned by Ministry of Transport and Communications, MOTC, and shall update the document as when deemed necessary.

3. References

[IAP-NAT-INFA]	National Information Assurance Policy, 2014
[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 2.0 (2006)
[CWA14167-1]	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements, CEN Workshop Agreement, CWA 14167-1, June 2003
[FIP186-2]	NIST FIPS PUB 186-2 “Digital Signature Standard (DSS),” with Change Notice 1, October 2001.
[FIPS-140-2]	National Institute of Standards and Technology, FIPS 140-2, Security Requirements for Cryptographic Modules, January 24, 2007
[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, “PKCS#1 v2.1: RSA Cryptography Standard,” June 2002.
[SFTP]	Galbraith & Saarenmaa, SSH File Transfer Protocol, draft-ietf-secsh-filexfer, June 2005

[SHA] NIST FIPS PUB 180-2, "Secure Hash Standard," National Institute of Standards and Technology, U.S. Department of Commerce., August 2001.

[SP800-67] NIST SP 800-67 “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher,” May 2004.

[ISO11770-1] Information technology – Security Techniques, Key Management, ISO/IEC 11770-1:2006(E) Part 1: Key Management-Framework, International Organisation for Standardisation & 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

Defined terms are specified in the Information Assurance Framework, [IAP-NAT-IAFW]. The following defined terms are used in this document: **Agency**, **Personal Information**, **Hot/Warm/Cold Sites**, **Q-CERT, MOTC, and National Classification Markings.**

Section B

1. Guidance on Governance Structure [IG]

1.1. Guidance on Policy and Baseline Controls

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

The NIA Manual mandates that the Agency appoint an Information Security Manager who will be the Business owner for all Information Security related programmes.

The Information Security Manager will be responsible for drawing up the budgets (Financial and Manpower) for the Agency's Information Security Program. The ISM would also be responsible for planning and executing the objectives for the IS department.

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

The NIA Manual mandates that Agencies demonstrates their commitment to Information Security by ensuring that adequate resources including budget and staff are allocated to operate the Information Security Programme.

A poorly funded program is worse than having no program, as it elicits a feeling of false satisfaction amongst its stake holders.

Paucity of funds may hamper implementation of proper security controls or execution of security programs. Ditto for resources, the best in class system will fail to deliver if enough resources are not available for manning its operations.

IG 3. *Ensure the Security Manager has a reporting line to the Agency's risk or internal audit function.

In order to ensure fair independence in the work of ISM, it is prudent that he has a direct reporting either to the Agency's Risk / Internal Audit department head or the Head of the Agency himself.
An ISM reporting to the Head of IT will introduce conflict of responsibilities and accountability.

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

The key to any successful Information security program is an unflinching support from the management/ Agency head in driving the information security program within the organization. The Agency head must ensure that the ISMS becomes an intrinsic part of all business processes and decisions.

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

Any variations or non-conformance to this manual should be approved by the Head of the Agency. In cases, where this may not be possible the Head of the Agency may delegate this responsibility to a person / official who has a higher authority than the Security Manager. This is to prevent misuse of power.

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

For an effective Information Security Management culture in the organization, it is imperative to ingrain Information Security responsibilities and awareness into each employee, contractors etc.
HR should ensure that Information Security responsibilities are defined in each and every Job description. The level of the responsibility may vary in accordance with the specific role and business process. Further the procurement process should involve sensitizing the vendors, supplier contractor to the information security policies, procedures within 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 Agency, especially operating systems, access & authorisation control systems/facilities and auditing facilities

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

The NIA Manual prescribes a list of requirements required of potential candidates and the obligations on management to ensure that the Information Security Manager is able to effectively perform his duties and responsibilities.

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 Q-CERT

Further to control IG7, the manual extends the list of responsibilities for an information security manager.

IG 9. Ensure the Security Manager is accountable 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 within IT Projects, system development, acquisition, procurement, implementation, change management, operation, support, and architecture

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

d. the certification of systems, when applicable

e. **ensuring the agency has an appropriate ICT security awareness and training program.**

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

Clause IG 8 and IG 9 in the NIA Manual mandate the minimum responsibilities for which the Information Security Manager should be accountable. Specific activities may be added as per the business requirements of the Agency.

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.

The NIA Manual lays specific emphasis on the requirement of ISM to have operational knowledge of the security procedures defined for systems and business processes. The insight will provide the ISM with a better understanding of the system and the impact of the same on the processes and activities. The information would further assist in identifying security responsibilities for various roles in relation to the usage of systems. Regular reviews of security operating procedures shall be part of the ISMS.

2. Guidance on Risk Management [RM]

2.1. Guidance on Policy and Baseline Controls

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)

The NIA Manual does not recommend a particular Threat Vulnerability assessment methodology, to be adopted to manage risks by the **Agency**.

There are a number of threat & vulnerability assessment frameworks and standards available notably from ISO (ISO 27005), Cobit, and various government standards like *AS/NZS 4360:1999*.

The procedure should define the "Risk Appetite" of the Agency. Risk Appetite in essence is defining the Minimum Risk that may be accepted by the **Agency**.

For example, an **Agency** may define risk levels as Low, Medium, High and Very High. They may further define that Risks at level 'Low' are acceptable and there is no requirement for action in terms of its mitigation.

It is expected that the exercise provides the **Agency** with sufficient insights to:

Ascertain the real threats and vulnerabilities in the system
Prioritize its available resources to implement a secure infrastructure.

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

The NIA Manual does not recommend any specific strategy or security controls for mitigating identified threats, other than specifying baseline controls. The controls chosen by the Agency may be either technical or administrative and may confirm to one of the following strategies:

Avoid Risk: Due to the inherent nature of risk it might be prudent to avoid the 'Risk' all together. For example, modify or terminate the process that induces the risk.

Transfer Risk: In some cases it may be advisable to transfer the risk to another entity. For example, some operational risks may be taken care of by outsourcing. Another example might be providing an insurance cover to mitigate the financial losses. However, the areas or services being outsourced remain the governance, compliance and risk management responsibility of the Agency. Please see TM1 in Third Part Security Management for more information on controls related to outsourcing.

Mitigate Risk: Most of the time it may not be possible to either avoid or transfer risk, also there may be scenario's where critical processes need to be run in spite of the risks associated. In such scenarios it is necessary to reduce the risk to an acceptable level. This includes applying specific controls to reduce the consequences (impact) or the likelihood of the risk occurring. For example, installation of effective fire detection alarm system, along with a fire suppression system can effectively reduce the consequence and likelihood of fire.

Accept Risk: A thumb of rule in designing and implementing controls to mitigate risk is to ensure that the cost of risk mitigation is not more than the cost of the information asset and / or the service it provides (considering the legal and contractual obligations). Even after applying controls, the risk may still not reduce to acceptable levels (Risk Appetite), in such cases the relevant authorities in the Agency need to decide if they are prepared to accept the risk.

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 Agency.

The NIA Manual ensures that effective controls are chosen while addressing critical assets. The policy will ensure that Senior Management of the Agency are effectively involved in the decision making process related to security of critical infrastructure.

Senior Management shall include Head of Agency, Head of Internal Audit.

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

The NIA Manual mandates an effective procedure is in place to ensure effectiveness of the implemented controls. The implemented controls shall be monitored to ensure that the desired level of risk mitigation is achieved.

Threat scenario changes and so do associate vulnerabilities, the process should ensure that a closed cycle is maintained and any changes and its impact on the infrastructure are assessed and effectively addressed. The process shall ensure that the implemented controls remain effective in the changed scenarios and are able to meet the new challenges.

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

Risk management must be incorporated into all business processes. The business environment may also change the risk to the organization and these must also be noted in the risk assessment process. Whenever, the process is changed, a risk assessment should be done to ensure that the changes are aligned to the risk appetite of the organization or corrective actions are taken to do the needful. The same is true for any changes in the business environment eg legal/regulatory changes, opening up of new channels of delivery (online business).

3. Guidance on Third Party Security Management [TM]

3.1. Guidance on Policy and Baseline Controls

TM1. *The areas or services being outsourced remain the governance, compliance and risk management accountability of the Agency.

The NIA Manual mandates that in case when the Agencies outsource some of the processes; it does not transfer the liabilities for the process to the external parties. The Agencies shall be responsible for the governance, compliance and risk management of the outsourced processes. Agencies shall ensure that all outsourced processes are backed up by proper Service Level Agreements (SLA's).

All such SLA's shall have identified Key Performance Indicators (KPI's) which include among other things Confidentiality, Integrity and Availability of the process. Security Management shall be inherent in the outsourced contract.

Agencies should setup some specific agreements as, for example, dedicated to access to internal resources from 3rd parties, as a 3rd party connection agreement, that will include references to internal policies on system and network resources usage, liabilities and description of parties involved.

TM2. *They understand and acknowledge the risks associated with the outsourcing of their services.

The NIA Manual mandates that a proper Risk Assessment has been carried out and all pros and cons have been weighted prior to outsourcing the services. This includes assessing the information security risk assessment. All risks identified out of this exercise shall be mitigated and residual risks shall be acknowledged by senior management.

The Agency and third parties should develop RACI charts (responsible, accountable, consulted and informed) to define roles and responsibilities for effective risk management

TM3. That the security controls and baseline policy specified in this NIA Manual is included in the third party service delivery agreement or contract. This SHALL also apply to sub-contractors used by the third party.

The NIA Manual mandates that the third party contractor or service provider has access to the National Information Classification Policy and the National Information Assurance Manual. This will ensure that they are well versed with the policy and it requirements and further ensure compliance with the policies.

TM4. The third party SHALL be contractually required to regularly report on the outsourced service'(s) security posture, including any incidents.

The NIA Manual mandates that a mechanism is in place to ensure flow of communication between the Agency and the Third party service provider. The reporting provided by the Third party service provider shall include updates security incidents and posture of the security infrastructure. The third party service provider shall imbibe the processes dictated by the NIA manual which includes amongst others Change Management. All Changes relevant to the outsourced process shall be communicated and approved by the Agency.

TM5. 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.

The NIA Manual mandates that due diligence is carried out in monitoring the services outsourced to the Third party service provider. Regular audits should be carried out to ensure adherence to SLA's and the contract. The agreement between the Agency and third party service provider must include provisions for facilitating such audits. Depending on the criticality and nature of the outsourced service to the Agency, the Agency may include provisions to audit third party security, business continuity, risk management, compliance programs, etc.

4. Guidance on Data Labelling [DL]

4.1. Guidance on Policy and Baseline Controls

DL1. *Serve as a labelling authority for the data and information that it collects or maintains.

The NIA Manual mandates that the Agency shall be the Labelling authority for the data and information that it collects and maintains. This means that designated nominees or the business process owners within the Agency shall have the responsibility to identify and classify the information that it collects or maintains.

DL2. *Rate all information assets in accordance with [IAP-NAT-DCLS]. All assets rated with a Confidentiality rating of C1, C2 or C3 SHALL be suitably marked the data label of Internal, Limited Access or Restricted respectively.

The NIA Manual mandates that the Agencies shall ensure that all information is classified. This includes information in all forms i.e. digital, paper, audio / video format etc.

The classification shall be based on the National Information Classification policy. All classified information shall be suitably marked for identification. Digital data shall also be suitably marked and Agencies shall ensure that suitable controls exist in the system to ensure that dissemination of the information is in line with the C-I-A ratings of the information

DL3. *By default, classify information assets as 'Internal' unless they are specifically for public release or consumption.

The NIA Manual mandates that a base minimum protection is offered to all information assets to mitigate the risks associated with oversight in classifying the document. There may be cases that a document has not been labelled since it is still in draft stage or has not been complete, further the label may have been damaged or tampered, in all such cases the above control will ensure that all information assets that are not labelled or classified have a default classification of C1 i.e. Internal.

DL4. Establish the data labelling system to support the "Need-To-Know" requirement, so that information will be protected from unauthorized disclosure and use.

The NIA Manual intends to assure that the Data labelling system complements the "Need-To-Know" requirement. Classification and labelling of the information will ensure simplification of the process to allocate rights to information. Until access to information is made based on an authorized need, the information should be made available on a specific authorized requirement.

DL5. Establish data labelling awareness and training for its staff, employees and contractors.

The NIA Manual mandates that the staff and the target audience are aware and understand the concept of data labelling and its implications on the information security. Appropriate training should be allocated to employees on how to label and interpret these labels

5. Guidance on Change Management [CM]

5.1. Guidance on Policy and Baseline Controls

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:

- **Change that results in business interruption during regular business hours**
- **Change that results 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**
- **Security breach or threat**
- **A response to a natural disaster**
- **A response to an emergency business need**
- **A change requested by emergency responder personnel**

The NIA Manual mandates that a defined change management procedure exists within the Agency. This is to ensure that all changes are documented and deliberated on the scope, effects and pros and cons in context of the Agency's business. The CM process further ensures that the management and the audience are aware of the impending changes and its effects on the business process. Change Management records should be kept in a dedicated Change Management Database (CMDB) and reviewed regularly.

The NIA Manual further mandates that all changes are categorized in categories such as the one defined above. Agencies may have their own categorization which may be an improvisation of the above.

A proper categorization of the Change puts in to focus the right resources that may be required to execute such a Change.

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

The NIA Manual mandates that Agencies form a Change Management Committee (CMC), which comprises of representations from various business / functional units, process owners and must include representatives from information security and risk management divisions as a minimum.

The CMC shall be responsible to evaluate each Change Requests submitted to them, and assess the impact of the change on the business process, its technical and financial viability and impact on the security posture of the Agency.

Ensure that the plan conforms to Agencies SOP. Care must also be exercised in keeping with the Segregation of duties principle. The Segregation of duties principle suggests that the maker of a request must not be the one who is making the change or checking it.

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

The NIA Manual mandates that ad-hoc changes are not introduced in the system / business. All proposed changes should be deliberated, documented and approved by the CMC. The CMC is responsible to ensure that all changes are introduced in a systematic manner and follow SOP's and are backed by fallback mechanisms.

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 NIA Manual mandates that if an introduced change (be it major or minor) has a major impact on the security posture of the Agency, then the CMC should assess if the system would require a re-certification and if yes to initiate and execute a plan to achieve the same. CMC should also ensure the changes will satisfy, at a minimum, the baseline controls. Risk analysis should also be conducted as part of change process to keep the residual risk at an acceptable level.

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

The CMC should ensure that post implementation of a change, all related processes and system related information is updated. Change Management records shall be kept in a dedicated Change Management Database.

CM 6. Emergency changes may be carried out on the basis of 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.

It is possible that there may be time or situations where an urgent change may be required to be implemented without prescribing to the due diligent CM procedure. The CMC should lay down criterion that defines under what conditions and how such Changes may be carried out.

CMC should also ensure that post emergency and completion of the Change Management, the Change implementers should follow due diligence and re-run the proposed change through standard procedures and processes.

All related documentation and risk analysis should be completed.

6. Guidance on Personnel Security [PS]

6.1. Guidance on Policy and Baseline Controls

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

Humans are the weakest link in the Security Chain. In order to build an effective security posture it is imperative to ensure that proper controls are in place to mitigate the human risk. The NIA Manual lays the foundation for such controls by ensuring that security best practices are integrated in all HR processes. It is necessary that HR process is integrated with information security procedures as they deal with a lot of corporate and personal information.

PS 2. *Ensure the HR department documents security requirements and obligations and ways of working in HR manual, which is read, understood and available to all staff to ensure they are aware and comply with their obligations to information security.

The NIA Manual mandates that information security responsibilities for employees are documented and are made available to the employees at all time. Integrating information security responsibilities within the HR manual ensures all employee needed information (Rules, code of conduct, disciplinary actions, responsibilities etc) are available from a single point of information. This ensures that the information is easy to update, maintain and distribute (no multiple sources to edit, update and distribute). HR should take efforts to assume that employees read and understand these policies and procedures. It might be a good idea to have a manager write the function, who can interface with the employee and provide the guidance and answer queries.

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 Proposed Information Privacy & Protection Law.

The NIA Manual mandates that Agencies devise internal procedures to handle personal information it collects by way of employee information, and or as part of its business processes to prevent misuse by its constituents. These constituents can be internal or external to the Agency. Furthermore the Agencies should ensure that the procedures comply with the relevant regulations while processing personal information. MOTC has Proposed Information Privacy & Protection Law to mandate how such personal information should be collected, processed and secured to prevent mi-use of such information.

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.

Furthermore, the NIA Manual mandates that information security responsibilities are defined as part of employee's responsibilities and is part of standard job descriptions. This is to ensure that employees understand their information security responsibilities right from the day they apply for a job. This ensures that due focus is imparted on Information Security.

The NIA Manual further mandates that these responsibilities are adhered and monitored throughout the employees stay with the Agency.

A simple example of implementing this would be by ensuring that this is part of the employee's performance appraisal methodology. Information Security linked Performance metrics should be identified and linked to SMART performance appraisal if possible.

PS 5. *Conduct adequate screening to ascertain the integrity of prospective candidates for employment and contractors (including sub contracted workers). The Agency 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".

The NIA Manual mandates that **Agency's shall** perform suitable background checks to establish and confirm the integrity and information provided by the prospective employee. Background checks confirm the appropriateness of the employee for the job. The level of background check may vary based on the nature and the sensitivity of work. Background checks may include some or all of the following:

<u>Credential Checks:</u> This includes investigation of records submitted by the prospective employee for e.g. Educational qualifications, Past Employment History, Membership of Organizations, Reference checks etc. Internet can be a very effective tool in this regards. Checks on social networking sites (examples include Facebook, LinkedIN), blogs, forums could provide some insight on the candidate. However all such information should be used with due caution as there has been cases where the virtual identity of people has been compromised or sabotaged by vested people for vested reasons.

<u>Criminal Check:</u> This includes investigation to ensure that the employee does not have criminal history or background. The **Agency** SHALL however have the right to decide on candidates who have minor history like offences related to driving.

Such checks shall be extended to contractors and sub contracted workers depending on the nature and sensitivity of the work they will be involved in.

The Agency will have the discretion to extend this check to existing if employees in case of situations such as Change of Responsibilities or Suspicions raised on the conduct of an employee. However, Agencies shall employ due diligence to ensure that such suspicions are not part or result of witch hunting.

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

a. Confidentiality and non-disclosure obligations

Agency's must inform the prospective candidates regarding their compliance to the established Security framework of the **Agency.** This includes amongst other things

1. Confidentiality and Non Disclosure Agreement.

2. Understanding and acceptance of the Corporate information security policy, Acceptable usage policy and other related policies and procedures.

A signed document is legal evidence that ensures employee's conformance to compliance with the Agency's regulations.

Agencies should look in to options on reviewing the security obligations and regulations at regular intervals. Such review could happen annually, or during contract renewal or during change of responsibility when an employee is promoted/demoted/moved in a different role within the organization.

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 Agency security policies.**

Agencies should understand that providing awareness on information security responsibilities, signing of NDA etc are administrative controls which may deter an employee to breach the security. However needless to say there is always a possibility where such controls may not be effective and as such it is necessary that the Agencies employ other kinds of technical control to deal with the risks of information security breach.

