The New India Assurance Company Ltd.

INFORMATION AND CYBER SECURITY POLICY

Document Control

Document Name: Information and Cyber Security Policy

Document ID Reference Number: NIA /ISMS/L2/1/Information Security Policy

Security Classification: Internal

Version history

Version	Issue date	Description
1.1	31/01/2017	Board approved Information Security Policy
1.2	20/12/2017	Board Approved Information & Cyber Security Policy
1.3	05/04/2019	Policy reviewed by MISC

Table of Contents

Page

1. Introduction

- The New India Assurance Company Ltd.'s (hereinafter referred to as 'NIA') information systems, and the information and data they contain, are fundamental for its daily operations and effective service provision. NIA shall implement adequate security policies, procedures and controls to protect confidentiality, maintain integrity, and ensure availability of all information stored, processed and transmitted through its information systems.

2. Information and Cyber Policy scope & applicability

- This policy applies to all users of NIA's information assets including employees, all third parties (including vendors and service providers), stakeholders, and contractor personnel. This Policy covers all Information Systems environments operated by NIA or contracted with a third party by NIA.

3. Information and Cyber Security Policy

- The specific objectives of the Information and Cyber Security Policy are:
  - To prevent unauthorized disclosure of information stored or processed on NIA's information systems (CONFIDENTIALITY)
  - To prevent the accidental or unauthorized deliberate alteration or deletion of information (INTEGRITY)
  - To ensure that information is available to authorized persons whenever required (AVAILABILITY)
- The information and Cyber security policy shall be approved by the management and published and communicated to all the employees and relevant third parties.

4. Policy framework

- The Information and Cyber Security Policy is supported by Information Security Procedures and implementation guidelines in the form of templates. The Information Security procedures are derived from the policy statements and provide the details of necessary actions to achieve the objectives of the policy statement. The templates are derived from the detailed procedures and aim at facilitating the implementation of the ISPP (Information Security Policies and Procedures).

5. Policy owner

- The ownership and responsibility for the maintenance of this information and cyber security policy lies with the Chief Information Security Officer. He/she must be contacted in the event of any questions on the contents of this policy, suggestions for improvements and any other areas relating to the security of systems, data or information of NIA.

6. Policy review and approval

- This policy document shall be reviewed at least annually by the CISO (Chief Information Security Officer) and the Management Information Security Committee or in events of any significant changes in the existing Information Security environment affecting policies and procedures. The policy owner will be responsible to make the changes to the policy document.In case of significant changes, the Management Information Security Committee will review & recommend to the Board necessary changes to the high level IS policy.

7. Compliance

- NIA expects all employees and relevant stakeholders/third party vendors having access to NIA's information and information processing facilities to comply with the policy.
- They should sign a document acknowledging abiding by this policy (Refer: ISMS L3- Agreement to Comply with ISPP (Information Security Policies and Procedures) of NIA.
- All violation or any attempted violation of the Information and Cyber Security Policies shall result in disciplinary action to be taken by the Management Information Security Committee in consultation with Human Resources Department. Disciplinary action shall be consistent with the severity of the incident, as determined by an investigation.
- All violations of the Information and Cyber Security Policies must be reported to the respective Department Chief Manager and the Head of Information Security Risk Management Team.

8. Segregation of duties

- Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

9. Contact with authorities

- Appropriate contacts must be maintained with relevant authorities such as law enforcement, regulatory and supervisory bodies by the Information Security Committee.
- The CISO (Chief Information Security Officer) must maintain a protocol to initiate contact with and report information security incidents in a timely manner to the concerned authorities.

10. Contact with special interest groups

- Appropriate contacts must be maintained with special interest groups such as security forums and professional associations by the CISO.
- This will help gain access to best practices in information security, timely advisories, and warnings of alerts, specialist security advice and to create liaison points while dealing with information security incidents.
- Specialist advice on security may be sought from either internal or external advisors, if required.