Controls on a technical front could include content management techniques, on an administrative level it could be forbidding any personnel other than then "designate spokesperson" from making public statements etc.

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.

A potential cause for breach of information (knowingly or unknowingly) arises in scenarios where the employee / contractor have access to information beyond their rights or requirements. A common myth exists that “If I have Access, I can use it”.

NIA Manual mandates that information provided to Agency’s employees / contractors is limited to effective delegation of their responsibilities and is strictly based on a “Need to Know” rule.

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.

Agencies shall implement controls to ensure that NO single individual has complete control over the process. Process Owners should ensure that processing and authorizing or processing and auditing works are not handled by the same individual. This will ensure that a collusion of more than one person is required to pull a breach.

Furthermore for highly critical and confidential systems and applications, the passwords or access should be split to a minimum of two entities. For e.g. the access to the system may require dual level of access control and these shall be distributed between two persons, in case if this is not entirely possible, the password for the system shall be split in to two, with no single person having access to both the parts.

However due caution should be exercised by the Agencies to ensure that such controls are implemented on the most sensitive processes, as the approach may itself be a cause for Denial of Service at critical times.

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 manual.

Agencies shall define a disciplinary process and ensure that the STAFF is made aware of the same through suitable Security Awareness sessions. Such Disciplinary process may be documented in the Employee or HR Manual and be made available to the concerned staff through means like intranet, printed copies in section / library etc.

PS 11. *Ensure that vendors, contractors, delegates or guests visiting Agency 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 Agency**

e. **escorted by Agency employees while accessing secure areas**

The nature of business carried out by **Agencies** or the requirements of business may mandate that visitors in the form of vendors, contractors, delegates or guests may visit the premises of **Agency**. While it may be difficult to dwell into the motives of each **a**nd every person, it is prudent on the part of **Agency** to exercise caution and implement controls to regulate such visitors.

NIA Manual mandates that all such guests, vendors, contractors, delegates etc are escorted in office areas. The guests should be briefed about the security and controls in place. This may usually be done by ensuring that the visitor badge is accompanied by a folder or small pamphlet which provides basic information to the guests and warns them that they are monitored and educates them about their responsibilities.

Staff should be educated and encouraged to challenge and report strangers moving in and around the Agency premises without proper identification i.e. Employee ID or Visitor Badge.

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 Agency assets and physical & logical access are amended/removed as appropriate.

NIA Manual mandates that HR and Facilities Administration and IT are tightly integrated in processes related to manpower. Any new staff or terminations or change of responsibilities shall be tracked using an appropriate Change Management process.

This is to ensure that all concerned stakeholders i.e. HR, Facilities and Administration and IT are updated whenever a new person requires access to Agency's facilities (physical or logical) and whenever such person leaves the organization by way of retirement, termination or resignation or end of duty.

This will ensure that all access control rules (physical and logical) are suitably amended to ensure that there are no residual accesses in the system. A similar process should also follow when there is a change of responsibilities by way of transfers, promotions or demotions.

7. Guidance on Security Awareness [SA]

7.1. Guidance on Policy and Baseline Controls

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

Security Awareness is crucial to ensuring that all related parties understand the risks, and accept and adopt good security practices. Training and education can provide users, developers, system administrators, security administrators and any related parties with the necessary skills and knowledge in implementing the security measures.

The NIA Manual mandates that the Agencies allocate adequate budgets to initiate, execute and maintain a Security Awareness programme within the Agency.

SA 2. *As a minimum, such training includes

- **a. Baseline requirements specified in this NIA Manual**
- **b. Agency'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**

The NIA Manual mandates that the Security Awareness is designed to adequately cover topics relevant to the Agency's business.

1. Training material shall include, at a minimum, content that:
   - a. Enables the individual to understand the meaning of IT security, why it is needed, and his/her personal responsibility for security along with the importance of complying with **Agency's** specific security policies and standards. Where **Agency's** IT security requirements are more stringent than National IT security policies and standards, those elements should be clearly explained.
   - b. Includes or references Government Laws and regulations. Create awareness within employees about obligations arising out of these laws.
   - c. Enables the individual to better understand social engineering persuasion techniques that may be used to deceive an individual into revealing confidential, private, or privileged information in order to compromise the confidentiality, integrity, and availability of **Agency's** data/information and IT resources.
   - d. Covers, but is not limited to
     - i. The responsibility of individuals to report IT-security-related issues; and the mechanism for doing so
     - ii. The fact that an individual's activities can be audited;
     - iii. The legal requirements for data privacy and protection(*Proposed Data Privacy and Protection Law);
     - iv. The ownership of data and data marking
     - v. Non-business use issues;
     - vi. The budget unit's password requirements for usage and management;

vii. Virus and malicious code protection;
viii. Acceptable use policy for Information assets, email and Internet Use;
ix. Software licensing
x. The sensitivity of **Agency** systems to threats, risks, and vulnerabilities;
xi. Social engineering techniques commonly used to deceive users into giving away access or revealing confidential or privileged information;
xii. Physical security; and
xiii. Applicability of security requirements to all IT resources, including portable IT devices, such as laptops, etc.

2. Security awareness training materials (manuals, documents, etc.) as well as IT security policies, standards, and procedures should be made readily available, either electronically or via hard copy, to all **Agency** employees, and to contractors, temporary workers as applicable.

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

The level of security awareness and training SHOULD be commensurate with the level of access and expertise required in relation to the system components and information resources for which the **Agency** employee / contractor / third party user is responsible.

1. All **Agency** employee / contractor / third party user should receive security training prior to being provided any access to IT systems and resources. Prior to accessing **Agency** specific software applications, employees should receive any specialized security training as appropriate focused for their role and responsibility relative to the software application system.
2. Security awareness shall be promoted on an on-going basis. **Agency** employees SHOULD have their security awareness training updated annually or upon occurrence of a specific event, such as a change in job responsibilities, employment status, etc.

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

The NIA Manual intends to emphasize on the risk of social engineering that may lead to disclosure of information. More often than less, it is human behavior to discuss based on personal experiences. It is possible that while on trainings the government personnel may discuss and deliberate using Agency's internal information (business or technical). This may lead to un-intended disclosure of sensitive information.

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

The NIA Manual mandates that the Security awareness training content be created and regularly reviewed, and updated, to ensure that it addresses and stay relevant to the **Agency's** objectives, culture, business, technology, legal /regulatory, systems and data/information requirements.

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.

The NIA Manual mandates that Information security is integrated into the different business processes of the Agency. Integration of Security Awareness training and Induction training program helps create synergies between the HR and Information Security department.

Moreover the integration emphasizes upon the new employee the importance of Information security. The awareness trainings should be organized at regular intervals to ensure that employees remember and are updated with the relevant changes that may happen from time to time.

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.

Agency should incorporate formal evaluation and feedback mechanisms to gauge the appropriateness and effectiveness of its security awareness and training programs, techniques, and materials.

Agency should maintain records of information technology security education efforts. Attendance of security awareness training should be documented in the employee's personnel file with the employee's acknowledgement of having received and understood the training.

Agencies should define and maintain key performance metrics which help to illustrate the effectiveness of security awareness education efforts.

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

Agencies shall determine the appropriate methods used for awareness and education, which may include but are not limited to:

- Posters
- Computer-based training
- ***Intranet*** materials and resources
- Videos
- Newsletters
- Memoranda
- Briefings
- Formal classroom instruction
- On-the-job training
- Conferences

8. Guidance on Incident Management [IM]

8.1. Guidance on Policy and Baseline Controls

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

The NIA Manual mandates that the Agency defines a process owner for Incident Management. The person should be completely responsible for the functioning of the Incident Management programme, which includes managing budgets, defining the programme, executing the programme etc.

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

The Incident Management process owner (IM Manager) shall assess the requirements for the Incident response capability in context of the Agency's business requirements. The IM Manager shall review this requirements on a periodic basis based on a Threat & Vulnerability analysis.

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

The Agency shall define procedures to detect, evaluate and respond to incidents. As a minimum, the procedures should include:

1) Detection of incident.
   a) Procedures for detecting shall include monitoring and reporting of incidents.
   b) All users are encouraged to report security incidents observed by them. This includes any incidental mistakes that have happened which may cause the security to be jeopardized.

   c) Information System monitoring tools like Network Monitor, Intrusion Detection / Prevention system etc may be configured to automatically alert or report suspicious events or incidents.
   d) Security incidents comprise of both IT and Non IT events.
      - Virus infection.
      - Unescorted person or unidentified (Non Staff) moving in the premises.
      - Problems with Door Locks (Entry gates)

2) Evaluation of incident.
   a) Assess if the report is an incident, false trigger or a hoax.
   b) Assess the type and extent of the problem.
   c) Determine the priority level and action the plan accordingly.
   d) Determine whether the incident activity is actively occurring or has ceased; if ceased, whether it is likely to resume.
   e) Determine which and how many systems and data are actually or likely affected; also assess whether the incident activity has occurred solely within your domain, or whether external activity is involved (as a source or downstream target).
   1. Evaluate the damage done if a breach has already occurred.
   2. Estimate a rough schedule of recovery or control measures.

3)Response to an incident
   a) Inform the concerned authorities
      - Inform the management / superiors about the incident and the path forward.
      - Make sure the management is informed at critical milestones.
      - Decide in accordance with management's approval the immediate aims. This could include bringing the system back, minimizing the down time or going all out to track the attackers etc.
      - Inform Q-CERT, Legal Enforcement and request assistance if required.

b) Collect the evidence
- Document the damage done.
- Take a full backup of all logs and the complete system.
- Take a backup of logs from the firewall, routers, IDS and other security devices that may help in diagnosing the breach.
- Document actions performed to control / contain / eliminate the incident.

c) Control / Contain / Eliminate damage
- Identify the source of problem (Threat).
- Identify the weakness that caused the system compromise (Vulnerability).
- Make sure that the vulnerability is eliminated / mitigated and the breach is controlled. Realize that intruders may have installed Trojans, key logger or such programs on compromised systems

d) Restore Services
- After eliminating the vulnerabilities in the system and confirming that the damage is controlled ensure that the system is up and running.
- Check all live services provided by the system.
- Monitor the system for any further problems or deterioration of services.
- Conduct security tests (Penetration test / Scan) to ensure that the system is performing as required.
- Release the system for public usage.

IM 4. Define procedures to report, manage and recover from information security incidents, internally, with Q-CERT and with other Agencies.

An IM Manager shall build an Incident Response Capability (IRC) within the **Agency**. In this case, Q-CERT would play the role of Government Incident Response Office (GIRO) and provide central coordination and support to the operation of individual IRCs of **Agencies**.

Respective IRCs of **Agencies** would be responsible for overseeing the incident handling processes of specific information systems or networks, computer services, or functional areas within their own **Agency.**

Communication plans and channels shall be established to communicate information with QCERT , Law enforcement agencies and other Agencies (if needed) during normal and crisis situations.

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

The NIA Manual mandates that the Incident Management process is integrated with Security Awareness training. All users should be educated to report incidents. Users may also be educated on how to respond to certain incidents e.g. Fire, Natural disasters etc.

Agency shall create user friendly channels for reporting of incidents.

IM 6. Categorise and prioritize all incidents according to the incident criticality classification provided in Appendix C.

In order to ensure uniformity and optimum utilization of resources, it is prudent to classify and prioritize the security incidents based on the incident criticality classification table provided as an appendix to the NIA policy.

IM 7. Co-ordinate with Q-CERT to create a repository of incidents in the Agency.

The NIA Manual mandates that all security incidents are documented. After ensuring that the system has recovered, the IRC shall endeavor to record the following information:
- ➢ Document and compile all the information regarding the complete incident.
- ➢ Open a case with concerned Law enforcement agency, depending on the type of incident and amount of loss and dependent upon severity.
- ➢ Identify the lessons learned during the incident. Evaluate if the processes could be improved to handle the situation better. Share the lessons with other **Agencies** through Q-CERT to prevent similar attacks.

IM 8. *Report all Criticality Level 1 incidents to Q-CERT within one (1) hour of identification.

The NIA Manual mandates that optimum government resources are available to resolve an incident that may be of paramount interest to the nation. Criticality Level 1 incidents are identified as those that may involve a part of Critical Infrastructure of the nation.

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.

Incident management coordinator should draw up an annual plan to simulate how the organization should respond to as incident. Tests may be carried to check efficacy of the processes and cautions in place. Such tests include but are not restricted to Table top review & simulation, practical tests, audits, etc. The idea is to ensure the organization maintain currency of its processes, controls and systems and that they are operational and work as designed during an incident or crisis. Testing should also include chain of custody, handling of logs, forensics and lessons learned.

9. Guidance on Business Continuity Management [BC]

9.1. Guidance on Policy and Baseline Controls

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

The Agency shall appoint a person (known as the Business Continuity Manager) to manage the Business Continuity (BC) Program. The Agency should further ensure that the BC Manager has commitment and support from the management, together with approved and allocated budgets for Business Continuity Management (BCM). The BC Manager may in turn form a team, which includes champions from individual business divisions to drive the BC program.

The BC Manager or team shall have the following responsibilities

- Develop and approve (in consultation with the **Agency's** management) a BCM program.
- Undertake or manage the appropriate BCM activities within the **Agency**.
- Promote BC across the **Agency** and externally where appropriate.
- Manage the BCM budget.
- Maintain the BCM program documentation.
- Research the current state of readiness of **Agency** and the level required by legislation and regulation.
- Report on the current state of readiness to the **Agency's** management on a regular basis highlighting where there are identified gaps.
- The BCM team may (in consultation with business managers) identify and train BC representatives in operational departments or at other locations to:
  - Act as a point of contact for BC issues affecting the department or location
  - Assist the department to identify the BC implications of process change
  - Notify the BCM team of process changes
  - Assist or lead the department's or location's recovery in the event of a disruption.

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 Agency process.

Agencies should follow a defined procedure while preparing a BC plan. The key step in preparing a BC Plan is conducting a Business Impact Analysis (BIA) to identify the processes and functions critical to the Agency. The exercise is an extension to Information Classification exercise performed by the **Agency.**

1. Identify key processes and their owners within the Agency.
2. Identity process dependencies: information, applications, systems, networks, etc.
3. Identify the Availability requirements. This is A of the C-I-A triad (Confidentiality / Integrity / Availability).
4. Document time sensitiveness of key processes. For example: Availability requirement for payroll application is very high at month's end, while processing salaries.
5. Estimate tangible (Financial and Non-Financial) and intangible impacts, resulting from the inoperability of each critical function or service.
6. Define Maximum Tolerable Outage (MTO)* for the process.
7. Define the Recovery Point Objective (RPO)** for the process.
8. Based on the above calculate the Recovery Time Objectives (RTO).

Agencies should use the results of the business impact analysis and threat and vulnerability assessment to develop and implement an information technology business continuity plan that will help enable the continuation of critical information technology processes and delivery of essential services, at an acceptable level, in the event of a disruption. The plan should also address the recovery of agency information technology facilities and capabilities if those processes or services fail.

The result of BIA along with the Threat Vulnerability assessment (Risk Assessment) would enable the Agency in implementing controls to ensure availability of the process by mitigating the risks and in effect designing a suitable BC Plan.

The BCP should be updated regularly to ensure it is current and effective. The plan must be approved by the management should be tested.

* Maximum Tolerable Outage (MTO): This is defined as the duration after which an organization's viability (either financially or through loss of reputation) will be irrevocably threatened if delivery of a particular product and service cannot be resumed.

**Recovery Time Objective: This is defined as the target time frame for the restoration of a process or service after a disruption has occurred. RTO SHOULD be less than the defined MTO

***Recovery Point Objective (RPO): This is defined as the point to which information must be restored to enable an activity to operate once it is resumed

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

The NIA Manual mandates that while conducting a BIA, **Agencies** should take in to account different Business Disruption Scenarios, whether mild or severe. The BC plan should anticipate a variety of disasters and incorporate protections that are common to as many scenarios as possible.

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.

Agencies should ensure that any major change or improvement in their process or infrastructure is reflected and updated in the Agency's BC Plan. It should also ensure that all such changes are tested during the next regularly scheduled testing exercise.

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.

Agencies shall ensure that business continuity plans are properly secured and distributed.

Agencies shall maintain copies of the **Agency's** business continuity plan (BCP) and any other related critical documents and materials at a predetermined, secure off-site location. Designated personnel on the contact list should be given location and access information.

Agencies should ensure that, where appropriate, the existence and content of the **Agency's** business continuity plan (BCP) is conveyed to other **Agencies**.

Agencies should draw up procedures to ensure that a copy of the most updated (as per the policy of the Agency and governed by RPO and RTO) back up is available on an off-site location.

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 Agency's requirements.

Based on the results of BIA and other regulatory requirements, Agencies should identify the needs for an alternative site. Choice of an alternative site should be governed by the RPO and RTO factors.

Hot Site:

A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software. Following a disruption to the original site, the hot site exists so that the organization can relocate with minimal losses to normal operations. Ideally, a hot site will be up and running within a matter of hours or even less. Personnel may still have to be moved to the hot site so it is possible that the hot site may be operational from a data processing perspective before staff has relocated. The capacity of the hot site may or may not match the capacity of the original site depending on the organizations requirements. This type of backup site is the most expensive to operate. Hot sites are popular with organizations that operate real time processes such as financial institutions, government agencies and ecommerce providers

Warm Site:
A warm site is a location where the organization can relocate to after a disruption, which is already stocked with computer hardware similar to that of the original site, but does not contain backed up copies of data and information. It may or may not have the same capacity as the original site depending on the organization's requirements. Data will have to be restored onto the equipment at this site before activities can re-commence.

Cold Site:

A cold site is the most inexpensive type of backup site for an organization to operate. It does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. The lack of hardware contributes to the minimal start-up costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster.

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

Agencies should establish strong controls in information technology contracts that involve outsourcing a portion of their business or information technology functions or business continuity services. **Agencies** should consider whether the risks associated with maintenance of agency data preclude use of a contractor for outsourced functions. The BCM should be involved in the staffing of outsourcing contracts.

Agencies should assess whether contractors have the following business continuity controls in place:

a. A business continuity plan (BCP) based on business impact analysis and risk assessment
b. A testing plan for the business continuity plan that is exercised regularly
c. Assurances that notification for service outages will be given which are backed and governed by SLA’s

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.

Agencies should test their business continuity plan at least once a year. At a minimum, the test should be for the most likely scenario with tests for less likely scenarios conducted as deemed necessary. The type and extent of testing will depend on the criticality of the business function supported by technology and the complexity of its processes and components.

Business Continuity Tests may include any or all of the following:

Table top Exercises: A table top exercise is a method of testing the business continuity plan that does not have a significant impact on daily operations. The business continuity team reviews and discusses the actions they would take to specific disruption scenarios as outlined in their plans, but they do not actually perform any of these actions. The exercise can be conducted with a single team or multiple teams as appropriate.

Simulations / Workshops: A Test Scenario is compiled based upon realistic circumstances considering industry / location and potential threats. The team members will then be asked to invoke the plans (as per the BCP) and to perform their individual roles in order to recover from the scenario.