11. Exceptions

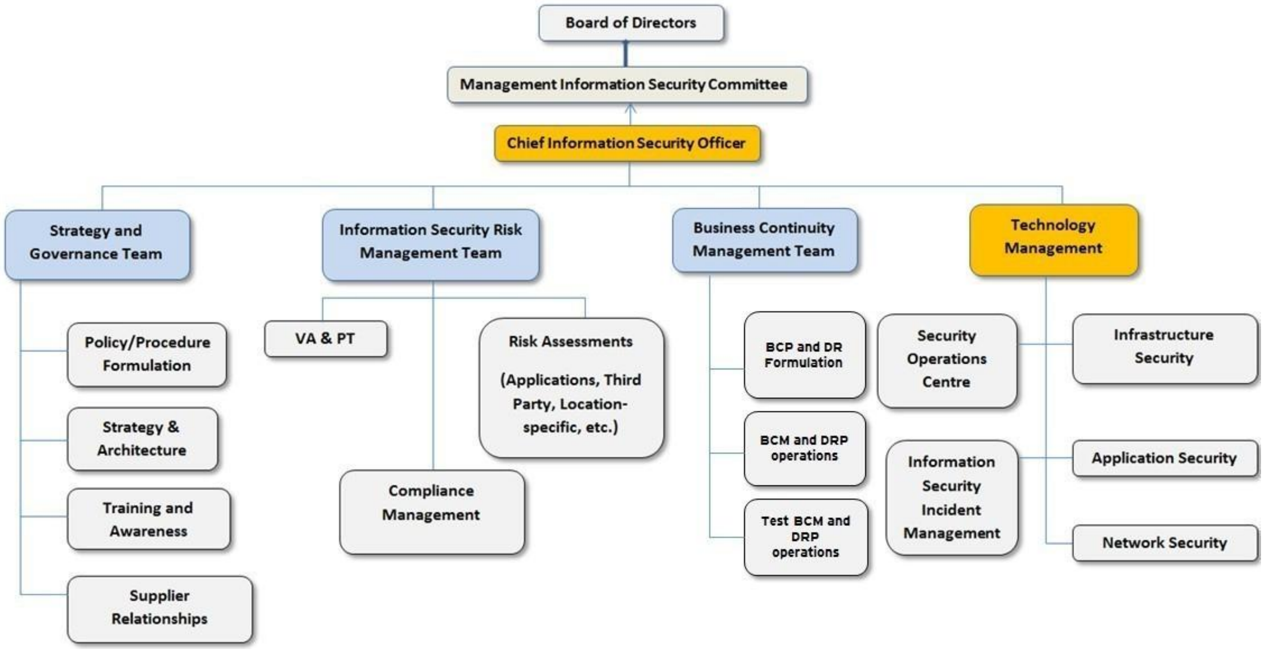
- Approval for exceptions or deviations from the policies, wherever warranted, will be provided only after an appropriate assessment of the risks arising out of providing the exception. This assessment will be conducted by the Information Security function. Approval for the exception will be provided by CISO. Exceptions will not be universal but will be agreed on a case-by-case basis, upon official request made by the information asset owner.
- All exceptions during implementation must be submitted by the Information Security Manager to the Head of Information Security Risk Management Team. All the exceptions are to be raised as per NIA's Information Security Policy Exception Form (Refer: NIA – ISMS – L4 – Information Security Policy Exception Form).
- The Information Security function will review all exceptions, as the case may be, every year for validity and continuity.
- The list of exceptions shall be reported to the CISO and the MISC (Management Information Security Committee) as deemed appropriate by In case there are any significant risks arising out of the exceptions granted or to be granted, the same should be reported by MISC to the board

12. Information and Cyber Security Organization Structure

12.1 Purpose

The purpose of this section is to outline NIA’s Information and Cyber Security Organization, responsible for implementation, monitoring and improvement of NIA’s Information Security Management System.

12.2 Information Security Organization Structure


Board of Directors
Management Information Security Committee
Chief Information Security Officer
Strategy and Governance Team
Policy/Procedure Formulation
Strategy & Architecture
Training and Awareness
Supplier Relationships
Information Security Risk Management Team
VA & PT
Risk Assessments (Applications, Third Party, Location-specific, etc.)
Compliance Management
Business Continuity Management Team
BCP and DR Formulation
BCM and DRP operations
Test BCM and DRP operations
Technology Management
Security Operations Centre
Information Security Incident Management
Infrastructure Security
Application Security
Network Security

12.3 Board of Directors

The Board of Directors is responsible for approving

- The overall framework to information and cyber security policy and strategy
- The information and cyber security implementation and assurance initiatives

12.4 Management Information Security Committee

The Management Information Security Committee (MISC) is responsible to:

- Provide overall guidance on the information security strategy and governance for ensuring information security at NIA
- Report the status of Information Security Management System to the Board of Directors.

Composition

The Management Information Security Committee comprises of the following members:

- Chairman Cum Managing Director – Chairman of MISC
- Head/GM (General Manager) – Information Technology

- Head/General Manager – Business
- Head/GM– Human Resources
- Head/GM– Legal
- Head/GM– Compliance
- Head/GM– Finance
- Head/GM- Risk
- Other GMs
- Chief Information Security Officer (CISO) – Secretary of MISC
- The Chairman Cum Managing Director is the chief sponsor of the Information Security Agenda. The MISC must earmark a budget for implementing information and cyber security initiatives and for meeting emergency responses for encountered security incidents.
- The CISO shall be the member secretary of the Management Information Security Committee. The CISO shall finalize the Information Security Goals and Objectives with the MISC, drive the implementation of approved Information Security program and report the state of Information Security to the MISC twice in a year.

Roles and Responsibilities

- The MISC will be responsible for the following:
    - The MISC shall develop the Information Security Strategy and take financial decisions on the Information Security plans. The MISC shall also define and document the information security goals and objectives of the organization.
    - Review and recommend to the Board necessary changes to the high level IS Policy. The Committee shall approve standards and procedures in line with the Board-approved IS policy.
    - Review and approve exceptions to the Information and Cyber Security Policy, any significant risk to be reported to the Board. However operational level exceptions can be approved by Respective Business owner in consultation with CISO
    - Review security roles and responsibilities defined in the Information and Cyber Security Policy from time-to-time and recommend changes to the constitution and functioning of the committee
    - Ensure compliance to regulatory and statutory requirements related to Information Security
    - Ensure that the information security governance framework is supported by an information security assurance programme (Implementation Plan)
    - The MISC (Management Information Security Committee) shall direct Strategy and Governance Team to raise specific security awareness across the organization and devise authority to take action on employees not adhering to information and cyber security policies and procedures.

  - The MISC shall assist in selection of the technology platforms for information security and guiding the implementation of the security strategy.
  - The MISC shall discuss any new significant information security risks identified as part of the Information Security strategy and determine suitable actions for risk mitigation.
  - Ensure the assessment of cyber security initiatives and assess information security incidents that have been encountered at NIA and make appropriate changes to the organization's information security policies, procedures and standards.
  - The MISC shall submit a report on the status of the Information Security program to the Risk management Committee of the Board, at least twice a year, in a format deemed fit by the Board.

12.5 Chief Information Security Officer (CISO)

- The CISO shall to report to the Head of Risk Management and will have a working relationship with the CIO to develop the required rapport to understand the IT infrastructure and operations, to build effective security in IT across the organization, in tune with business requirements and objectives.
- The Chief Information Security Officer will be responsible for the following:
  - Articulating and enforcing the policies to protect their information assets
  - Providing advice and support to management and information users in the implementation of Information and Cyber Security Policy.
  - Build and lead the information security team with appropriate competencies and attitude to deliver the information security program.
  - Promote user awareness initiatives within the organization.
  - Propose Information and Cyber Security Policy to the MISC, incorporate feedback on the implications of the policy from the MISC and other business areas into the policy-making process.
  - Be responsible for providing advice and support to management and information users in the implementation of Information and Cyber Security Policy.
  - Build and lead the information security team with appropriate competencies and attitude to deliver the information security program.
  - Promote user awareness initiatives within the organization