Part Recovery Tests: In this scenario a disruption scenario is considered and a live recovery is attempted. However, only a part of the process or function or infrastructure is tested. In some variants this may involve recovering certain functions, infrastructure etc, usually off-site without disturbing the live scenario.

Full Recovery Tests: In this scenario, a disruption scenario is considered and the complete system, process or infrastructure is recovered usually on an alternative site as per the defined BCP. This usually involves a complete mobilization of the work force, management authorization and carries a high risk as normal operations are affected. However the success of this test is a real indication of the effectiveness of the BCP developed by the team.

BC 9. *Awareness about the BC plan is created amongst its employees.
Agencies shall establish Business Continuity education and awareness efforts as part of the Agency's Security Awareness program. At a minimum, the awareness program should address the following:

a. Convey to all employees the rationale and importance of a Business Continuity Plan.
b. Explain to employees their roles, responsibilities and expectations of Agency in case a crisis or a business disruption occurs.
c. Educate and create awareness amongst employees on the different communication channels and processes that shall be used to communicate in case if a crisis or a disruption occurs. For e.g Explain how to use a "Call Tree" to communicate with colleagues, alternative means of communications e.g. Satellite Phones, Radio communications etc as may be available within the agency.

10. Guidance on Logging & Security Monitoring [SM]

10.1. Guidance on Policy and Baseline Controls

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.

Agencies shall ensure that procedures exist which mandate logging, identification and monitoring of access to and protection of information. The procedure should define the assets and the processes that should be monitored. Suitable processes/technology should be employed for enabling continuous monitoring.

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

Agencies should ensure that monitoring practices are established in accordance with the criticality of the information, process and the infrastructure. This is to ensure that adequate resources are being expended in monitoring the resources.

The NIA Manual further emphasises the fact that split responsibilities or 4 eyes principle should be in place for the monitoring process as well.

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.

Agencies should ensure that all monitoring and logging activity is in line with various regulatory and legal frameworks. Monitoring and Logging should cover use and access of the system.

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 with a confidentiality rating of C2 and above.

Agencies should ensure that as a baseline, all data equipment protecting or processing information classified with a confidentiality rating of C2 and above should be enabled with logging.

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.

Agencies should ensure that Security logs of the system are rated with a confidentiality rating of C3, while application and system logs should be accorded ratings as per the confidentiality rating of the system. Access controls should be defined to ensure that security logs are protected from unauthorized access and tampering.

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

Agencies should ensure that logs that contain personal information are adequately protected in line with the Proposed Information Privacy & Protection Law.

SM 7. *These logs are retained for a minimum of ninety (90) days and a maximum depending on criticality assessments and sector specific laws and regulations.

Logs shall be retained for 90 days. It is not required to have the logs online in a system and the same may be archived or available offline. However in case it is maintained offline or archived, means should exist to access these logs with relative ease.

SM 8. Agency'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 systems to its original state.

Agencies should ensure that adequate and appropriate logs are maintained in the system to assist in reconstruction of incidents if required. This specifically being a case; when the administrators may deem it necessary to prune the quantity of logs generated by way of logging only specific events alerts and alarms.

Basic elements such as date, time, authentication, failed actions should be logged to be able to identify red flags if any.

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

Agencies should ensure that the processes are well integrated. In this case the System monitoring should be integrated with Incident Handling. Exceptions observed in the system by way of monitoring system logs; alarms etc should be registered and action through the Incident Management process. The integration may be automated or manual.

11. Guidance on Data Retention & Archival [DR]

11.1. Guidance on Policy and Baseline Controls

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. Agency policies & needs

b. Regulatory requirements

c. Legal requirements

One of the biggest challenges today is about storage of data and how long do we store it. The NIA Manual mandates that the Agencies draw up a policy which defines the retention period for the information they collect, generate and hold. The Agencies should decide on the retention period primarily on the factors mentioned above. There may be other factors that may be considered based on the Agencies specific requirements.

Procedures should exist to destroy information as per the Agency's Media Sanitisation policy once it has completed its usability.

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.**

Agencies should ensure that Data retained for business needs complies with the confidentiality, integrity and availability requirements of the data classification. The controls should be applied not only to data that is online, but also that has been archived or stored offline in line with Agency's archival policy.

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

NIA Manual would like to re-emphasize the importance of adhering to government laws and regulations that may be applicable to information in custody of the Agency. Personal & sensitive information that is retained by the Agency should be retained as per the proposed Data Privacy legislation.

Procedures should exist to destroy personal information after it is no longer necessary to maintain it in line with the proposed Data Privacy 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.**

Agencies shall define standard operating procedures (SOP) for backup, archival and recovery of information. Care shall be taken to ensure that confidentiality and integrity of data is not compromised during these processes. Controls shall be enabled in accordance with the highest classification of data stored, processed or recovered.

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

"Out of sight and Out of mind" is an age old proverb, but yet highlights to a certain degree the way how human mind works. It is not very uncommon that technologists tend to concentrate on online data and data that are in perennial use. However Agencies should ensure that security controls on data that is archived and backed up on offline media, disaster recovery sites or off site areas are in place in accordance to the classification of information it holds. All such media should be suitably marked and secured accordingly. Procedures should exist that define how such media shall be marked and handled.

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.

One of the key concerns while archiving data is maintaining the relevancy of the technology. Technology for storing and accessing data has made rapid strides in the past few decades. Bulky magnetic data tapes have given way to DAT, DLT, CD, DVD etc. It is necessary to ensure that data during its life time is maintained so that it may be readily accessible, in case of scenarios where the Agencies have changed their technology it should ensure that all relevant data in archive is suitably migrated to the new technology.

12. Guidance on Documentation [DC]

12.1. Guidance on Policy and Baseline Controls

DC 1. *Produce an Agency security policy, incorporating the requirements of this National NIA Manual.

Agencies shall prepare an Information Security Policy customized to the needs, requirements and objectives of the Agency and aligned with the National IA policy.

The Agency's security policy shall form the core foundation for the implementation of an Information Security Management System within the Agency.

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

The NIA Manual mandates that the Agency undertakes due diligence in maintaining the information system documentation. At a minimum level every system that has been deemed as critical to the Agency shall be assessed and covered by a security plan.

Agency shall ensure that at minimum critical processes are identified and Standard Operating Procedures are created to maintain such processes. Such SOP's should include agreed information security controls.

NIA Manual does not intend to document each and every process in a written format as long as all the employees (related with the process) are conversant with the procedure and a mechanism exists to ensure the flow of knowledge to new employees.

However, Agencies should note that written procedures provide immense value during emergencies and disasters.

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

NIA Manual intends to re-emphasise that Agency's information security standards and procedures should be aligned with the Agency's security policies and objectives which in turn should be aligned with NIA Manual.

A consistency in following the above edict will ensure that all processes are in sync and inline with the Agency's policies and procedures and NIA Manual.

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

All ICT security documentation shall be classified as a minimum of C3. Relevant security controls shall be applied in accordance with this classification.

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

Agencies shall have defined procedures as part of its document management methodology to perform periodic checks to ensure that ICT documentation is current and up to date.

It shall ensure that Change Management procedures include provisions to update the relevant system documentation as part of the process.

Documentation shall have a defined review cycle which should be maintained as part of the document management attributes.

13. Guidance on Audit & Certification [AC]

13.1. Guidance on Policy and Baseline Controls

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

Agency shall ensure the establishment of an Information Security Management System (ISMS) in compliance with the National Information Classification Policy and the accompanying National Information Assurance Manual.

Agency shall appoint an Information Security manager, where the **Agency** is spread over multiple geographical sites with significant Information assets at remote sites, a local site Information Security administrator, may be appointed.

However, the Agency's Information Security Manager will retain the overall information security responsibilities.

Agency shall ensure that

1. Information Security Manager is suitably qualified and has the requisite experience and domain expertise.
2. Information Security Manager has the security clearance to access the highest classification of Information processed by the **Agency.**
3. Information Security Manager has access to and the full support and confidence of the senior management of the Agency.
4. Information Security Manager does not hold any other conflicting roles and responsibilities.
5. Information Security Manager reports directly to the head of **Agency** or **Head Internal Audit.**
6. In case if the Information Security functions are outsourced, the Information Security Manager shall remain independent of the outsourcer.

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

Agencies shall comply with the relevant provisions of Laws and Regulations that exist at the time and those which may be amended and added at a later date in time.

Agencies shall specifically ensure compliance with the following laws (*Existing and Proposed New)

1. CIIP Law
2. Proposed Information Privacy & Protection Law
3. Ecommerce Law
4. Cybercrime Law

AC 3. *Be audited by the Certification Body or an independent body designated by MOTC.

Designated Certification Bodies shall be responsible for auditing compliance of Agencies with the National information Classification Policy and the National NIA Manual. Alternatively the Certification Body may designate independent third party auditors that may be suitably accredited by them to carry out such audits.

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 Agency.

The audit carried out by the Certification Body or its designated authority shall be valid for a year. Agencies shall be responsible to ensure that they remain certified all the time. As such an annual exercise shall be carried out to review and audit the security posture of the Agency.

In case if a major change has occurred that has impacted the infrastructure, people or processes then it is mandatory to have a re-audit by the Certification Body or its designated authority.

AC 5. *Ensure that the scope of the audit process includes all information assets, people and processes.

The Certification Body should ensure that the scope of the audit process includes all information assets, people and processes.

The NIA Manual mandates that the Agency includes all its infrastructure, processes and people as part of the scope; however it may not be prudent or possible to have the complete accreditation in one attempt. However the wheel should be set in motion to achieve the final target.

The Certification Body shall provide advice on setting up SMART scopes for the Agencies. The Agencies on their part shall provide a roadmap to the Certification Body for achieving the complete compliance.

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.

In case if a major change or a security incident has occurred that has impacted the infrastructure, people or processes or invalidates or questions the existing accreditation, then it is mandatory to have a review of the accreditation by the Certification Body or its designated authority within the prescribed time.

The review time shall be prescribed by the Certification Body once it has been notified of the change. Agencies should ensure that they collaborate with the Certification Body in case of a planned change and or notify immediately in case of an unplanned change / security incident.

AC 7. *Ensure that all non-conformances are fixed in a defined timeline.

Agencies shall ensure that any non-conformance highlighted during the audits is fixed in a defined timeline. The Certification Body or its designated authority shall be responsible for ensuring that the review has been carried out by the Agency in the defined period of time.

The time limit shall be defined by the Certification Body or its designated authority in consultation with the Agency.

AC 8. *Ensure that any exemptions are approved by the Certification Body.

Agencies shall ensure that all infrastructure, people and processes are part of the audit. In case if they wish to seek an exemption, a case shall be presented to the Certification Body defining the scope of exemption, reason for exemption, risk analysis of the exception and an approval from the head of the Agency or the head of the Internal Risk department.

MOTC shall decide and approve on the exemption based on the merit and demerits of the exemption case.

Section C

1. Guidance on Communications Security [CS]

1.1. Policy Objective

1.2. Guidelines on Policy & Baseline Controls - Cabling

In order to comply with this policy, **Agencies** MUST ensure:

CS 1. Conduits (tubes, ducts or pipes) are used to protect cables from tampering, sabotage or accidental damage, when they are carrying data classified at C4 and above. This control is RECOMMENDED for data classified at C2 and above.

Sniffing and wiretapping are amongst the most common means of pilfering information. The task becomes easier if the cables are left unprotected and uncovered. Basic controls like running cables through tubes, ducts or pipes can provide protection for the cable and the data flowing through it against tampering, damage (wilful or accidental) and sabotage. The protection chosen should be based on the classification of the information and a proper threat assessment.

NIA Manual mandates this control for information classified as C4 and recommends it for information classified as C2.

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

In order to reduce the risks of sniffing and wiretapping, Agencies should ensure dedicated cable distribution system for information classified as C4 and above. This shall be further improvised with proper access controls (physical and personnel)

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

The NIA Manual intends to subscribe to the concept of “Security by Obscurity” albeit in a limited manner. It would be prudent on the part of Agencies to ensure a certain amount of obscurity while labelling cables and conduits especially in public or visitor areas if they are not under surveillance.

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.

NIA Manual mandates that Agencies maintain proper documentation for network points (data and voice) under their jurisdiction. A detailed documentation of network points assists the support team in trouble shooting network issues, identifying rogue devices connected to Agency’s networks and capacity planning.

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

Agencies shall draw up procedures to ensure that cables and connected points are consistent with its documentation. A regular audit / check shall assist the Agency in identifying rogue devices connected to the Agency's network, damage that may cause deterioration of network services amongst other things.

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

In a critical organization or a critical environment it might be prudent to build redundant communication pathways to facilitate redundant cabling through redundant routes. This will reduce the threat of a redundant cable fails on case if one of the pathway is damaged due to any reason.

1.3. Guidelines on Policy & Baseline Controls - Telephones & Faxes

In order to comply with this policy, **Agencies** 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

Talking is one the identified ways in Social engineering for leakage of information. Humans talk with each other as a primary means to communicate their thoughts. And telephone systems (mobile / landline / satphones) are the most common technological medium used by humans to overcome the distance hurdle. Though an effective medium it is prone to threats like wiretapping, miscommunications (wrong numbers), identity management (you cannot identify a person on the other hand in a fool proof manner). As such it is essential that the Agency implement controls that include educating users on the permitted levels of classified conversations, usage of encrypted channels etc.

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.

Ensure that employees are educated on the perils of using speakerphone or conferencing systems while discussing classified information. This may lead to information leakage due to overhearing. In case if a situation warrants the use of such a medium, controls should be in place to suppress sound by way of sound proof offices.

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

NIA Manual mandates that pilfering or Sabotage of conference equipment through remote connections is not possible. This will mitigate the risks of being able to snoop on conversations through remote initiations of conference equipment.

Agencies should also look in to options of restricting the use of mobile phones in such sensitive locations, especially when sensitive information is discussed.

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

NIA Manual mandates that information is not compromised while being discussed in designated rooms due to leakage of sound or by overhearing by wilful / non wilful employees. The risk can be mitigated to an acceptable level by ensuring that suitable controls like use of sound absorbing materials are implemented.

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

The NIA Manual mandates that while faxing information classified with a confidentiality rating of C2 or above, encryption devices should be used at both the ends. This is to mitigate the risks of sniffing by encrypting the transmission channels.

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.

The NIA Manual mandates that any designated personnel within an Agency that sends a facsimile transmission is responsible to ensure that all baseline controls are applied to ensure confidentiality of the transmission. This covers ensuring that applicable standards are met at both ends including use of encryption devices for transmitting information classified as C2 or above. The Sender should inform the receiver before transmitting the fax and arrange for him to collect the fax as soon as possible. The receiver on his part should inform the sender if they do not receive the fax with the designated time e.g. 10 minutes.

2. Guidelines on Network Security [NS]

2.1. Policy Objective

2.2. Guidelines on Policy & Baseline Controls - Network Management

In order to comply with this policy **Agencies** MUST ensure that:

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.**

Agencies shall classify internal network and system related configuration, directory services etc as a minimum C2 i.e. limited access.
They shall implement sufficient controls to ensure that the information is not accessible by unauthorized personnel. This may include controls to protect the network perimeter e.g. firewalls.
Paper copies and electronic documentation of network device configurations, network diagrams, etc., shall be destroyed, when superseded, or no longer needed. Agencies should adhere to Data / Media Disposal policy in the NIA Manual while disposing such documents.
Employees / Outsourced Staff / Vendor personnel shall be educated on the Agencies policies through appropriate Security Awareness courses.

NS 2. **They remove or disable all the default accounts e.g. root, administrator, etc. or change the password as specified in section C-6, Guidance on Software Security** [SS]

The most basic Access Control system includes controls to identify and authenticate the user. The username provides identity and the password authenticates the claimed identity. Conversely to compromise a system's access the malicious user would also need to know the username and password. By ensuring that default usernames are disabled or deleted from the system, it would become increasingly difficult for the malicious user to compromise the system.

In case if this is not possible due to technical limitations, such user account shall be secured with password as specified in section C-6, Software Security.

All such user activity shall be audited to trace malicious activities

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, Guidance on Change Management** [CM]

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

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

Agencies shall define ownership for the operation and maintenance of the networks. A person shall be appointed as a Network manager or similar with responsibilities to operate and manage the network.

The Network manager shall be the custodian for all network related configurations. He shall maintain an updated documentation for the complete network. He should also be responsible for housekeeping which includes destroying old copies of network configuration other than those maintained for specific reasons like history or technical analysis or backup.

All changes to the network configuration shall be approved through a formal change control process as defined in section B-5; Change Management.

The Network manager shall be responsible to ensure compliance of the proposed change with the Agency's network security policy and security plan as defined in section B-12; Documentation.

The network manager shall review the network configuration at regular intervals.

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

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

The NIA Manual intends to re-emphasize the importance of complete and up to date documentation. The manual mandates that the Agencies have the necessary processes in place to maintain the documentation, further it advises on what documentation should be maintained.

NS 5. *Networks are designed and configured to limit opportunities of unauthorized access to information transiting the network infrastructure. Agencies 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 Agency network through techniques such as MAC address filtering.**
- **i. IPS/IDS to detect/prevent malicious activity within the network**
- **j. Time and day restriction**

The NIA Manual provides baseline security controls that shall be implemented in the Agency's network architecture. Due diligence shall be done to ensure that Networks are designed and configured to limit opportunities of unauthorized access to information while in transit in the network. The design and implementation shall restrict opportunities for sniffing of packets, hijack of sessions, eavesdropping of network etc.

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

a. **dedicated network 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.**

Agencies shall ensure implementation of the minimum specified controls for securing management networks. Device management shall be carried out either by in-band or out-of-band channels. In case of in-band channels, it shall prescribe to logical separation by means of virtual LANS. All such channels shall be suitably encrypted as it carries confidential information like username and passwords having administrative privileges, information monitored or inspected from other ports etc.

2.3. Guidelines on Policy & Baseline Controls – Virtual LANs (VLANs)

In order to comply with this policy **Agencies** MUST ensure that:

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

NIA Manual recommends baseline controls such as use of VLANs to segregate Data and Non data (Voice, Video) traffic in an Agency's network. Voice traffic requires a defined quality of service, in order to secure the voice traffic from bursts of data traffic it should be configured to operate in a separate dedicated vlan with defined QoS. Segregating the traffic also secures it against possible sniffing attacks on the local LAN.

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.**

Network Configuration is configured as a minimum of C2 level of information. NIA Manual mandates that administrative access to switches, network devices (which effectively means accessing the network configuration) should be from a VLAN which is at a same Classification level or higher. This will ensure that appropriate controls are in place to access these information.

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

NIA Manual mandates that the network switches are hardened (a process of securing the operating system and configuration of the switch) as per the best practices recommended by the vendor. Moreover additional security controls as recommended by the Agency's risk assessment shall be implemented.

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

The NIA Manual mandates that Trunking is not used on switches managing VLAN's of different classification to prevent possible compromise of information.