12.6 Information Security Team

- Organizations shall form a separate information security Team to focus exclusively on information security management. There should be segregation of the duties of officials dealing exclusively with information systems security and the Information Technology Division which actually implements Information Security controls at operational level. Information security team is divided into four teams with separate duties as below:
  - Strategy and Governance Team

  - Information Security Risk Management Team
  - Business Continuity Management Team
  - Technology Management Team
- Information Security team shall: -
- Develop and maintain IS (Information and Cyber Security) policy, standards, procedures and guidelines to support the organizations' information security program.
- Translate the information security program into specific actions which shall include awareness, security infrastructure, security incident response and risk management.
- Work closely with IT (Information Technology) and other functional teams and monitor implementation of information security projects and controls for new or identified deficiencies.
- Identify current and potential legal and regulatory issues affecting information security and assess their impact in conjunction with legal and compliance team.
- Act as consultants and advisors to different stakeholders for information security matters.
- Perform information security risk assessments on an ongoing basis and report any significant risks to ISC (Information Security Committee).
- Monitor information security incident management i.e. identification, response, remediation and reporting.

12.6.1 Strategy and Governance Team

- Develop, monitor and review Information and Cyber Security Policies and Procedures and obtain Senior Management commitment to information security
- Provide ways to improve efficiency and effectiveness of the information security function through training of information security staff; documentation of processes, technology and applications; and standardization and automation of processes, wherever feasible.
- Translate the information security program into specific actions which shall include awareness, security infrastructure, security incident response and risk management.
- Coordinate the implementation of Information and cyber Security Policies and Procedures across various business departments. Work closely with IT and other functional teams and monitor implementation of information security projects and controls for new or identified deficiencies.
- Collaborate on critical projects to ensure that security issues are addressed throughout the project management life cycle
- Participate in security investigations and compliance reviews, as requested by internal or external auditors
- Develop and maintain the appropriate metrics, dashboards and channels to measure the effectiveness and maturity of the information security awareness and training program

- Report status of information security initiatives and report compliance and issues identified to the Chief Information Security Officer
- Act as consultants and advisors to different stakeholders for information and cyber security matters.
- Monitor information security incident management i.e. identification, response, remediation and reporting

12.6.2 Information Security Risk Management Team

- Identify current and potential legal and regulatory issues affecting information security and assess their impact in conjunction with legal and compliance team
- Evaluate risks faced by NIA due to non-compliance to the organization's Information and cyber Security Policies and Procedures and provide strategic decisions to mitigate the risk
- Perform annual risk assessments using relevant procedures
- Conduct annual vulnerability assessments and penetration testing activities for NIA internally or with the help of external parties.
- Ensure that environmental and facilities management adheres to information security requirements.
- Executing planned approach for the audit
- Validate conformance to legal, contractual and regulatory requirements as part of risk assessment procedures performed

12.6.3 Business Continuity Management Team

- Formulate a comprehensive Business Continuity and Disaster Recovery framework for NIA information and information processing systems hosted on NIA premises as well as outsourced to vendors by contractual agreement.
- Manage BCM (Business continuity management**)** and DRP **(**Distribution resource planning) operations across the organization and invoke security measures/ initiatives
- Recommending recovery strategies and options, and assisting with the implementation of recovery solutions.
- Coordinating Business Continuity Plan exercises, mitigate exposure during disruptions of service
- Assign responsibilities for business continuity across NIA locations and promote awareness material in consultation with Training and Awareness team.
- Periodically test BCM /DRP and provide report to relevant stakeholders

12.6.4 Technology Management Team

- Manage technical security solutions deployed to support the Information and cyber Security Program across infrastructure, network and applications stack.
- Participate in technology remediation efforts through cross functional liaison with various teams
- Identify and respond to security incidents encountered

- Identify and communicate information security threats, desirable behaviors and changes needed to address these threats
- Manage implementation of minimum baseline security standards across platforms used on firm’s infrastructure