2.4. Guidelines on Policy & Baseline Controls – Multifunction Devices (MFDs)

In order to comply with this policy **Agencies** MUST ensure that:

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

The NIA Manual mandates that Network connected MFD's only process information classified at the level of their network connectivity classification or below. For e.g. if a network has been rated to carry information classified as C2, then a MFD connected to this may not process an information classified as C3.

NS 12. Where network-connected MFDs have the ability to transmit information via a gateway to another network, agencies 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.**

The NIA Manual mandates that all network connected MFDs that have an ability to transmit information via a gateway to another network must implement the minimum level of controls prescribed in the NIA Manual.

The prescribed controls are similar to those applied to a user workstation and include user identification, authentication and audit functionality. Passwords used should be of sufficient strength as per the Section 9.3; Access Management in the NIA Manual. MFDs are primarily shared appliances on network, as such it is necessary to identify task owners for information processed by the MFD. In case of an occurrence of an incident, it is necessary to identify the breach to an individual. Proper authentication and audit functions will provide the necessary tools to resolve such breaches.

Content filtering should be implemented to identify and filter data in accordance with the requirements of Information Exchange. Data sent out should be labeled as per its document classification.

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,**

The NIA Manual mandates that MFDs are not connected to telephone networks classified with a confidentiality level lower than that of the information being processed by the MFD. This is to prevent information leakage that may occur by transmitting classified information on a network that does not have sufficient controls.

Connections may be provided subject to an assessment that ensures sufficient controls exist within MFD to control data flow based on information classification.

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

Agencies should develop specific set of policies and procedures governing the use of MFDs within the Agency and / or its networks. The policies should define technical, management and operational controls.

The following are some management and technical security controls for consideration:

<u>Management and Operational Controls</u>

1. Educate users about the proper usage and protection of MFDs.
2. Implement sufficient physical security controls against thefts.
3. Conduct periodic IT security risk assessment covering the usage of MFDs in **Agency's** computer environment.

<u>Technical Controls</u>

1. Enable user authentication / password-protection feature of MFDs to protect against unauthorized usage.
2. Encrypt classified data before transmission.
3. Disable unnecessary network services such as infrared (IR) ports and Bluetooth to avoid being detected as attack points.

NS 15. Information classified at C1 or above is not retained permanently in the MFD. Where the MFD has features to schedule jobs, sufficient manual/automatic controls or configurations SHALL exist to remove the information from its memory once the job is complete.

Since MFDs are essentially shared devices, any information classified at C1 or above should not be permanently retained in MFDs. Controls should exist to clear memory of the completed tasks and any information related to it that may assist in reprocessing or replaying the information. This is essentially to ensure prevention of data theft.

NS 16. MFDs follow the procedures specified in section C, 8.3, Policy & Baseline Controls - Media Sanitization

All data stored by MFDs shall be deleted after the completion of task. In case when the MFDs are due for repairs (outside the office) or are being de-commissioned the storage media shall be treated as per the recommended Media Sanitization procedures. Agencies could consider controls / procedures such as ensuring that vendor technicians are escorted while the equipment is being repaired on-site.

2.5. Guidelines on Policy & Baseline Controls – Domain Name Service (DNS) Servers

In order to comply with this policy **Agencies** MUST ensure that:

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.

NIA Manual mandates that networks internal IP information is not released in the public domain. Segregating the DNS server for internal and external IP resolution shall ensure that IP information related to internal networks is not released or accessible from external networks.

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

DNS server forms a critical component in the network and is responsible for mapping the hostnames to IP addresses. NIA Manual mandates that this critical component is adequately secured and controlled. It emphasizes the need to own and locally host the services in a secured (hardened / bastion) server. Agencies may also use the Government DNS. Alternatively the Government DNS could also be configured as a backup DNS server.

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

The NIA Manual mandates that sufficient security and high availability design factors are considered while designing DNS services. Critical services such as DNS should be monitored pro-actively and secured as per the recommended industry best practices.

NS 20. ***Zones files are digitally signed, and cryptographic mutual authentication and data integrity of zone transfers and dynamic updates is provided.**

NIA Manual recommends security controls such as digital signing and cryptographic authentication of zone files that shall be implemented to ensure integrity and confidentiality of the data residing on a DNS Server.

NS 21. ***Cryptographic origin authentication and integrity assurance of DNS data is provided.**

NIA Manual recommends security controls such as cryptographic origin authentication and integrity assurance of DNS data that shall be implemented to ensure integrity and confidentiality of the data residing on a DNS Server.

NS 22. **DNS services including zone transfers are provided to authorized users only.**

NIA Manual recommends security controls such as restricting zone transfers to authorized users that shall be implemented to ensure integrity and confidentiality of the data residing on a DNS Server.

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, **Guidance on** Cryptographic Security [CY]**.**

NIA Manual mandates that Cryptographic functions related to NS 20 and NS 21 comply with requirements specified in section C-10, Cryptographic Security.

2.6. Guidelines on Policy & Baseline Controls – Internet Security

In order to comply with this policy **Agencies** MUST ensure that:

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

Agencies should ensure that security controls are in place to scan data downloaded from internet. All software and files should be scanned for malicious traffic e.g. viruses, spywares, Trojans etc. Mechanisms such as Content filtering gateways should be in place to scan web traffic such as HTTP, FTP etc. Limit daily downloads or strict prohibition of download should be considered for specific roles and systems.

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

Agencies should ensure that internet gateways are hardened and secured by implicitly denying all services except those specifically enabled and allowed.

NS 26. **Web browsers running on user's workstation are properly configured and updated. Agencies 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**

With the ever increasing dependency on internet web, web based applications, web browsers are one of the most widely used applications. NIA Manual provides guidelines to Agencies on how to secure web browsers to mitigate risks related to vulnerabilities in web browser software.

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

Agencies should ensure that they have adequate controls in place to monitor traffic, deduce patterns, usage etc in compliance with Section B-10, Logging and Security Monitoring. However such controls shall be governed by Agency's policies and procedures to ensure fair use of the technology. Security controls shall not be used to snoop on the privacy of the user, but to ensure that the user's usage complies with defined policies and procedures.

2.7. Guidelines on Policy & Baseline Controls – E-Mail Security

In order to comply with this policy **Agencies** MUST ensure that:

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.**

Agencies should ensure that they harden and configure their email server as a bastion server and adhere to the industry and vendor recommended best practices. NIA Manual provide guidelines to ensure that email servers are protected against recon attacks by ensuring that email headers do not reveal technical information (technology, version etc) about the server.

NS 29. **TLS protection is used with the SMTP Mail server in line with section C-10, Cryptographic Security [CY].**

NIA Manual mandates that Cryptographic functions related to TLS protection comply with requirements specified in section C-10, Cryptographic Security.

NS 30. ***They implement the email Sender Policy Framework (SPF) [RFC4408]. Agencies SHOULD only send undeliverable or bounce emails to senders that can be verified via SPF.**

NIA Manual recommends compliance with Sender Policy Framework (SPF) [RFC4408] to combat with the menace of SPAM.

NS 31. ***Internal email distribution lists are secured to prevent access from external parties to reduce the risk of unsolicited email.**

NIA Manual mandates that Agencies implement effective controls to prevent the menace of SPAM. Email policy should ensure that use of email distribution list is governed and restricted to internal usage. Such distribution list should not be addressable from entities external to Agency.

Additionally auto-reply types of e-mail (as the "out-of-office function) should be limited to only specific roles in order to minimize the spread of malicious e-mails such as SPAM, scam email etc.

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

Agencies should ensure that security controls are in place to scan incoming and outgoing email traffic. All data should be scanned for malicious traffic e.g. viruses, spywares, Trojans etc. Mechanisms such as Content filtering gateways should be in place to ensure that the SMTP traffic complies with the Agency's security policy.

2.8. Guidelines on Policy & Baseline Controls – Wireless Security

In order to comply with this policy **Agencies** MUST ensure that:

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.

Wireless Local Area Network (WLAN) is a type of local area network that uses high frequency radio waves rather than wires to communicate between devices. As such it becomes increasingly easy for malicious users to snoop into such networks. WLAN is based on IEEE 802.11 standard. The 802.11i standard was created for wireless-specific security functions that operate with IEEE 802.1X Agencies should ensure that where wireless LANs are used; sufficient security control mechanisms are put in place to secure the access. Security controls include documented policies and procedures which govern and advice on such connectivity. Technical controls such as strong user identification and authentication, use of encryption amongst other things should be used.

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. Agency 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 government network.

Agencies should ensure that technology is reviewed on a continuous basis. They should implement protocols which have been tested as secure. Currently WPA2 and EAP-TLS are recommended. Agencies however, should not rely entirely on the protocol to protect confidentiality and integrity of the data. Additional security controls such as secure Virtual Private Networks should be deployed

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.

Agencies should maintain an inventory of all devices with wireless interface cards. This shall assist the network administrator in detection of rogue wireless appliances. Procedures should be in place to maintain and monitor this inventory. Loss or Theft of wireless device shall be treated as a Security Incident and handled as per the Agency's defined Incident Management procedure. Remedial controls shall be initiated and may include controls like change of SSID and / or the encryption keys.

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

Rogue or unauthorized wireless access points provide a backdoor entry into the network. They may also introduce vulnerabilities in to a network by way of un-patched operating system used by the hardware, or an implicit vulnerability in a non-approved hardware. As such it is prudent on the part of Agency to ensure that procedures are in place and responsibilities assigned to scan the network at regular intervals to detect rogue / unauthorized wireless appliances.

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

NIA Manual intends to provide guidance on location of wireless access points. Agencies should ensure that Access points are located in such a way that it deters or minimizes attempts of network tapping from publicly accessible area. Agencies could opt for Security by obscurity approach here or ensure that all such access points are monitored.

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.

In an 802.1x setup, Agencies must also secure the client side. Some of the techniques can be to configure the clients to accept server certificates that are embedded/pushed by the IT team and disable the client from accepting new certificates, specifying the server address, etc. This is to prevent man in the middle attacks.

The 802.1x supports many authentication methods, from simple username and password, to hardware token, challenge and response, and digital certificates. This is made possible by using EAP (Extensible Authentication Protocol). EAP-TLS uses PKI for authentication, EAP-MD5 uses standard username and hashed passwords, LEAP is used for authentication both client and authentication server, EAP-TTLS uses PKI for authentication server and CHAP/PAP/MS-CHAP v2 to authenticate the client, PEAP is build-in to WinXP.

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 Agency's departments, system name or product name.

Agencies shall ensure that default passwords, SSID names, encryption keys, SNMP strings and any similar attribute shall be changed at the time of installation. Such default attributes introduce vulnerabilities in the system by making it easier for the malicious user to compromise the system. It has been found that the internet contains abundant resources on such attributes including default usernames, passwords and keys used by different brands of network and security appliances and software. Further attributes should not be named on organization or department names as it introduces additional vulnerability by allowing easy identification and further presenting itself as soft targets.

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.

NIA Manual mandates that when it is absolute must to use wireless for corporate business requirements, additional controls such as frequent change of encryption keys, disabling of SSID broadcast should be implemented. MAC address filtering although not fool proof is another effective but; cumbersome security control that may enhance the security posture.

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

Access Points (Wireless networks) should be secured from the Agency's network by the use of firewalls / gateways. Further the firewalls / gateways shall be configured with restrictive rules to control the data flow between the two networks.

NS 42. WIPS/WIDS installation is recommended for networks with C3+ to monitor threats from wireless installations like rouge Aps, DOS attacks, etc

The wireless network segment should contain the same controls used in the wired segment. Apart from these controls, there is risk of rouge access point. IPS/IDS capable of handling wireless traffic must be used to monitor them.

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 connection. Guest WIFI may have lower security and may only allow for connecting to the internet

The Agency may use multiple SSIDs to segregate varying levels of confidential information within a wireless network. For example: Corporate wireless access may be restricted to authenticated users, devices and encrypted, especially when handling sensitive information. Guest wireless may not have a similar security and may be logically/physically separated from the corporate network.

2.9. Guidelines on Policy & Baseline Controls – Clock Synchronization

In order to comply with this policy **Agencies** MUST ensure that:

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

The NTP server must also be hardened using best practices recommended.

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.

In today's era we have our processing equipment linked with each other. We no longer operate in isolated silos and companies have implemented enterprise solutions and have integrated various processes and solutions.

However, on a flip side when such systems face an issue or are compromised, it becomes an upheaval tasks to investigate on multiple systems.

The most important tool during such scenarios is the log files. This log files are time stamped according to the system time.

However if the time on different systems is not synchronized it would become very difficult to co-relate logs from different systems. In case of an incident the evidence may not have a legal standing.

The NIA Manual mandates that time on all computer and communication devices are synchronized to the local standard time. Agencies should draw procedures or implement controls to ensure that if there is a drift, the clock is able to correct itself either manually or through automated procedures.

The order of preference in using synchronizing clocks is as follows:

1) Internal atomic clocks,

2) Internet based atomic clocks.

For government agencies: GN clock (Government Network).

NS 46. Agency's MAY use the authorized Qatari Government time server (a part of the Government Network) as the primary NTP server.

Agencies MAY use the Qatari Government Time Server as the authorized NTP server. This server is being proposed as part of the Government Network. However till such time as this service is not available, Agencies may use one of the reliable publicly available NTP servers.

NS 47. All servers and network devices are synchronized with the local Agency NTP server which is synchronized as specified in NS 45 & NS 46.

To limit the flow of network traffic to the Government NTP Server, it is prudent on the part of the Agencies to configure a server in their local network as a NTP Server. This server will act as a secondary server to the Government NTP server and will have its time synchronized with the Government NTP Server.

2.10. Guidelines on Policy & Baseline Controls – Virtual Private Networks (VPNs)

In order to comply with this policy **Agencies** MUST ensure that:

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.).**

NIA Manual mandates that strong and secure authentication mechanism is used for VPN access control. It recommends the use of either one-time password authentication such as a token device or a public/private key system with a strong passphrase.

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

Unused connections to system / network hog resources and undermine the capacity of the system / network. Such connections if left unattended present a serious risk to the system, as it may provide an unauthorized access to the malicious user.

Agencies should ensure that controls are in place to conserve the network resources available and secure access windows provided to its staff to connect to its resources normally. Technical controls should be implemented to disconnect a user after a pre-defined period of inactivity. The user shall be forced to logon again to reconnect the network. This ensures that logon credentials are not cached which is again a security risk.

Further this controls are primarily intended for end users, however it may also be extended to site-site VPN connectivity subject to it meeting the network requirements.

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

Split tunnelling is a computer networking concept which allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection.

A disadvantage of this method is that it essentially renders the VPN vulnerable to attack as it is accessible through the public, non-secure network. When split tunnelling is enabled, users bypass gateway level security that might be in place within the company infrastructure. For example, if web or content filtering is in place, this is something usually controlled at a gateway level, not the client PC.

NIA Manual recommends that Dual (split) tunneling should not be enabled. In case where this is mandated by business requirements, Agencies shall ensure that suitable security controls are in place to mitigate the associated vulnerabilities.

NS 51. **All computers connected to an Agency'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 time and with the latest virus signatures and malicious code definitions.**

Agencies shall define policies and procedures for acceptable usage of VPN. Agencies should ensure that computers connected to Agency's networks via VPN are equipped with personal security software, updated security patches and malicious code detection and repair software. All such security software shall be activated at all times and updated with the most recent patches, signature and code definitions.

Agencies shall ensure that technical controls are in place to ensure compliance of the above policy by all connecting computers. NIA Manual recommends use of Network Access Control appliances to ensure policy adherence.

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

NIA Manual mandates that baseline controls such as Gateway level firewalls are implemented to control flow of traffic from VPN clients to authorized information systems or servers.

2.11. Guidelines on Policy & Baseline Controls – Voice over IP Security (VoIP)

In order to comply with this policy **Agencies** MUST ensure that:

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.**

Voice traffic requires a defined quality of service, in order to secure the voice traffic from bursts of data traffic it should be configured to operate in a separate dedicated vlan with defined QoS. Segregating the traffic also secures it against possible sniffing attacks on the local LAN.

Agencies should ensure voice and data networks are separated, although physical separation may be an ideal case, virtual LANs are permitted. Further the gateway employed to segregate the voice and data traffic should be voice compliant and should be able to effectively handle voice related protocols such as H.323, SIP etc.

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

NIA Manual mandates that the gateways deployed are voice capable and are complemented with appropriate security mechanisms designed to handle voice traffic.

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

The Secure Real-time Transport Protocol (or SRTP) defines a profile of RTP (Real-time Transport Protocol), intended to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications.

SRTP also has a sister protocol, called Secure RTCP (or SRTCP) Secure RTP control protocol; SRTCP provides the same security-related features to RTCP, as the ones provided by SRTP to RTP.

Utilization of SRTP or SRTCP is optional to utilization of RTP or RTCP; but even if SRTP/SRTCP is used, all provided features (such as encryption and authentication) are optional and can be separately enabled or disabled. The only exception is the message authentication feature which is indispensably required when using SRTCP.

NIA Manual mandates that Agencies evaluate and use security enabled protocols to ensure confidentiality and integrity of the voice data. It recommends protocols like SRTP, however in future Agencies may select other protocols that may be available and may be better suited to the Agency's requirements.

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

Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to perform traffic analysis. Therefore, adequate physical security should be in place to restrict access to VoIP network components. NIA Manual mandates that proper physical security controls are in place to secure the VoIP infrastructure.

NS 57. *Adequate call log monitoring is implemented.

VoIP has helped converge voice and data traffic. And although it provides numerous advantages it is besotted with as many disadvantages. Primarily being the security, it is now exposed to security concerns related to data traffic. Some of the risks include Toll frauds, Eavesdropping, Interception and modification.

Agencies need to do a proper risk assessment and come up with adequate control to secure their VoIP infrastructure.

NIA Manual's mandate to implement and monitor call logs is essentially an operational control to ensure that the organization's VoIP infrastructure is not compromised. By monitoring call logs Agencies shall be able to ensure if VoIP infrastructure has been compromised to make unauthorized calls, divert calls, or if unauthorized extensions have been created etc. It does not refer to recording of calls and must align with the Proposed Privacy Laws.

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

NIA Manual mandates that Agencies evaluate and define policies and procedure regarding the use of soft phones. If the use of soft phone is mandated by business requirements, Agencies should ensure that sufficient security controls are implemented to secure its connections.

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

NIA Manual mandates that sufficient backup power is available to ensure availability of VoIP services in case of a general power failure.

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

NIA Manual mandates that strong authentication and access controls are implemented to protect voice gateway systems.

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

NIA Manual mandates that IPSEC or SSH or any other similar secure protocol is used for remote management or access to the VoIP infrastructure.

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

Agencies should define and communicate to its employees its contingency plans for making voice calls in case if the VoIP infrastructure is not available.

Agencies may decide on this as part of their Business Continuity planning exercise. A BIA (Business Impact Assessment) may guide the organization in identifying a suitable backup technology. Examples include use of mobile phones, use of PSTN. Satellite phones etc.

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

NIA Manual mandates that port security features on network LAN switches are enabled to provide additional security for the VoIP devices.

2.12. Guidelines on Policy & Baseline Controls – Internet Protocol Version 6

In order to comply with this policy **Agencies** MUST ensure that:

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

Any technological change shall be implemented after due assessment of the risks it presents to the organization. Agencies shall conduct a risk assessment to assess the suitability of IPv6 to the organization. NIA Manual recommends that Agencies should have a defined roadmap for migrating to IPv6.

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

NIA Manual mandates that Agencies carry our Risk Assessment to specifically assess the threats and vulnerabilities in operating a dual stack environment. This scenario may arise considering facts like partial migration, legacy equipment etc.

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

As in any other major change impacting the security posture of the organization, Agencies shall have to reaccredit itself after migration of their networks to IPv6 technology. This shall be the case even if the migration has been partial as in some selected segments of the network

3. Guidance on Information Exchange [IE]

3.1. Policy Objective

3.2. Guidance on Policy & Baseline Controls

To meet the requirements of this policy **Agencies** SHALL:

IE1. Prior to establishing cross-domain connectivity, the Agency evaluates, understands and accepts the structure, security and risks of other domains. This risk review SHALL be documented for compliance requirements.

NIA Manual mandates that due diligence is carried out in assessing the structure, security and risks of the target domain with whom a cross domain connectivity is intended. The risk assessment carried out shall be documented and the records maintained as per the audit requirements.

Agencies shall ensure that classification of information is maintained across the target domain.

IE2. *When intending to connect an agency 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 agency network to the other network, particularly where a connection to an un-trusted network such as the internet may exist.

The NIA Manual provides additional instructions in terms of due diligence to be carried out while assessing the suitability of connecting the Agency's network to another secure network Agency. It should be understood that by connecting to an external network, the risks multiply manifold unless specific and stringent controls are implemented at the gateways connecting the two networks.

IE3. 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 a NDA template.

NIA Manual mandates that the two entities exchanging information have chalked out, agreed and signed appropriate agreements by authorized signatories in their respective agency.

The agreements shall include details on the agreement to exchange information, technical details on how the exchange shall be provided, defined responsibilities and named positions within each agency to govern, monitor and operate the exchange of this information.

Both the agencies shall agree on the controls (Technical and administrative) that shall be implemented to facilitate this control.

IE4. Ensure media which is used to exchange information is protected against unauthorized access, manipulation or misuse within or outside the Agency environment.

Agencies shall ensure that adequate controls (based on classification of information) are in place to secure the media against unauthorized access, manipulation or misuse within and outside the Agency.

Agencies should consider controls like tighter inventory controls, use of Agency procured and certified media, encryption of media, physically secured safes.

IE5. Maintain the classification and protection of information that has been obtained from another Agency.

Agencies shall ensure that they maintain the classification and protection of information that has been obtained from other Agencies. Such mandate shall be imbibed in agreements signed between the Agencies before they start exchanging data transfer with each other. Agencies shall have the discretion to deny information transfer if the destination agency does not have the wherewithal to meet this requirements.

IE6. 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.

Agencies shall ensure that appropriate level (based on classification of information) of physical security controls are in place to secure the media while it is at rest or in transit.

Agencies should consider appropriate controls for storage, filing and packaging of media. Examples of such controls include

1. Ensure that environment conditions specified for media is maintained e.g. temperature, humidity etc
2. Use opaque, non-reusable, closed and correctly addressed media covers / envelopes.
3. Ensure that the address includes correct addressee name and address, along with a return address in case of non-delivery
4. If you consider information particularly sensitive or strictly private and you do not want the mail to be opened by a third party (assistant, secretary, etc.), the envelope must not only bear the confidentiality indication, but also the message: "To be opened by the addressee only".

IE7. *Ensure only reliable and trusted courier service or transport organization SHALL be used based on a list of known and authorized couriers.

Agencies shall consider suitable controls for transportation of media. This should include controls like use of security vetted couriers, security vetted third party safe lockers.

Use of such third party service providers will be guided by controls specified in Section B3, Third Party Service Management.

IE8. *Protect information exchanged via electronic messaging from unauthorized access, change or interruption of service.

Agencies shall implement controls to ensure confidentiality and integrity of information exchanged via electronic messaging. Although primarily this refers to electronic emails, it shall include messages sent through mobile devices such as blackberry, SMS etc.

The controls chosen shall be based on the classification of information, while selecting controls for the platform or the infrastructure (e.g. Email Server) the controls chosen shall be based on the highest classification of information that the platform / infrastructure shall process or transmit.

Following are guidelines for choosing controls for electronic transmission.

a. Secure communication should be used for transmitting or receiving email. Most of the mail servers support SSL based POP and SMTP communication.

b. When sending by electronic email,

1. Double-check the accuracy of the address or the list of addressees before transmitting the information by e-mail.
2. When sending Restricted and Limited Access information by e-mail, double check e- mail addresses are correct. When using predefined address lists, double check that all persons included on these lists are authorized to receive the information. Do request for a proof of submission, and delivery.
3. Verify if additional protection in terms of password protected attachments, encryption or digital signature is required before transmitting the email.
4. All information classified as C2 shall be at a minimum protected using passwords. Information shall be sent in password protected attachments through email. The password shall be conveyed to the recipient through separate means of communication e.g. voice, sms, fax etc.

IE9. Ensure secure messaging (information is digitally signed and/or encrypted) is used for all information classified at C3 or above. Agencies SHALL use Secure Multipurpose Internet Mail Extension (S/MIME), equivalent or better protocol for secure messaging as specified in clause CY7 Guidance on Cryptographic Security [CY].

NIA Manual mandates that all information classified as C3 shall be encrypted and / or digitally signed using Agency approved tools when transmitted through electronic messaging. NIA Manual recommends S/MIME protocol for secure messaging as specified in clause CY6, section C-10 Cryptographic security.

IE10. *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 <Agency'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 <Agency>."

It is not certain whether an email disclaimer will provide immunity against liabilities in a court of law. However, a properly phrased disclaimer will certainly help the Agency's case and in some situations might exempt it from liability. More importantly, it may well prevent the actual occurrence of lawsuits against the Agencies since the mere presence of the statement might deter most persons from seeking legal compensation from Agency.

Therefore NIA Manual recommends the use of disclaimers. The above is a recommended disclaimer that may be used by the Agencies.

IE11. Exercise due diligence to ensure that any information sent/received is free of viruses, trojans and other malicious code

While transmitting information (emails, sharing data) the **Agency** shall exercise due diligence to ensure that the information transmitted is free of viruses, Trojans and other malicious code.

However the recipient is equally responsible and is advised to take utmost precautions to safeguard their Information infrastructure.
NIA Manual recommends appropriate controls to be used at gateways for monitoring, screening and ensuring compliance of data transferred across.

IE12. 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 CY4, section C-10, Guidance on Cryptographic Security [CY]**.**

Agencies should ensure that appropriate security controls are in place to protect the integrity and confidentiality of information exchanged between different systems.

The controls are primarily intended for inter-agency transfers; however it may be extended to intra-agency systems and will definitely enhance the security posture of the Agency.

NIA Manual mandates that all information classified as C2 I2 or above shall be transmitted over authenticated and encrypted data channels. Encryption shall comply with section C-10, Cryptography section.

NIA Manual recommends the use of following controls

a. While transmitting or receiving information secure protocols such as S-FTP, SSH must be used. Unsecure protocols such as Telnet, SNMP v1 and v2 must not be used.
b. Inter **Agencies** connections SHALL be through dedicated independent physical connections or through secured connectivity such as VPN through ISP Cloud. Government Network should be the preferred mode of connectivity.

IE13. *Limit the information provided to the general public (via media outlets), to sanitized and approved information, through a designated and trained media relation spokesperson.

NIA mandates that **Agencies** should have a designated and trained Spokesperson / Media relations team.
The designated spokesperson / media team shall be the single point of contact for disseminating information to audiences / stakeholders external to the Agency. Any information to be disclosed to the media, even if it belongs to the public classification, should only be communicated in consultation with the agency’s Public Relations department and by the designated spokesperson / media team.
The designated spokesperson / media team shall be responsible to ensure that the information released is classified as Public or Internal (Specific case basis when being released to a limited set of authorized persons / media) when the information is released.

4. Guidance on Gateway Security [GS]

4.1. Policy Objective

The main purpose of this policy is to provide minimum security requirement for securing gateways used for inter-agencies 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. Guidance on Policy & Baseline Controls - General

In order to comply with this policy, **Agencies** MUST ensure that:

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

Agencies should ensure that as minimum physical networks are protected from each other using gateways. NIA Manual recommends that gateways are used to protect logical networks within the Agency.

Further Agencies should ensure that the gateways are configured correctly in order that it may be an effective control. More often than less it has been found that gateways are configured with lax rules. This not only creates vulnerabilities within the network but further instils a false level of confidence.

GS 2. Gateways connecting Agency networks to other Agency 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.

Further to the controls mentioned in GS1, NIA Manual mandates that Agencies perform due diligence while choosing the gateway device to ensure that it meets the technical and functional requirements of the Agencies.

Ensure that data flows (rules) are controlled; any data flow change in the gateway should be vetted through the Change Management process. All such changes should be documented and reviewed regularly.

The gateway device should be physically secured.

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

Gateways are specialised security solutions and as such should be managed and maintained by trained staff. NIA Manual mandates that suitable access controls are in place to restrict access to authorized staff and that such staff are suitably trained. This will ensure that the gateway is properly maintained and configured.

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

Further to controls specified in GS3, Agencies should ensure additional level of controls for gateways processing or transmitting information classified at C3 or above.

Administrative and management access shall be provided on dual control and the four eyes principle. This will ensure that it will no longer be possible for a person to singlehandedly compromise the system. It will introduce a check and balance for configurations carried out on the system.

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

Gateways or any other network boxes by itself are mere information assets with no real Confidentiality or Integrity value or requirements. For e.g. a gateway appliance may be configured to connect two homes exchanging personal files or the same gateway appliance may be configured with two government agencies exchanging confidential information. In both the scenarios, the profile of gateway changes based on the information it is processing. As such Gateways shall be classified inline with the information they process or transmit and the security controls shall be chosen accordingly.

Agencies should ensure that information exchanged through gateways is labelled as per the Data Classification policy [IAP-NAT-DCLS] and is secured as per the controls specified in this document.

NIA Manual mandates that wherever possible, Agencies should ensure that the gateways are able to filter and manage the information content so that it complies with the policies.

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

NIA Manual mandates that networks are designed to effectively separate externally accessible systems from uncontrolled public networks and internal networks. It recommends use of firewalls or any other network security capable equipment like routers etc.

The equipment should be configured with suitable data flow / control rules.

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.**

NIA Manual mandates rules for configuring and managing the gateway appliances. The rules are based on the industry recommended best security practises.

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**

Any appliance / server / solution / system by default is configured to maximise functionality and ease of use. However this is general introduces a lot of vulnerabilities in the system which may put a system at risk. However by ensuring proper and needs based configuration of the system, many of the vulnerabilities in the system may be mitigated / eliminated or minimized. This process is generally referred to as Hardening.

NIA Manual mandates that gateways should be hardened prior to any implementation and deployment at any production site. It further provides guidance on key threats that should be considered while securing / hardening the gateway appliance.

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

Agencies should ensure that define procedures exist to ensure that gateway appliances are monitored, alerts logged and action as per Section B-10, Logging and Security Monitoring.

Agencies should ensure that appropriate resources are allocated to monitor the gateway systems. Gateway systems processing or transmitting information classified as C3 and above it should be monitored on a 24x7 basis.

Logs should be analyzed and if possible correlated with other system logs to detect threat patterns, attacks and anomalies in the system.

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.**

NIA Manual mandates that gateways should be able to analyze traffic at application layer. It provides the minimum requirements for content filtering that shall be met by gateways.

It is possible that a single device may not be able to meet this requirement; as such Agencies may employ a combination of devices that may achieve the desired result.

However Agencies should ensure all the devices in the combination adhere to the controls mentioned above.

4.3. Policy & Baseline Controls – Data Export

In order to comply with this policy, **Agencies** MUST ensure that:

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

NIA Manual intends to tie down accountability for data exports performed by Agencies. System users responsible for exporting data to external Agencies should ensure that they comply with the relevant provisions of this NIA policy and manual. They should primarily ensure that information being exported is classified, labelled as per the classification and the necessary controls in place to comply with the C-I-A requirements of the information classification.

GS 12. Data exports are either:

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

b. individually approved by the information security manager.

System user responsible for data exports shall ensure that they adhere to the established process / standards approved by the Agency. Any exception to the established process / procedure shall be explicitly approved and authorized by the Information Security Manager on a specific case to case basis.

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

Agencies should ensure that Information systems handling multiple classifications of information are classified as per the highest level of information processed or stored by them. Systems handling multiple classification of information may connect to other systems in external agencies that may be classified at a lower level.

However Agencies shall ensure that security controls are in place to ensure that information classified as high does not get exported to a less classified system. Systems shall be implement filtering solution which on a minimum will be able action on classification label of the information.

e.g. A system handling information classified up to level of C2 shall be classified as C2. This system shall connect to an external system classified as C1, however controls shall be in place to prevent export of information classified as C2.

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

Agencies should ensure that Content filtering mechanisms are employed at gateways that have the ability to perform keyword searches on textual data that is being exported to external Agencies. Such content filtering system should be able to scan for defined key words, including classification labels.

Any violation shall be quarantined, and will be subject to a review and approval by a trusted source other than the originator.

It should be noted that an automated search engine may not be able to scan encrypted or password protected files. Manual over-ride or sharing of encryption key by automated search engine may provide some help here. However the risks of decrypting and re-encrypting data at the gateway shall be duly assessed.

4.4. Policy & Baseline Controls – Data Import

In order to comply with this policy, **Agencies** MUST ensure that:

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.

NIA Manual intends to tie down accountability for data imports performed by Agencies. System users responsible for importing data in to Agency's systems should ensure that they comply with the relevant provisions of this NIA policy and manual. They should primarily ensure that information being imported is classified, labelled as per the classification and the necessary controls in place to comply with the C-I-A requirements of the information classification.

GS 16. *Data imports are either:

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

b. individually approved by the information security manager.

System user responsible for data imports shall ensure that they adhere to the established process / standards approved by the Agency. Any exception to the established process / procedure shall be explicitly approved and authorized by the Information Security Manager on a specific case to case basis.

GS 17. *Data imported to an Agency system is scanned for malicious and active content.

Agencies should ensure that controls are in place to scan data imported in to its systems for malicious contents.

5. Guidance on Product Security [PR]

5.1. Policy Objective

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

5.2. Guidance on Policy & Baseline Controls

In order to comply with this policy, **Agencies** MUST ensure that:

PR 1. The process for product selection is carried out with due diligence and ensures product and vendor independence.

Agencies should ensure that the process for procurement of IT services, solutions is fair and independent of product and / or vendor influences. Agencies shall invite sufficient number of proposals and each shall be duly evaluated. Assessment process should include relevant technical assessments relevant to ensure that the product meets its requirements.

PR 2. Products are classified and labeled as per National Data Classification policy [IAP-NAT-DCLS].

All products procured or built shall be labeled in accordance to the National Data Classification policy [IAP-NAT-DCLS]. Information system hardware shall be classified based on the information they process or store.

It may be prudent on the part of Agency to embark on a classification analysis during the analysis and design stage to evaluate the possible classification for the products procured / to be procured and / or built.

By giving thought to the possible classification during the analysis / design / procurement stage may influence the choice of vendors and the product itself.

E.g. You may not want to buy a product that may possibly be classified as “C3” from a vendor that does not have a very positive track record.

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

Agencies shall define a procedure for procurement of IT related goods and services. The procurement process shall on a minimum include identification and screening of vendors. An evaluation criterion shall be defined which on a minimum shall include

a. Vendor status and identification, including location and ownership: The process shall ensure due diligence in identifying the vendor. While considering solutions for national security or in the interests of safeguarding national integrity it may be prudent to ensure that the vendor or the product does not originate from an enemy country or a country with strained relations etc. It may be imperative that in certain sectors or for certain critical infrastructures the vendor or the solution is local or has a local partnership (local partner having a majority) to ensure proper support, provide legal cover and minimize the threat of misuse of foreign power. Further it should be ensured that there is no over reliance on a single vendor / product etc.

b. Financial situation: Agencies shall ensure due diligence in assessing the financial capabilities of the prospective vendor. Fly by Night operators present a risk to the organization jeopardizing the investments and the faith in the integrity of the systems. Further additional care should be taken while procuring solutions / services from young companies that may not survive long term or risk being overtaken from competitive forces.

c. References from previous successful engagements: Agencies should ensure that vendors provide references from previous successful engagements. References provided by the vendors shall be vetted by the Agency. Based on this references, Agencies should assess the capabilities of the vendor in terms of their strength to deliver the project / solution, product strength and capabilities, etc

d. The vendor must have in place a proper risk managed control environment. Doing business with vendors who do not have such controls will put the Agency data and processes at risk. The reliance on vendor provided 3rd party audit reports and right to audit clauses must be present. If 3rd party audit reports on the vendor are not available then relative assurance must be obtained by the Agency on the existence and effectiveness of those controls.

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

Agencies should ensure that procedures are defined to ensure that Acceptance Tests are part of the project closure process. Acceptance Tests should be comprehensive and ensure that it includes the following:

a. The solution meets the technical and functional requirements specified by the Agencies. Requirements may have been specified in the RFP / RFQ document, post contract agreed design documents etc.

b. The solution conforms to the claims made by the vendor during or after the bidding (procurement) phase.

c. The solution conforms to the claims made by way of standard documentation available with the system e.g. brochures etc.

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.

Agencies should ensure that new products are evaluated on a dedicated test bed. This shall ensure that the testing and evaluation of the product does not introduce any risks to the production environment.

Further, such tests shall also include functionality tests, security tests and hardening of the product by applying appropriate patches and fine tuning of configuration. This will ensure that the product performs as expected in the desired configuration reducing the risks introduced by performing tests in default configurations.

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

Agencies should ensure that its defined processes and procedures imbibe information security principles / practices. It should ensure that all products delivered adhere to this secure delivery methodology.

Vendors should ensure that the products delivered adhere to the Agency's recommended information security standards (e.g. NIA policies). All processes within service delivery adhere to the recommended information security best practices. This includes for e.g. defined SLA's, adequate documentation, implementation of agreed security controls etc.

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

Further to PR 6, Agencies shall ensure that delivery procedures include measures to detect tampering or masquerading of products, such as checking for product seals etc

This shall assist the Agencies in detecting physical products that are spurious, re-furbished or physically tampered to allow snooping by malicious users. Further controls such as code reviews shall assist Agencies in detection of malicious code in the software.

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

Further to PR1 and PR3, Agencies should ensure that they choose vendors / developers who have shown long term commitment and a will to maintain and develop their products.

Generally it is advisable to stick with core products / business of any developer. For e.g. Intel is the world leading producer for microprocessors. However if tomorrow Intel starts selling Personal computers or servers, it may not necessarily be a good idea to buy PC's and servers from them as it does not form their core business.