12.7 Functional Teams, Technology, Operations, Admin, HR

- Have primary responsibility for ensuring that appropriate and adequate security mechanisms are provided in the systems and network infrastructure shared across systems and business units.
- Be responsible for agreeing to security classification of all infrastructure components in agreement with the business owners.
- Have primary ownership to comply with specific security policies, which will be applicable for systems development and acquisition.
- Be responsible for maintenance of the various security tools and solutions.
- Be responsible for monitoring of secure status on each system and network within its control. Report on weaknesses or breaches of security to be made to the relevant Business owners or Infrastructure owners and to the CISO who shall in turn co-ordinate, the incident response.
- Technology/Operations/Admin/HR/ functional teams shall designate a suitable and qualified team member who will be responsible for reporting the incidents & effectiveness of security control to CISO/Information Security Team/ CIO.
- Legal Team — Legal Team is responsible for Engagement with Cyber security police officials, lawyers and Government agencies as required. Necessary details with regards to the incident are provided by information security team.
- Users and Information Owners — System users and data owners are responsible for the application of the policies relating to the systems, data, and other information resources under their care or control. They are also responsible for reporting any suspected cyber security incident to Information Security Team/IT Head/GM.
- Report status of information and cyber security initiatives and report compliance and issues identified to the Chief Information Security Officer
- NIA shall ensure segregation of duties for Information Security & IT operations teams.

12.8 Business Owners

- Hold the primary responsibility for defining the value and classification of assets within their control by participating in the risk management process and undertaking business impact assessment.
- Be responsible for authorizing access and segregation of duties for individual users and groups including Third parties to the information contained within the applications.
- Ensure that appropriate access of administration roles or teams exist for their applications to administer access in accordance with the IS Policy.

- Ensure implementation and compliance to Information and cyber Security Policies as applicable for their business units.
- Be primarily responsible for risk, data security and access of Third party partners and vendors to whom line of business has been outsourced
- Review the self-assessment of Third parties at defined frequency to whom line of business has been outsourced.
- Be responsible for conducting security assessments and audits of Third party processes / sites)
- Define Information Security requirements for third parties in concurrence with the Information Security team of the organization

13. Information Security Roles and Responsibilities

13.1 Asset Owner

- Asset owner is an individual or group responsible for controlling the production, development, maintenance, use and security of the assets. Asset Owner's primary responsibility is to maintain Confidentiality, Integrity and Availability (CIA) of the Information Asset.
- The responsibilities are described below:
- Review and update the asset list on a quarterly basis and share with Technology Management Team
- Determine sensitivity for the asset and define adequate controls to provide a coherent and consistent level of protection
- Define, approve and review the access control for the asset on a quarterly basis
- Define asset value based on CIA. The level of CIA should be valued in terms of its business value and impact on continuity of the information system (or impact on business operation). The asset value can be in form of risk ratings such as Restricted, Internal, Confidential and Highly Sensitive.

13.2 Asset Custodian

The Asset custodian is the individual or team managing the infrastructure needs of the NIA's assets.

- Implement protection measures and controls for the asset identified by the Asset Owner
- Provide secure infrastructure in support for the data hosting and administer access controls over the information
- Manage and monitor backup and recovery processes for the asset
- Validate the implemented controls and implement identified remediation measures for the asset

13.3 Information Security Manager

The Information Security Manager is the individual from specific departments identified to manage the information security activities within the respective department.

- Coordinate all information and cyber security activities in the respective department
- Assist in performing risk management activities
- Manage delivery of information security trainings and education programs in the respective department

14. Information and cyber Security in Project Management

Information and cyber security should be addressed in project management, irrespective of the type of the project.