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, Guidance on Change Management [CM]**.**

Agencies should ensure that all products procured are updated and patched regularly as defined by the Agency's security policy. All updates / upgrades shall be performed after a due risk assessment and in line with the change management policies specified in section B-5, Change Management.

6. Guidance on Software Security [SS]

6.1. Policy Objective

6.2. Guidance on Policy & Baseline Controls – Software Development & Acquisition

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.

Software applications (Operating System, Applications, Database etc) are the life and soul of any information system. The most powerful hardware is of no worthwhile use without an appropriate Operating system, and associated application to unleash its power.

However it should be noted that the appropriateness of the software (Operating System, Applications etc) is not only in its ability to provide a variety of workable solutions but also in complementing it with a secure environment.

Agencies should ensure that security is considered in all phases of the SDLC. A software development life cycle (SDLC) consists of the following phases

a. Initiation

b. Acquisition / Development

c. Implementation

d. Operation / Maintenance

e. Disposal

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

Based on the **National Information Classification Policy**, **Agencies** shall conduct sensitivity assessment (information, potential damage, laws and regulations, threats, environmental concerns, security characteristics etc) to ascertain the confidentiality, integrity and availability ratings.
Further, the Agencies shall perform preliminary Risk Assessment to ascertain the threat environment in which the system will operate.
The results of this risk assessment exercise shall be incorporated into the decision-making process regarding the development/acquisition of the system.

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

Based on the results of the Risk Assessment exercise, Agencies shall analyze the security (functional, technical and assurance requirements) requirements of the applications and devise controls to mitigate the risk. The controls shall be an inherent part of the system design and implementation.

Agencies should ensure that the following requirements are captured in the design phase and thereafter implemented in the system

1. Data backup strategies: Requirements include frequency of data backup, details of backup media, access privileges to the backup and whether the backup be encrypted.

These requirements shall provide inputs while sizing the storage requirements for the system. Further it shall ensure that the C-I-A requirements of the information are met.

2. Data transmission strategies: Depending on the classification of information / system, an appropriate transmission / exchange method shall be chosen. Agencies should consider requirements such as encryption of data in transit, end-end encryption, any other security controls etc
3. Data storage security requirements: Security requirements for data at rest (storage) shall be governed by the classification of the data. Data required for authentication should be given more thought, such as applying one-way encryption.
4. Authentication strategy: Agencies should ensure that appropriate Authentication strategy based on the classification of the system is implemented as this is the entry point of the system.
   Some of the things that may be considered are strong password policy, two-factor authentication for critical applications, input validation strategies, account inactivity period, account locking, password retrieval mechanism, and a username/password storage strategy.
5. Identify trust boundaries, trust levels, entitlements, encryption requirements: Agencies shall analyze and identify trust levels and trust boundaries in the overall context of how the information flows within the system and how the information flows in the infrastructure including connectivity to external systems (both inter and intra agency). The requirements will provide a broad security requirement in the overall context.
   Agencies shall consider extra security controls where trust level is low. Data classification shall help in determining encryption requirements. Encryption details such as encryption algorithm, hashing algorithm, and key length should be identified and documented in the design document. Similarly, access requirements should be identified. The design document should identify entities and resources. It should map the level of access between an entity and the resources in the system.
6. Design audit logs: Agencies should identify the log requirements for effective monitoring, administration and troubleshooting of the system. The log retention and management strategy should be agreed upon. System designers should ensure that audit log assist not only in identifying system errors but also in co-relating various other logs to identify system compromise patterns and / or attacks.
7. Prepare and implement infrastructure security best practices (System Hardening) document addressing operating system, Web server, application server, database, FTP, e-mail: This document will help strengthen the security of the infrastructure and SHOULD be prepared during the design phase.

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.**

Agencies should ensure that dedicated test and development infrastructure is available, separate from the production systems. This is to ensure that the production does not suffer from any breaches or outages due to development work being carried out. Agencies should further ensure that the information data is protected and that live production data is not used for development work. Developers should develop their own test data to prevent any information leakage.

Agencies shall define policies and procedures to regulate and secure the development process. Controls shall be defined to control flow of information between the development, test and production systems. Access to the systems will be controlled on a Need to know or a Need to have basis.

Additional access controls including logging and auditing shall be enabled to ensure protection of the authoritative source of the software. Procedures shall be defined to govern software revision management including deployment.

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.

Agencies shall ensure that all applications (acquired and / or developed) conform to defined acceptance criterion. Such Acceptance criterion shall include conformance to appropriate quality and security assurance tests.

Agencies should define procedures to ensure that no application be deployed in production unless, it has passed the appropriate quality and security assurance tests.

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.

Agencies should ensure that its developers are trained to use secure programming practices when writing code. The NIA Manual provides guidance on some of the factors that shall be considered to ensure that programming style reflects secure coding style.

As part of security best practices secure coding guidelines such as OWASP guidelines, should be adhered to.

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.

The NIA Manual mandates that the software (acquired and / or developed) is tested for vulnerabilities before it is used in a production environment.

The following mechanisms may be used to analyze the security strength of the software; however it is recommended that such tests / audits are carried out by a third party or an independent quality assurance department within the organization.

1. Code review for secure coding guidelines: Code review helps in identifying bugs and / or bad coding practices. This can help in mitigating the vulnerabilities in the code that can be exploited by attackers.
   There are some automated tools available in the market to do a security code review.
2. Vulnerability assessment/pen testing/ethical hack: Such tests help in identifying the security vulnerabilities in an application in the overall context of its infrastructure.
   Companies can leverage this testing to strengthen their application and the associated infrastructure.
3. Encryption testing: There is no point using encryption if it is not secure enough. With tools such as rainbow tables, it is becoming relatively easier to break

encryption. Hence, the companies should test for the strength of the encryption being used. Secure key management is equally important

4. Applications should also be tested by specialized applications security testing technologies such as SAST (static application security testing), DAST (dynamic application security testing), and IAST (Interactive application security testing). (SAST technology is recommended for testing Source/byte/binary code of all Acquired applications/packaged applications or packages developed by 3rd party provides)Web application developed by 3rd parties should be tested in runtime environment (DAST technology is recommended for testing).

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

Agencies should ensure that all system (acquired and / or developed) complies with all legal requirements like licensing, copyrights, IPR etc.

All software and hardware shall be licensed throughout its life cycle. Agencies shall ensure that they abide with the license requirements of the software / hardware at all times. Agencies should ensure that Intellectual Property Rights are not violated.

Agencies shall ensure that they comply with all the legal (laws and regulation) requirements that exist at the time and further commit to abide to legal regulations that may be formulated in future.

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

Documentation forms a key process in any system. Agencies should ensure that all software / system (acquired and / or developed) are documented in an adequate manner. Documentation shall include the following:

1. Requirements Document: Requirements documentation is the description of what particular software does or shall fulfil. It is used throughout development to communicate what the software does or shall do. It is also used as an agreement or as the foundation for agreement on what the software shall do.

   This document will capture the initial design requirements for the system / application acquired and / or developed. Example: RFP / RFQ or any other similar document.

2. Architecture / Design Document: Architecture documentation is a high level design document. In a way, architecture documents are third derivatives from the code (design document being second derivative, and code documents being first). The architecture documents do not contain anything specific to the code itself. These documents do not describe how to program a particular routine, or even why that particular routine exists in the form that it does, but instead merely lays out the general requirements that would motivate the existence of such a routine. It may suggest approaches for lower level design.

   Design Document is a detailed low level document that contains Conceptual, Logical, and Physical Design Elements. It details the relationships and data flows between various entities. It identifies and documents the strategies how the system will implement and conform to identified requirements.

3. Technical Documentation: When creating software, code alone is insufficient. There must be some text along with it to describe various aspects of its intended operation. This documentation which includes How-to and overview documentation specific to the software application or software product being documented may be used by developers, testers and also the end customers or clients using this software application. Technical documentation has become important as more and more critical processes are automated and the related basic and advanced level of information may change over a period of time with architecture changes.

4. Functional / User Documentation: User documentation describes each feature of the program, and assists the user in realizing these features. A good user

document can also go so far as to provide thorough troubleshooting assistance. It is very important for user documents to not be confusing, and for them to be up to date. User documents need not be organized in any particular way, but it is very important for them to have a thorough index. Consistency and simplicity are also very valuable.

5. Acceptance Test Reports: The final step in completion of software acquisition / development is testing the software to ensure its functionality and compliance with the agreed design, standards etc. Agencies may conduct different kinds of tests to ensure to ensure final acceptance. These tests could include User Acceptance tests to ensure functionality, code reviews, penetration tests to test security compliance, an audit to ensure compliance with NIA policies etc. All such reports shall be documented and action items highlighted in the reports shall be worked upon.
6. Threats and vulnerability document: This document shall identify and document any existing threats or vulnerabilities in the system at the time of deploying it in a production environment. The document shall be signed off by the business process owner.

SS 10. *Source code of custom developed critical applications is available and in the case of commercial applications (Serving critical applications / processes) an Agency SHOULD look into options of arranging an escrow for the source code.

Agencies should ensure that source code of critical custom built applications developed in-house or through third party is available for code reviews and is secured adequately to protect its confidentiality, integrity and availability.

In case of ready to use commercial software (customized according to requirements) for critical applications and processes, Agencies should look into options of arranging an escrow for the source code. An escrow arrangement is an agreement between the Agency and the Software developer, wherein the developer agrees to place the most updated source code of the software with a third party who will act as a trustee.

In the worst case scenario of the software developer being not in a position to maintain the software due to reasons such as bankruptcy, mergers / acquisitions by another company, change of roadmap etc, the Agency shall have a right to acquire the source code from the trustee, so that it can continue to maintain its critical application.

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

Agencies should ensure that all new software application is accredited prior to commissioning as production software. However, Agencies may postpone the accreditation to ensure it is in line with its roadmap subject to the authorization by the Head of the Agency / Head of Internal Audit. They shall also notify the Certification Body on the same.

6.3. Policy & Baseline Controls – Software Applications

In order to comply with this policy, **Agencies** MUST ensure:

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

Agencies should ensure that information system (servers, workstation and associated hardware) are classified and relevant security controls identified and documented. All such hardware shall be hardened as per their classification and as per agreed security controls mentioned 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.

NIA Manual mandates baseline controls that shall be considered while hardening the standard operating environment.

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.

NIA Manual mandates baseline controls that shall be considered to ensure mitigation of vulnerabilities in the system. Such controls shall be imbibed in SOEs deployed in the Agencies to achieve a minimum baseline of security protection.

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.

NIA Manual mandates that servers running critical services and / or essentially being in high risk zones (e.g. Web, Email servers in DMZ) have additional security controls in place to mitigate the risks of compromising other servers when it is compromised itself.

SS 16. Check the integrity of all servers whose functions are critical to the Agency, 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

NIA Manual mandates that controls shall be implemented to monitor the integrity of servers providing functionality which are critical to the agency and or servers that may be at high risk of compromise.

It is recommended that such checks be performed from a trusted environment preferably a secure zone which is at a similar or higher level of security than the servers whose integrity is being monitored. It is recommended that monitoring is centrally managed to ensure effective audit and monitoring rather than independent agents installed on each server.

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

Further to SS16, NIA Manual mandates that integrity information (e.g. HASH codes etc) shall be stored securely off the server. It is recommended that the integrity information be stored in the management server which resides in a secure and trusted environment. Integrity information shall be classified as I3 and shall be secured accordingly.

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

Further to SS16 and SS17, Information Security Managers should ensure that for an effective integrity check and monitoring the integrity information is updated at all times.

ISM's should ensure that as part of the CM5 in Section B, Change Management the updated system documentation includes updating of integrity information. This will eliminate the generation of false positives when a system has undergone a legitimate change.

SS 19. *As part of the Agency'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

Further to SS17, NIA Manual mandates that Agency's audit schedule shall include within its scope, server integrity checks.

The Auditor shall compare the current integrity information against the stored integrity information to determine whether a compromise or a legitimate but incorrectly completed system modification has occurred.

The checks shall be held at regular interval in order that the integrity checks may aid as an effective security control and tool.

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

The detection of a change, signals a high probability of system compromise. Agencies should ensure that any such change detection is dealt according to its Incident Management procedure.

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

As part of code review and vulnerability tests, Information Security Managers shall analyze the behaviour of the application. ISM's should review the information flow design of the application, the various components in an infrastructure that it establishes connection with and the type of connection it makes.

ISM's should ensure that the final product complies with the design document. They shall ensure that the connections made by the applications are in line with the controls specified for its classification. E.g. use of secured channels for information classified as C3.

Further they shall ensure that the communication ports used by the application are in line with the Agency's network policy.

ISM's shall perform a Risk Assessment to assess the threats and risks on allowing such connections and this shall form the basis for the business process owners to validate or invalidate this connection.

6.4. Policy & Baseline Controls – Web Applications

In order to comply with this policy, **Agencies** MUST ensure:

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

Web based applications are largely preferred by developers as it allows the usage of thin client. It makes it easier to deploy applications on a large number of users, without having the encumbrance of installing clients on each computer. It allows the flexibility to have a uniform front end and the liberty to have diverse back end processing systems.

However this ease introduces a lot of security concerns. Years of research have proved numerous vulnerabilities in web servers, its protocols and consequently its applications.

NIA Manual mandates that Agencies ensure due diligence in screening and reviewing the active contents on the web servers. NIA Manual mandates that Agencies adhere to secure programming practises. It recommends the use of OWASP guide to build secure Web applications and Web services.

Applications should also be tested by specialized applications security testing technologies such DAST (dynamic application security testing), and IAST (Interactive application security testing).

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

NIA Manual mandates that connectivity and access between each web application components and various stake holders is minimized to a “Need to Have” basis. This shall minimize the threats related to open connections.

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

NIA Manual mandates that Agencies adopt sufficient controls to secure personal information and sensitive data collected through web portals. The data should be secured during transmission and whilst in storage.

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.

NIA Manual mandates that Critical Sector portals that need strong authentication use SSL certificates provided from a Certificate Service Provider licensed in the State of Qatar.

SS 26. Web application firewall (WAF) MUST be used for applications with MEDIUM or higher risk rating.

Web applications with Medium or High ratings must be protected using a Web Application Firewall (WAF). WAF prevents many of the application vulnerabilities from reaching the application. It should be noted that network firewalls do not have these functionality. (WAF operates at the Application layer of the OSI model while network firewalls work at the Transport layer and Network layer).

6.5. Policy & Baseline Controls – Databases

In order to comply with this policy, **Agencies** MUST ensure:

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.

Agencies should ensure that all information within the database is classified and labelled in an appropriate manner especially if the data can be exported to another system or contains information of multiple classifications.

SS 28. Agencies 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.

Further to SS27, NIA Manual mandates that within a database classification is applied at a granular level. It should be sufficient enough to identify handling requirements for any information retrieved or exported from the database.

This is especially true for large databases (RDBMS, ERP etc) where large amount of information is stored and co-related with each other. Not all information has the same C-I-A classification ratings. It is essential that the information is classified in a pragmatic way at granular levels to ensure suitable security controls.

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

Agencies should ensure adequate security for the databases. In general a database will have its own access controls, Agencies should ensure that it is not possible to bypass this controls.

This shall be provided by preventing access to database file using operating system (kernel) functions. Access to databases shall be audited and the logs reviewed at regular intervals.

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

NIA Manual mandates that databases shall support detailed auditing facilities. It shall be possible to audit system user's action. This includes administrative functions such as database creation, deletion, table modifications, user rights modification etc.

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, agencies MUST ensure that all query results are appropriately sanitized to meet the minimum-security privilege of system users.

Agencies should ensure that manipulation of information classification and access controls shall not be possible in the database system.

As a thumb rule, access to information in a database shall be governed by "Need to Know" or a "Need to Have" basis. In case where a database contains information classified at different levels, data shall be classified at granular levels and access to information shall be controlled at a granular level.

This shall ensure that users do not get access to information that they are not authorized to view.

However it may be possible to bypass these controls through the use of search routines, cache engines etc as this process may be executed through different privilege level. Agencies should ensure that controls are in place to prevent this misuse especially by system users.

Agencies should further ensure that Database administrators have sufficient rights to carry out their responsibilities, whilst at the same time ensuring restriction at the meta-data level.

Sensitive database i.e. containing classified data level C3 and above will be subject to specific care. Admin privileges must be subjected to password splits and 4-eyes principle.

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

For database that carry information classified at C3 & above must mask the data using data masking technology so as to prevent administrators from access/retrieving it.

7. Guidance on System Usage Security [SU]

7.1. Policy Objective

7.2. Guidance on Policy & Baseline Controls

In order to comply with this policy, **Agencies** MUST ensure that:

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 / Agency's Acceptable usage policy.

NIA Manual mandates that system users shall be responsible for the information assets (systems / infrastructure) along with the necessary access provided to them to carry out their official responsibilities. They must perform due diligence to ensure that they do not become a direct or indirect reason for the failure or compromise of the system. They must endeavor to handle the assets with due care and operate them according to defined guidelines / acceptable usage policies.

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

System users shall be made aware that the resources provided by the Agency including access to internet are for business use. Personal usage may be permitted but shall be governed by policies of the Agency.

Agencies on their part shall define policies and guidelines on Acceptable usage of web and its resources in line with their business requirements. Based on a Risk Assessment exercise, Agencies shall decide on the appropriateness of the usage of various web based functionalities such as web based email, chat, social networks etc

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.

Agencies should ensure that security controls are in place to protect ICT assets against web based threats.

NIA Manual recommends that the risk can be mitigated by ensuring controls that prevent downloading of programs from web; active content and non-business related web sites. It has been found that sites related to social networking, free downloads, music, torrents are the biggest source for spreading malicious contents.

Agencies will implement the above recommendations in line with the controls specified in SU1 above.

SU 4. Web access is provided through secure proxies and filtering gateways as defined in section -C4, Guidance on Gateway Security [GS]**.**

NIA Manual mandates that Web access is provided through secure proxies and filtering gateways as defined in Section B-4, Gateway Security. This shall ensure that the Agency's web access policy is centrally managed and effectively monitored and controlled.

SU 5. *Staff are aware of the types of content permitted and restricted within the Agency, as specified in section B-4**, Guidance on** Gateway Security [GS]**.**

Agencies SHOULD consider an effective solution for monitoring content of encrypted channels.

Agencies shall ensure that the staff is educated on the acceptable usage of web resources provided to them. Agencies shall ensure that the Security Awareness courses conducted by them highlight on the effective usage of web and its resources.

Further the access of web resources shall be monitored to ensure compliance of web policy by the staff. Agencies should consider an effective solution for monitoring of encrypted / secure web sites. A thorough Risk Assessment shall be done to weigh the pros and cons and the effectiveness of such a solution.

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

Agencies should educate their staff on acceptable usage of email services. Staff on their part should ensure due diligence while using email services provided for business needs. Personal usage may be permitted in line with the Agency's acceptable usage policy.

Agencies should consider restriction on use of official email ids in public forums and non- work related web sites

Staff shall ensure that the emails are suitably classified and labeled based on the contents / attachments in the email.