- Project management activities carried out at NIA premises or at third party locations where NIA information or information processing systems are located should be integrated with information and cyber security requirements and principles to ensure that information and cyber security risks are identified and addressed as part of the project lifecycle.
- The project team shall identify applicable information security objectives as part of the project management activities.
- Information and cyber Security risk assessment shall be performed at an early stage by consulting with Information Security Risk Management Team as well as Technology Management Team.
- Controls required to implement and govern information security shall be identified and documented as part of the project implementation plan.
- Implications of information security events should be addressed and reviewed regularly by the respective team.
- Responsibilities for information security should be clearly defined and allocated to specified roles/teams defined in project management.

15. Information Security Risk management Policy

15.1 Objective

- This policy provides guidance on performing the risk assessment and determining appropriate information security controls that should be implemented for information assets.

15.2 Risk Management

- NIA shall define a process of identifying and evaluating risks to its information and information processing systems, and the potential impact on the IT (Information Technology) processes.
- Risk Assessments shall be performed on an annual basis covering the NIA Head Office and other locations for the various information and infrastructure assets.
- The Head/GM (General Manager) of Information Security Risk Assessment Team shall initiate risk assessment exercises by sending formal communication to Information Security Managers with various departments to perform the risk assessment activities.
- Additionally, the Risk Assessment shall also be performed in case of any specific events as mentioned below:
  - Major changes to processes, application, network and security architecture
  - Addition/ Changes to third party services
  - Emergence of new threats or vulnerabilities due to changes in the environment
  - Triggers from business and regulatory changes, compliance, etc.
- The scope of the risk assessments performed in case of the specific events as mentioned above, would be specific to cover potential information security risks that may arise due to the trigger event.
- The Risk Assessment activities performed by the Information Security Risk Management Team shall follow the procedures outlined in the Risk Assessment and Management Procedure document.
- NIA shall take risk remediation steps and mitigate the identified risks based on the priority. These mitigation steps could consider:
  - The business importance of the assets, processes and resources
  - The probability and frequency for the occurrence of the risk
  - The direct and/or indirect costs associated with each risk treatment and the benefit of risk reduction.
- A Risk Treatment Plan shall be documented based on the risk assessment activities performed and shall be communicated to the MISC (Management Information Security Committee) for approval.
- Information Security Managers should assist the Risk Owners to track risk treatment activities to closure in their respective departments.

- The Management Information Security Committee shall oversee the status of Risk Treatment activities performed across various departments to manage the identified information security risks using appropriate governance mechanisms.

16. Mobile Device and Teleworking Policy

16.1 Objective

- This policy provides guidance on securing technology platforms for mobile devices and teleworking facilities used by NIA employees on which business information may be stored.

16.2 Mobile device security policy

- NIA shall identify and allot mobile computing devices to its employees on need basis.
- NIA shall ensure that an inventory is maintained of the mobile computing assets along with the current users and software status. This inventory shall take into account at least but not limited to the list of identifiers such as device name, owner’s ID (Identity Document), device serial number, device IMEI (International Mobile Equipment Identity), device’s MAC (Media Access Control) address, device capabilities, etc. The mobile device inventory should be reviewed at least once a year
- Sensitive data stored on laptops and other mobile storage devices shall be kept to a minimum to reduce risk and impact shall a breach of security occur.
- Mobile devices containing confidential, personal, sensitive and generally all information belonging to NIA, except public information, shall employ encryption or equally strong measures to protect the corporate data stored on the device.
- Appropriate secure authentication and authorization mechanism shall be put in place for providing access to the mobile devices/Tele-working into the NIA’s network. All mobile devices used by users shall have access control by using strict password mechanisms.
- The mobile devices shall always have an up-to-date anti-virus program installed.
- NIA shall ensure that information held on any mobile device must be erased before the device is reassigned to another user or for another purpose.
- It is the responsibility of user to follow the guidelines regarding usage of mobile devices outlined in the ‘Acceptable Use Policy’ in this document.
- NIA should implement remote device wiping or blocking mechanism for all devices accessing NIA’s internal networks to protect a data in case of loss/theft of devices.