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

NIA Manual mandates that Agencies implement adequate security controls to protect email against potential threats such as viruses, trojan's, spam emails, forgery etc.

Agencies should ensure that its security awareness courses provide awareness to its staff about the potential threats against email services.

NIA Manual recommends use of email gateways to filter and manage the email and its contents.

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

Agencies should ensure that the use of web based email and / or any other non-agency related email services is prohibited. Such email services introduce a backdoor in to the system which cannot be effectively monitored and may eventually be used as a channel for information pilferage.

Agency's shall ensure this through their Acceptable usage policy. Staff should be provided awareness on this through effective security awareness courses.

Further Agencies should look into effective technical controls that shall assist in enforcing this policy.

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

NIA Manual provides guidelines to prevent confidential emails being sent to wrong addressees in error. It may be possible that a defined Distribution list (personal or agency's) may contain recipients to whom the email is not intended, as such it is a best practice that confidential emails be sent to only named individuals.

Agencies through their Security awareness programs shall communicate this to the users.

SU 10. Staff are 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 Agency's systems.

NIA Manual provides guidelines to prevent leakage of confidential emails by the use of automatic forwarding.

Automated forwarding within the Agency may be permitted as in the case of a secretary handling the boss's email. However a certain amount of caution is advisable when the emails are forwarded to temporary replacements or colleagues who are in acting position during period of absence.

Emails classified at C2 and above shall not be automatically forwarded to an email address external to Agency. The user shall ensure that sufficient security controls and authorizations (permission to use personal accounts by concerned business process owner / ISM) are in place before forwarding an email classified as C2 or above outside the Agency's email system.

Agencies through their Security awareness programs shall communicate this to the users.

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

NIA Manual provides guidelines to ensure that relevant security controls and information handling procedures are in place at the external party. NIA Manual recommends that relevant Non Declaration and Confidentiality agreements are in place with the external parties and the necessary risk assessment has been done before exchanging data with external parties.

8. Guidance on Media Security [MS]

8.1. Policy Objectives

8.2. Guidance on Policy & Baseline Controls - Media Classification and Labelling

In order to comply with this policy, **Agencies** MUST ensure:

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

Hardware or media in general has no value; it derives its value from the information stored in it. A media containing key financial plans and forecasts of a company is of much value and critical than a similar media containing copies of games.

Agencies should ensure that they classify the media at or above the classification of the information it contains or may contain. This is to ensure that adequate controls are allocated to secure the media.

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

Further to MS1, if a media contains information classified at multiple levels, the media should be classified at the highest level.

E.g. A USB drive may contain three documents. The first document could be classified as C1, the second as C2 and the third as C0. In this scenario, the effective classification of the media (USB Drive) will be C2; which is the highest classification of the 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.

Further to MS1 and MS2, NIA Manual intends to clarify that in case of volatile media, the media may lose its classification after the loss of power, as it will no longer retain any information.

Volatile media in a non-powered state should be treated as C1 classification.

E.g. Assume a laptop that is used to store and process information classified as C2. This laptop primarily contains two media types; Random Access Memory (RAM) which is volatile and Hard disks which is Non Volatile.

As long the laptop is witched ON, the Hard disk and the RAM will be classified as C2 ratings. Once the laptop is switched OFF, the HDD will retain its C2 ratings while the RAM will be de-classified as C1.

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**

Agencies should define procedures to ensure that media classification is maintained up to date. Users shall be educated on the importance and procedure for classifying the information and associated media.

NIA Manual mandates guidelines that shall be used to determine if the media needs to be reclassified.

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**

Agencies should define procedures to ensure that media classification is maintained up to date. They shall ensure that the procedures are adhered to upon increase or decrease of classification as well.

Although from a security stand point, maintaining a higher media classification may not entail security vulnerability, but it may entail higher costs of maintenance.

Users shall be educated on the importance and procedure for de-classifying the information and associated media.

NIA Manual mandates guidelines that shall be used to determine if the media needs to be declassified.

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

Agencies must ensure that storage media containing classified information is sanitized in line with section C8.3 Policy and Baseline Controls – Media Sanitization, before it is declassified. If the information cannot be sanitized, then the media must be destroyed lest it leads to information leakage.

MS 7. *The classification of all media is readily visually identifiable. Agencies SHOULD achieve this by labelling media with a protective marking that states the maximum classification as specified in section B-4, Data Labelling [DL]

NIA Manual mandates that the classification of media is readily and visually identifiable. Agencies should define procedures and identify controls that ensure that media is suitably labelled as per the classification.

The label should identify the maximum classification and be protected against tampering.

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

NIA Manual endorses the use of non-textual representations of classification markings (e.g. barcodes) to enhance the security, however Agencies shall ensure that the labelling scheme is documented and uniformly applied across the organization and further that the staff is trained to use them effectively.

8.3. Policy & Baseline Controls - Media Sanitization

In order to comply with this policy, **Agencies** MUST ensure:

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

Agencies should define procedures for sanitisation of media. They shall identify and adopt appropriate tools to meet the Agency's media sanitization requirements subject to they being successfully tested.

Such tests shall be conducted at regular interval to ensure effectiveness of the tool.

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

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.

NIA Manual mandates that non-volatile memory that cannot be sanitized shall be destroyed prior to disposal. It provides examples on these media types. All such and similar media that may contain information classified at C1 or above shall be destroyed prior to disposal.

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.

NIA Manual intends to provide guidelines on sanitizing volatile media.

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

a. overwriting the media, if pre-2001 or under 15GB, in its entirety, with an arbitrary pattern followed by a read back for verification three times

b. overwriting the media, if post-2001 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)

NIA Manual intends to provide guidelines on sanitizing non-volatile media.

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 pseudo random pattern. Sanitization of media with rating C3 & above SHOULD be documented.

NIA Manual intends to provide specific guidelines on sanitizing non-volatile EPROM media.

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.

NIA Manual intends to provide specific guidelines on sanitizing Flash memory media.

8.4. Policy & Baseline Controls - Media Repairing and Maintenance

In order to comply with this policy, **Agencies** MUST ensure:

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

Agencies should ensure that only authorized persons carry out repairs and maintenance work on classified hardware. The authorized staff (staff and / or contractors) shall comply with the necessary controls specified in Section B6. Such authorized staff shall be briefed on the relevant security procedures, policies and guidelines of the Agency.

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

Agencies should ensure that repairs on system containing classified information rated C3 or above are carried out under supervision. Although the manual does not specify specific type of supervision, automated (for e.g. under camera and access control) methods may be used, however when such works are carried out at an off-site it shall be strictly under human supervision.

This is to mitigate the risk of tampering with the intent of stealing or destroying the integrity of information and pilferage of information

8.5. Policy & Baseline Controls - Media Destruction & Disposal

In order to comply with this policy, **Agencies** MUST ensure:

MS 17. They document procedures for the destruction and disposal of media.

Agencies shall document procedures for destruction and disposal of media. The procedure shall be in line with the controls specified in this National Information Assurance Manual.

MS 18. *Media is destroyed by:

a. Deguassing non-volatile magnetic media

b. breaking up the media

c. heating the media until it has either burnt to ash or melted.

The NIA Manual provides guidelines on how the media is to be destroyed. When breaking the media it should be done such that it may not be possible to reconstruct or repair the media. Non-volatile media should be degaussed.

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.

NIA Manual provides guidelines to ensure that the procedures for destruction of media are successfully carried out and documented, especially for media classified at C3 and above. Agencies should ensure that due diligence is carried out in destruction of data.

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

NIA Manual mandates that as an added security control, all media including faulty, shall be sanitised prior to disposal.

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

NIA Manual intends to adhere to the principle of security by obscurity in ensuring that the facilities and processes for disposal of media and media waste do not attract undue attention. This may lead to attempts by malicious users to go dumpster diving in their bid to pilfer information or their controls.

9. Guidance on Access Control Security [AM]

9.1. Policy Objective

9.2. Guidance on Policy & Baseline Controls - General

In order to comply with this policy, **Agencies** MUST ensure:

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.

Least Privilege is a basic principle in information security which advocates that entities (people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions.

For example, the restrictive "need-to-know" approach defines zero access by default and then opens security as required. All data in a corporate network would be off-limits except to specific people or groups that need to access this data for the purpose of their official business.

Agencies should ensure that users are provided access based on the concept of "Least Privilege" and governed by "Need to Know" and a "Need to Have" basis. This will ensure that the entity is able to carry out his designated work without causing an incident unless it intends to go against the defined policies.

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. This request for access SHALL be authorized by a staff member's supervisor or manager.

NIA Manual mandates that the choice of Access controls shall be governed by the sensitivity of the information it controls. Agencies shall identify suitable controls to identify and authenticate the user and audit the access trail.

User identity and Authentication is based on the following:

Knowledge Factor: What a user knows? Password / Pin

Ownership Factor: What a user has? Security tokens / Access Cards

Inheritance Factor: What a user is or has? Biometrics

Based on the sensitiveness of the system the system owners may implement a multiple factor authentication scheme. For e.g. An ATM card (Ownership factor) and a PIN (Knowledge factor)

Agencies should ensure that an effective Audit trailing is established to identify misuse and / or compromise of Access Control systems and to further identify perpetrators in case of an incident.

Further all requests for user access (creation / deletion / modification) shall be authorized by the staff member's supervisor or manager. This shall ensure that controls are in place to protect system against the threat of dummy user creation or self elevation of user privileges.

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

NIA Manual intends to elaborate on assignment of Access rights, further to the basic principles mentioned in AM1.

NIA Manual puts the onus of defining the rules of access rights effectively to the owner of the information. The information owner shall further define this based on the business requirements.

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,

NIA Manual mandates a tight integration between the Agency's processes. Agencies should ensure that a process exists to facilitate information flow between HR and IT / Operations department.

Since HR is involved in the process of hiring, promotion / demotion or termination of an employee's services, they should ensure that the information is relayed on to IT / Operations department who may ensure that the Access control system within the Agency is effectively updated to reflect the changes. Agencies should ensure that this control is extended to Physical Security as well, since in many organizations Access Control for Physical Security is effectively disassociated from IT / Operations department.

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

NIA Manual mandates that effective controls are in place to mitigate bypass / compromise of the access control system to gain access to information. System Administrators are effectively in positions that may provide them unfettered access to the information system. Suitable controls including audit trails, rotation of job duties and regular audit by an independent entity shall be implemented to put checks in place to avoid such misuse.

However, there may be situations, where the system administrators may require such access to investigate incidents, troubleshoot issues etc. System Administrators can utilize such privileges albeit with the formal authorization from the Security Manager. The Security Manager on his part shall ensure that the circumvention of access control is effectively used only for the intended activity and for the intended time. Such activity shall be duly logged.

AM 6. *Any unauthorized effort to circumvent the Agency'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.

NIA Manual mandates that any attempts to circumvent the Agency's access control system, shall be perceived as a Security Incident. Any such successful / un-successful attempts should be dealt as per the established Incident handling procedures and / or appropriate HR policies and procedures.

The incident shall be handled in accordance with the Agency's defined Incident Management / HR disciplinary process.

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.

Agencies shall ensure that auditing is enabled on its Access Control System and is configured in an appropriate manner. The audit logs shall assist in monitoring compliance to the Agency's security policies and procedures. The audit logs shall further assist in investigation of security incidents.

The audit logs shall comply with controls prescribed in Section B10, Logging and Security Monitoring requirements.

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

NIA Manual mandates that Agencies deploy additional controls to ensure security of its information assets. Further to identifying and authenticating the user, controls shall be in place to ensure that the authenticated user does not introduce vulnerability in the system by way of the system that it uses.

For e.g. a user working remotely may connect his home PC infected with a virus to the Agency's network and thereby causing the virus to infiltrate and infect the Agency's networks,

Further controls shall be in place to ensure the user authenticated by the system is also authorized to carry out the intended work. There is a fine line between authentication and authorization.

For e.g. A user may have valid credentials to access a system, but he may not be authorized to access all the information existing on that system.

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.

Agencies should ensure that proper records with regards to the Access control system are maintained. NIA Manual provides guidance on some of the mandatory records that should be maintained to assist in an effective audit exercise, Investigation of an incident etc.

NIA Manual also mandates the life of the records to be maintained, essentially tying up with the system life.

AM 10. *Wherever possible 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. the 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

Agencies should where possible ensure effective use of resources and tools to educate the user on his security responsibilities and to deter potential intruders.

Agencies should implement banners that proclaim, access is only permitted to authorized users, the user has to abide the relevant security policies, the system is monitored, defines acceptable usage of the system and spells out legal ramifications against misuse of the system (the banner can be in visual or auditory formats).

Agencies should further ensure (if possible) to obtain the users acknowledgement of the banner and his acceptance to abide by its terms prior to providing access to the system.

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

Centralised authentication repositories such as LDAP etc are prime and soft targets for malicious users. Compromise of such systems may aid a malicious user to infiltrate the system without raising red flags. Moreover a Denial of System attack may render all the integrated services inaccessible to all users.

Agencies should ensure that such systems are effectively protected against threats of DoS attacks. Communication between involved entities shall be through secure and authenticated channels e.g. encrypted channels.

Agencies shall ensure that key activities (at a minimum those mentioned above) are logged. These log events shall assist in investigation of security incidents.

9.3. Guidance on Policy & Baseline Controls – Identification & Authentication

In order to comply with this policy, **Agencies** MUST ensure:

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

a. identification

b. authentication

c. authorisation

Agencies shall define relevant policies and procedures in line with the National Information Classification Policy [IAP-NAT-DCLS] and the National Information Assurance Manual. The policies and procedures shall cover the domains of identification, authentication and authorization.

The Policies shall be based on the concept of least privilege and governed by the principles of "Need to know" and "Need to have" basis as discussed in AM1.

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

Agencies should ensure that system users are educated about the Agency's policies and procedures.

Induction training provided to new employees shall include awareness on the Access Management policies and procedures. Regular security awareness courses shall be conducted and shall include awareness regarding Access Management.

AM 14. All system users are:

a. uniquely identifiable

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

Individual accountability is essential for IT systems security. **Agencies** must not authorize the creation of accounts that can be used anonymously or by more than one person. A guest account enables anonymous access to an IT system, while a shared account (or shared password) hides individual accountability within a group. Both types of accounts, and the sharing of passwords or other logical access methods, are prohibited.

Agencies should ensure that all employees, contractors, consultants and temporary staff must use Unique User IDs and passwords to gain authorized access to any of the **Agency's** information assets.

The Unique User IDs shall not be shared with other users for the purpose of gaining access to the Agency's information assets.

Authorized users shall be held accountable and responsible for the use and activity of assigned Unique User ID.

Further controls shall be implemented to ensure that user credentials are not cached. Users shall be authenticated on each occasion that access is granted. However Agencies may be permitted to deploy Single Sign-ON (SSO) applications as long as they can ensure that the password is maintained in a secure manner.

AM 15. *Individuals who are not employees, contractors, or consultants are not granted a user account or are given privileges to use the Agency'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.

NIA Manual mandates controls to ensure that Access Control system of the organization is not compromised or breached. By default, individuals who are not employees, contractors or consultants (contractors and consultants with whom specific business or working partnerships exists and who have been given a security clearance) shall not be provided the access to the Agency's Information Systems.

Any exceptions (e.g. new vendors who may want to demonstrate a product/service) to the above rule shall be explicitly approved by the Security Manager who shall ensure that necessary security clearance is in place prior to providing an access.

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

Agencies should ensure individual accountability by assigning each user a unique user id. However in case where there may be a limitation (technical or otherwise) in implementing such a solution, Agencies should identify alternate methods of identifying the system user whilst using shared / non-specific accounts.

Controls could include account sharing based on time (e.g. Shift users), location (e.g. workstations, office area etc)

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.

Agencies should ensure that authentication information that grants system access or decrypts and encrypted device should be suitably protected. In worst case where this may not be possible due to reasons such as legacy systems, proprietary systems such information should not leave the system for which it grants access to. This will ensure that on a minimum the information would be protected using suitable physical controls that may be applicable on this system.

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

Agencies should ensure that adequate controls are in place to protect authentication data against threats such as replay, man-in-the-middle and session hijacking amongst other things.
Agencies should choose technologies that encrypt authentication data whilst in transmission, processing and storage.

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 (0-9)**
- **d. punctuation and special characters**

Agencies should define a password policy and its related procedures. NIA Manual mandates the requirements on how the passwords should be formulated. It promotes the usage of pass-phrases which are relatively easier to remember and difficult to crack.

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

NIA Manual mandates that passwords are changed every 90 days.

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

Further the NIA Manual mandates controls to minimize system / administrator overheads by ensuring that users cannot change passwords more than once in a day. It also mandates that system should force the users to change the passwords at logon time after it has expired or has been 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**

Agencies should ensure that wherever technically feasible, controls should be implemented to ensure that the system complies with the password policy. Further the controls should protect against re-use of passwords, password strengths etc.

Users and administrators shall be educated to ensure compliance with the password policies.

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

- **a. activate after a maximum of 15 minutes of system user inactivity**
- **b. activate manually 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.

NIA Manual mandates that controls are in place to secure active sessions. Systems shall be configured to activate screen / session locks after a maximum of 15 minutes of system user inactivity.

Users shall also be able to activate the screen / system lock in a manual mode.

Systems shall be configured to ensure that once locked, the screen completely conceals all the information; however it should not appear as turned off (to prevent somebody from switching off the power supply).

Systems shall remain locked until the user reestablishes access using appropriate identification and authorization procedures (i.e. user ID and password)

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 Agency.

NIA Manual mandates that Session controls are in place to prevent misuse of accounts / passwords.

System shall be configured to ensure that they lock user accounts after no more than three unsuccessful login attempts in a row and delay login for no less than 30 minutes, or require an administrator to reset the account before allowing login.

Agencies shall ensure that the manager of a user who is transferring (out of the Agency) retiring, receiving disciplinary action, etc., shall request the deletion of the computer logon ID and removal of access rights to all the allocated information assets.

Agencies shall ensure that the manager of a user who has had his duties re-assigned within the Agency by virtue of a promotion or internal transfer shall request a re-assignment of access rights to various IT resources in line with the new responsibilities.

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

Agencies must document procedures for dealing with lost, stolen, or otherwise compromised passwords. At a minimum these procedures must require users to:

a. Immediately report, to the Information Security Manager, the loss, theft, or compromise of passwords
b. Immediately change their password, if compromised
c. Agencies should establish and adhere to consistent, secure processes for verifying user identity before providing a replacement password.

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

Agencies should define procedures that monitor user access activity. Accounts that have been inactive for more than three months (e.g. long leave / medical leave) shall be suspended subject to further investigation. In case if the account is no longer needed, appropriate procedures shall be initiated to delete the account.

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

Agencies shall define procedures to ensure that accounts on system processing information rated C2, I2, A2 and or above shall be audited every 6 months to ensure it is current and up to date.

The audit shall confirm that in case of employees whose status, roles and responsibilities have changed on account of promotion, demotion, transfer, termination etc are reflected in the system.

9.4. Policy & Baseline Controls – System Access

In order to comply with this policy, **Agencies** MUST ensure:

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

Agencies should ensure that its security policies mandate the requirement to document access requirement form, security clearances, briefings, security awareness that may be necessary prior to providing system access.

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

Further to AM28, Agencies should ensure that system users are vetted in line with the requirements specified in section B6, Personnel Security. System users shall include employees, consultants and contractors. The requirements such as vetting of employees shall be defined as part of the procedure for providing system access.

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

Further to AM29, the NIA Manual mandates that controls are in place to educate the user on his responsibilities, security awareness and acceptable usage prior to providing him access to the system.

9.5. Policy & Baseline Controls – Privileged Access

In order to comply with this policy, **Agencies** MUST ensure:

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**

Agencies should ensure that procedures are in place to de-motivate the use of privileged accounts. Any such accounts shall be documented, monitored and be held accountable. All activities performed by a privileged account shall be audited.

The use of such accounts shall be minimized and shall only be used for administrative work only.

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

Further to AM33, System users with privileged access shall have different account for their normal day to day activities.

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.

In view of the National Security, only Qatari nationals (who have the requisite security clearance in line with the requirements of Section B-6 Personnel Security) shall be assigned privileged access to systems processing information classified as C4 and above

Any exception to the above rule shall be authorized by the Information Security Manager and the Head of the Agency.

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.

Agencies should define procedure to log key system management activities. The records of such activities shall be maintained in line with the requirements defined in Section B10, Logging and Monitoring.

Key activities include system availability (start-up, shutdown, recovery), maintenance, backup and recovery etc.

9.6. Policy & Baseline Controls – Remote Access

In order to comply with this policy, **Agencies** MUST ensure:

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 analyze associated risks and suitable controls are implemented to mitigate the identified risks.

Agencies shall not provide remote access to its user unless it is warranted by business requirements and authorized by the department head and / or ISM.

The department head and / or ISM shall base their authorizations on a due diligence exercise carried out to analyze risks associated with providing remote access facilities to its users. They shall further ensure that sufficient controls are in place to mitigate any identified risks prior to provisioning of the service.

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.

Agencies should ensure that additional controls including dual factor authentication is used to authenticate users, remotely accessing systems 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, Guidance on Cryptographic Security [CY]**.**

NIA Manual mandates that security control such as end to end encryption as specified in section C1-, Cryptographic Security is implemented to secure information in transit.
The encryption must begin with the initiation of the session, include all user identification and authentication, and not end until the session is terminated.

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.

Agencies shall ensure that remote access computers shall be installed with personal firewall, anti-virus software and malicious code detection and repair software. All these security software should be activated all the time.
Controls shall be implemented to ensure that users cannot disable or terminate these services. Further controls should be in place to ensure that remote access computers are free of computer virus and malicious code before connecting it to Agency's network. Agencies should look in to options of using Network Access Control or Endpoint Compliance solutions.

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

Agencies should define procedures to ensure that the remote access computers are updated with the latest virus signatures and malicious code definitions. Besides, latest security patches shall be applied to these remote access computers.
Agencies may look into options such as providing computers for remote access.

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

Agencies should define procedures and educate its users against accessing Agency's internal systems from public computers e.g. Cyber Cafes and using public printers for printing classified information.

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 Agency. Vendor remote access SHALL only be for a defined period of time, dictated by the duration of the task being undertaken.

Agencies should define policies and procedures to ensure that by default Remote Access is not provided to vendors.

Any exceptions as in case of a business requirement where there are no other viable alternatives available, explicit permission shall be provided by the Information Security Manager.

ISM shall ensure that appropriate controls exist in place to control and monitor the connections through its stages e.g. Initiation, Execution, and Termination. Further the connections shall be provided for a defined period of time governed by the tasks to be executed.

10. Guidance on Cryptographic Security [CY]

10.1. Policy Objective

10.2. Guidance on Policy & Baseline Controls

In order to comply with this policy **Agencies** MUST ensure that:

CY 1. The cryptographic algorithms, encryption hardware/software, key management systems and digital signatures, meet the requirements specified in Appendix B of this manual for Approved Encryption/Cryptographic Algorithms and Systems.

Agencies should ensure that cryptographic algorithms, encryption hardware/software, key management systems meet the requirements specified in Appendix B for approved Encryption / Cryptographic Algorithms and Systems.

Cryptographic algorithm chosen shall be of appropriate strength and recommended for designated use.

The validity of the specified algorithms will be assessed at regular intervals. NIAM shall recommend alternatives and or updates to the cryptographic algorithms as and when necessary. The Appendix B in NIA Manual will be updated to regularly reflect the technological change and the security threat profile.

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.

Agencies should ensure that the lifetime of the keys are determined based on the requirements of the application and the information infrastructure it is used in. This includes factors like operational requirements and ease for changing keys, Confidentiality and Integrity requirements of the application etc. Further if the key has been compromised or has been suspected of being compromised it shall be changed immediately and an incident is logged and managed as per the Incident handling procedures.

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. Agencies MAY apply these cryptographic controls to assets with lower confidentiality requirements, if determined necessary by their risk assessment.

NIA Manual mandates that information assets classified as C3 are encrypted and protected against unauthorized disclosure when stored and / or in transit regardless of the storage format and / or media.

Information assets classified below C3 may be secured with cryptographic controls if deemed necessary by their risk assessment.

CY 4. Information assets classified as I3 [IAP-—NAT-DCLS] have assured integrity by the use of cryptographic hashing. Agencies MAY apply these cryptographic controls to assets with lower integrity requirements, if determined necessary by their risk assessment. Appendix B to this section specifies approved hashing algorithms.

NIA Manual mandates that information assets classified as I3 have assured integrity by the use of cryptographic hashing.

Information assets classified below I3 may be secured with cryptographic controls if deemed necessary by their risk assessment.

CY 5. *The following protocols or better, with approved algorithms outlined in Appendix B, 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.

NIA Manual mandates approved algorithm specified in Appendix B for securing data in transit. Going further it mandates controls for securing specific types of application which handle data in transit and S/MIME v3 or better for securing email traffic

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.

NIA Manual mandates cryptographic controls to secure passwords against unauthorized disclosure when they are stored and / or in transit.

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

NIA Manual mandates that where Hardware Security Models are used, they are certified to at least FIPS 140-2 Level2 or Common Criteria [CC3.1] EAL4.

FIPS 140-2 are security requirements for cryptographic modules, published by NIST. It provides the basis for testing, validation and ultimately certification of cryptographic modules.

The standard is currently under review by NIST with a new version of the document. FIPS PUB 140-3 being planned to be published in soon.

The different levels within the standard provide different levels of security and in the higher levels, have different documentation requirements.

Level 1: The lowest level of security. No physical security mechanisms are required in the module beyond the requirement for production-grade equipment.

Level 2: Tamper evident physical security or pick resistant locks. Level 2 provides for role-based authentication. It allows software cryptography in multi-user timeshared systems when used in conjunction with a C2 or equivalent trusted operating system.

Level 3: Tamper resistant physical security. Level 3 provides for identity-based authentication.

Level 4: Physical security provides an envelope of protection around the cryptographic module. Also protects against fluctuations in the production environment.

The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. It is currently in version 3.1.[1]

Common Criteria is a framework in which computer system users can specify their security requirements, vendors can then implement and/or make claims about the security attributes of their products and testing laboratories can evaluate the products to determine if they actually meet the claims. In other words, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard manner.

Evaluation Assurance Level (EAL) - the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements (SARs, see above) which covers the complete development of a product, with a given level of strictness. Common Criteria lists seven levels, with EAL 1 being the most basic (and therefore cheapest to implement and evaluate) and EAL 7 being the most stringent (and most expensive).

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

Hardware Security Module (often abbreviated to HSM) is type of secure crypto processor targeted at managing digital keys for server applications. They are physical devices that traditionally come in the form of a plug-in card or an external security device that can be attached directly to the server or general purpose computer.

The goals of an HSM are the: (a) secure generation, (b) secure storage, (c) and use of cryptographic and sensitive data material. HSMs provide both logical and physical protection of these materials from non-authorized use and potential adversaries. In short, they protect high-value cryptographic keys.

Agencies should ensure that only HSMs that comply with CY5, are used for storing Cryptographic keys.

CY 9. Suitable key management processes are defined, as per [ISO11770-1] 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**

Agencies shall define policies and procedures to manage the lifecycle of the cryptographic keys. The procedures shall at a minimum cover the functions mentioned above.

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

NIA Manual mandates that licensed Certificate Service Providers (CSPs) comply with the requirements mentioned in CY10.

NIA Manual recommends that Agencies and CSPs evaluate and deploy online revocation systems to minimize the risk of fraudulent use of digital certificates. Such systems include Online Certificate Status Protocol (OCSP), Delegated Path Validation (DPV), Delegated Path Discovery (DPD) etc

CY 11. Security token/smartcard provisioning systems of CSPs meet the requirements for Subject Device Provision Services as specified in [CWA14167-1].

Security token / smartcard provisioning systems of CSPs meet the requirements for Subject Device Provision Services as specified in [CWA14167-1]

This CEN Workshop Agreement (CWA) specifies security requirements on products and technology components, used by Certification Service Providers (CSPs), to create Qualified and Non-Qualified Certificates. These certificates are used in conjunction with electronic signatures and advanced electronic signatures in accordance with “Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures” [Dir.1999/93/EC].

This CWA is specifically relevant for manufacturers of Trustworthy Systems (TWSs) used for managing certificates. It provides an overview of a CSP system broken down into a number of services. Some of these services are mandatory, termed ‘Core Services' whereas others are optional, ‘Supplementary Services'.

Core Services covers the following CSP services:

a. Registration Service - to verify the identity and, if applicable, any specific attributes of a Subject

b. Certificate Generation Service - to create certificates;

c. Dissemination Service - to provide certificates and policy information to Subjects and Relying Parties;

d. Revocation Management Service - to allow the processing of revocation requests;

e. Revocation Status Service - to provide certificate revocation status information to relying parties.

Supplementary Services covers two optional CSP services:

a. Subject Device Provision Service – to prepare and provide a Signature Creation Device (SCDev) to Subjects. This includes Secure-Signature-Creation Device (SSCD) provision;

b. Time-stamping Service – provides a Time-stamping Service which may be needed for signature verification purposes.

A CSP must implement systems that provide all Core Services.

This specification provides standards for Trustworthy Systems (TWSs) providing Core and Supplementary Services, issuing both Qualified Certificates (QCs) and Non-Qualified Certificates (NQCs). Meeting the requirements for issuing of QCs automatically implies meeting the requirements for issuing NQCs.

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

NIA Manual mandates that certificates used in a production system shall have been issued by a CSP licensed in Qatar.

11. Guidance on Portable Devices & Working Off-Site Security [OS]

11.1. Policy Objective

11.2. Guidance on Policy & Baseline Controls - General

In order to comply with this policy, **Agencies** MUST ensure:

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

Agencies should define policies and procedures that govern the usage of Mobile Devices and laptops within the organization. Policies should cover amongst other things ownership of such devices, security controls inline with the asset classification, tracking and compliance.

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

NIA Manual does not recommend the use of Bluetooth protocol. In case where it is used, users should ensure that it is not used to carry out classified conversations. This includes the usage of Bluetooth enabled headsets.

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

Further to OS2, MDs and laptops holding classified information shall have their Bluetooth serial connection disabled to avoid being detected as attack points.

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

Agencies shall define procedures and identify controls to ensure that MDs with recording facilities are not permitted in controlled areas without prior approval from the Security Manager.

MDs shall include cell phones, PDAs, portable cameras etc. Recording shall include all forms of audio and video recording.

High risk area are those where any form of C2+ information is present. For example, offices of high ranking officials, meeting rooms, etc

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

Agencies should ensure that all laptops and MDs (where possible) encrypt the information. The encryption shall be of suitable strength and in line with the requirements specified in Section C10, Cryptography.

In case of MDs where encryption is not possible, strong PINs or passwords should be used.

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

Agencies should educate its users that MDs and laptops are susceptible to thefts easily. Users should therefore safeguard MDs and laptops and not leave them unattended. MDs and Laptops should be kept secure when not in use.

For e.g. while travelling for instance, users should consider using laptop cable locks to physically secure laptop and portable computers.

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

Agencies shall define policies and procedures and implement controls to ensure that MDs and laptops not directly owned or controlled by Agency are not used with the Agency's systems.

This is to ensure a controlled SOE exists on such devices and reduces the vulnerabilities associated with such systems.

All Agency owned and controlled MDs and laptops shall be installed with anti-virus and malicious code detection and repair software with the latest virus signatures and malicious code definition files to protect against computer viruses and malicious codes.

In case of MDs and laptops which are not directly owned or controlled by Agency, but permitted to access the Agency's systems shall be managed, accounted for and accredited in the same manner as Agency owned device.

Agency's MDs and laptops may be temporarily connected to a non-Agency network, provided a suitable firewall is used to protect the device from any potential threats originating from the non-Agency controlled network.
Users should ensure that the MDs and laptops are scanned for malicious software before connecting it back to the Agency network.

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

Agencies should define procedures to ensure that Unaccredited MDs and laptops are not connected to Agency's systems or store Agency's classified information.

However, unaccredited MDs and laptops may temporarily connect to Agency's guest network for purposes such as accessing the internet or printing etc. Such networks shall be segregated from the Main network by use of firewalls.

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 agencies. The loss / theft SHALL be handled as per the B-8 Incident Management [IM]

Employees shall be educated on to immediately report loss / theft of MDs and Laptops to Information Security Manager / Office and concerned Law enforcement agencies. Agencies shall handle all such incidents in line with the defined Incident Management policies and procedures.

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

Agencies should educate its users on how to destroy or lock out a MD and / or a laptop in situations where there is a high probability of loss or compromise. Agencies should define procedures for destruction and lockout of MDs and laptops, and ensure that its users are trained to use them.

Agencies should look into controls that will facilitate the above requirement. MDs should allow this feature to be operated remotely.

12. Guidance on Physical Security [PH]

12.1. Policy Objective

12.2. Guidance on Policy & Baseline Controls

In order to comply with this policy, **Agencies** MUST ensure:

PH 1. 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.

NIA Manual mandates that Agencies adopt a risk based approach to identify and define physical security requirements. Such Risk assessments shall occur during the design phase of a new construction. In case of physical structures that are already built, risk assessment shall assess the suitability of the structure; identify appropriate controls to mitigate the risks.

Controls may include defined standard operating procedures, monitoring and control equipment.

The physical security shall be evaluated 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'.

NIA Manual mandates that controls implemented for security control are in line with their zoning / classification. Division of a physical area into zones will enable the Agency to identify suitable controls and effectively use the resources at its disposal.

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 Agency MAY incorporate additional controls in addition to those mandated by this policy.

Further to PH2, NIA Manual mandates that each physical zone is appropriately classified and necessary security controls implemented. Appendix A of the National Information Assurance Manual provides details on the minimal and baseline controls. It further recommends additional controls for medium and high level of security. Agencies may incorporate controls in addition to those mandated by this policy.

PH 4. Implementation of a “clean desk” and “clean screen” policy.

Agencies shall implement a “clean desk” and a “clean screen” policy at all times, ensuring that restricted material are not left un attended or unsecured on their desks, offices etc. A “clean desk” and a “clean screen” policy inculcate the importance of security amongst the users, further it mitigates risks associated with pilferage of information by extending concepts of “security by obscurity”.

Agencies should ensure that they provide necessary tools to its users to effectively comply with this policy. This may include:

a. Use of locked cabinets and containers to protect sensitive documents during working hours. The selection of containers shall be based on the level of risk. Threat factors such as unsupervised access to Building Maintenance Staff after office hours SHOULD be taken into consideration.

b. Offices of personnel storing sensitive information or assets should be locked when left unattended.

c. Staff trained to keep an eye and report on offices inadvertently left open or sensitive information assets left unsecured.

d. Screens and keyboards positioned in a way that they cannot be seen by unauthorized people

e. Use of opaque glasses, Blinds or drapes fixed on the inside of windows, glass partitions to prevent visibility from outside.

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

NIA Manual mandates that Server / Data or any similar information processing / storage rooms are on a minimum provided with medium protection requirements.

PH 6. *Cabling carrying information at levels C1-C3 is physically separate (including for fibre optic cabling) and is in separate ducting to that carrying Nationally Classified information

Cables carrying information classified at level C4 and above shall be physically separated from cables carrying information classified at C3 and below. The cables shall be secured through physically independent conduits. This is to provide adequate protection against interception and damage.

Further additional controls shall be implemented to secure cables carrying information classified at C4 and above. This may include

a. installation of armored conduit and locked rooms or boxes at inspection and termination points;
b. use of alternative routings and/or transmission media providing appropriate security;
c. use of electromagnetic shielding to protect the cables;
d. controlled access to patch panels and cable rooms;

PH 7. A site security plan and where necessary standard operating procedures (SOPs) for each secure areas 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.**

Agencies shall develop a comprehensive security plan complemented with standard operating procedures for secure area within the organization. The security plan at a minimum shall detail the points identified above.

13. Virtualization [VL]

13.1. Policy Objective

13.2. Policy & Baseline Controls

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.**

Agencies must evaluate the pros & cons of using virtualization. A thorough risk assessment needs to be done to evaluate the merits and demerits, it should extend from beyond the normal ROI to cases in use such as legal, regulatory impact that it may have. It should also ensure the availability of required skills & expertise within the organization.

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.

Agencies must harden the virtual environment using vendor recommendations and security guidelines. This includes hardening the hypervisor apart from the normal OS hardening steps. Improper settings on the hypervisor could allow virtual machines to cross-over to other virtual machines hosted on the same computer.

VL 3. Enforce least privilege and separation of duties [Refer to section C-9 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, Agencies 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.

Since the virtual setup is an aggregation of multiple systems with possibly multiple security ratings or multiple measures, it is very important to ensure that access, management and administration is tightly controlled.

Physical security of the machine hosting the virtual environment is important. Physical access would enable a person to bring down the virtual environment or copy the virtual machine to be used at another place thus leading to information leakage.

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.

Third party security technology like anti-viruses, IDS, etc must be used in each of the virtual environments setup, apart from the security controls used on the host machine. It should not be assumed that the host controls would be sufficient to protect all the hosted virtual environments.

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

Virtual Machines having data classification of HIGH should not be hosted on the same virtual environment as a virtual machine classified as LOW; because the LOW classified machines have lesser controls in place as compared to a HIGH classified machine. The LOW classified machines can thus be easier to compromise and then an attacker can find it easier to compromise the HIGH classification machine hosted on the same host. The host machines classification level should be the highest classification of its vm's.

VL 7. *A change management [Refer to Section B-6 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).

Change Management process must be followed for virtual environments to maintain the integrity of the virtual environment.

VL 8. *Logs from the virtual technology environment SHALL be logged and monitored along with other IT infrastructure. [Refer to Section B-10 Logging and Security Monitoring].

Logging must be enabled and monitored in the virtual environment as done with normal IT infrastructure.