16.3 Bring Your Own Device (BYOD) policy

- No external mobile devices (i.e. devices owned by the users) shall be connected to NIA corporate network without approval from Head/GM of Technology Management Team.
- NIA shall assess and document the mobile devices and platforms allowed as part of the BYOD facility.
- NIA’s IT (New India Assurance’s Information Technology) team shall identify requirements for various BYOD user types, profiles and devices

- Users can be provided with temporary access to NIA infrastructure using their mobile devices with valid business justification and with relevant approvals.
- While using such approved devices, users shall adhere to the Acceptable Usage Policy guidelines.
- NIA shall consider long-term plans for BYOD activities in line with the enterprise strategy and business requirements.
- Any violation shall be identified and raised as a security incident for appropriate resolution.
- NIA shall develop and document a list of all software approved to be used on the employee devices for compliance to NIA’s Information Security Policy requirements. This list should be reviewed on half yearly basis
- NIA employees shall ensure that strong authentication mechanisms are deployed on their personal devices to allow secure access to sensitive business information.

16.4 Teleworking security policy

- NIA employees shall be granted remote connection access in case of business criticality after appropriate approvals.
- Teleworking shall be allowed only after analysis of business justification and due approval by Chief Manager/ Regional Manager and Head/GM of Technology Management Team.
- NIA Technology Management Team shall maintain the access list and review the same annually.
- NIA’s IT (New India Assurance’s Information Technology) department shall ensure that necessary secure remote connections mechanisms are in place such as secure VPN (Virtual Private Network) tunnel, encryption or equivalent technology.
- In-bound connections to internal NIA network and/or information systems from external sources shall pass through an additional access control point (e.g. a firewall, gateway, or access server) before users can reach a login screen.
- Remote access must be strictly controlled by the use of unique user credentials.
- NIA shall ensure that remote access provided shall be for a specific time only and shall be revoked on expiry of duration.

17. Asset Management Policy

17.1 Objective

- The purpose of this policy is to help NIA in effectively managing various information assets in the organization.

17.2 Responsibility for assets

Inventory of assets

- All NIA assets shall be listed in an Information Asset Inventory.
- Each Asset shall be clearly identified individually and (if appropriate) collectively in combination with other Assets to form an identifiable asset.
- The Asset Inventory shall contain the following information as a minimum:
  - Asset Identification
  - Name
  - Quantity
  - Asset Owner
  - Asset Custodian
  - Location
- Examples of assets include:
  - Information: Assets such as the information contained in a database, tapes, configuration files, software media, licenses, contract copies, physically signed documents, reports, and application licenses and all employee and vendor contracts
  - Physical: All hardware & peripherals, such as – servers, PCs (Personal Computers), laptops, routers, switches, etc.
  - Software: Assets such as the operating system, database and the applications running on a server are all software assets.
  - People: Key people required for day to day operations.

Ownership and Custodianship of assets

(Refer: Section ’13. Information Security Roles and Responsibilities’ in this document)

Rules for Acceptable use of Assets

- NIA shall ensure that there shall be rules defined for the acceptable level of use for all the information assets of the organization.
- NIA shall ensure that the employees, contractors and third parties follow the guidelines for the acceptable level of use of all the information assets. Assets shall be used for official business purposes only.
- (Refer: Acceptable Use Policy in this document)

Return of Assets

- NIA shall ensure that employees, contractors and third parties must forfeit access to information assets owned by NIA during termination of employment or contractual agreement.
- Physical assets assigned to employees, contactors and third parties must be returned to the respective department before termination of employment or contractual agreement. The Department Chief Manager must ensure receipt of all assets provided to the individual.
- In cases where an employee or external party user purchases the NIA's (New India Assurance) equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment.

17.3 Information Classification Standard

Classification Guidelines

- The level of security to be applied to the information of NIA will depend directly on the classification of the information. NIA's information shall be classified by the respective Information Owners into one of the following categories:
  - Public
  - Restricted
  - Internal
  - Confidential
  - Highly sensitive

Classification Level	Definition	Examples
Public	This classification applies to information, which has been explicitly approved by the management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm.	• Service brochures • Advertisements • Press releases • Websites
Restricted	Applies to business information to be communicated to a limited section of recipients outside the company and may cause undesirable implications if disclosed to the general	• Third party agreements • Service level agreements • Information exchanged with business partners

	public.	
Internal	Applies to business information for which unwanted disclosure can have damaging consequences. This is generally information which is accessible to a wide circle of employees but is not intended for outsiders	• Internal communications, correspondence, internal e-mails • Internal guidelines, like circulars, office notes, office orders, organization plans • Internal information, like, bids, contracts, reports, plans
Confidential	Applies to sensitive business information, the unwanted disclosure of which can bring substantial financial damage, or damage to the company's reputation. Confidential information is important information determining the technical or financial success of parts of the company.	• Personnel data • Confidential information about third parties • Information on security measures and serious deficiencies, information on internal network topology
Highly sensitive	Applies to most sensitive business information, the unwanted disclosure of which can bring substantial damage to the company's goals, grave legal consequences, or severe damage to the company's reputation. Typically, secret information can influence the success or the existence of the entire company.	• Organization's strategies • Technology, or strategic planning • Commercial and budget plans

- All unclassified information at NIA in both physical and electronic form shall be automatically classified and considered as ‘Internal’.

Information Labeling

- All the classified information shall be appropriately marked by labelling on the respective asset.

18. Media Handling Policy

18.1 Objective

- The purpose of this policy is to provide guidance for effectively information and cyber security implications associated with managing portable media access at NIA.

18.2 Management of removable media

- Media, or removal media, refers to any storage devices that can be used to extract, store and transfer information outside NIA's (New India Assurance) corporate network.
- Storage devices shall not be allowed to connect to the NIA network. NIA shall deploy an end-point protection service to disable USB access from all desktops, laptops and end-user computing devices.
- Documented approval shall be taken from Chief Manager and Head of Technology Management Team for the use of removable media for business purpose.
- The Technology Management Team shall review access to media devices on a half-yearly basis in collaboration with Chief Managers.
- Perpetual access to media devices is strictly prohibited. Access shall be time-based as per business justification only and duly revoked in time.
- Employees or vendors shall get proper authorization from the Department Chief Manager if removable media are required to be taken out of office premises.
- Removable media shall be sanitized before being issued to employees. The contents of any re-usable media shall be made unrecoverable before putting it to re-use.

18.3 Disposal of media

- Media containing Restricted, Internal, Confidential and Highly Sensitive information shall be disposed-off in a secure manner.
- The content of removable media to be disposed that is no longer required must be made unrecoverable and a record of such removal must be made to maintain an audit trail.
- The technique used for the disposal of media shall depend on the type and information present in the media.

18.4 Physical media transfer

- Removable media i.e. tapes carrying information shall be transported using the services of only authorized employee(s) or designated third party personnel.
- Media to be transported must be encrypted at all times in accordance with the classification of information stored. Where media is not in electronic form and cannot be encrypted, additional physical security measures must be deployed.

- Physical security measures such as safe packaging must be ensured during transfer of media containing sensitive information.
- All employees and vendor staff carrying media are required to ensure its appropriate protection during transit as stipulated by NIA’s (New India Assurance) Information Security Policies and Procedures.
- Logs must be recorded documenting the content of media, source location of transfer and receipt of media at the destination.

19. Acceptable Use Policy

19.1 Objective

- The purpose of this policy is to control the various activities that are not permitted by the Information and Cyber Security Policy with respect to usage of NIA assets.

19.2 General use of NIA assets

- Preventing the misuse of the assigned Access Card/Visitor Card is the responsibility of the cardholder.
- The data on NIA's (New India Assurance) network shall be the property of NIA and the users shall not exercise privacy to the data.
- Employees, consultants, contractors and business partners shall use NIA's (New India Assurance) Information Systems only for reasonable personal use.
- All users shall follow the Clear Desk and Clear Screen Policy while at the NIA premise. While leaving their work area unattended, the computer screen should be locked or protected by a screen saver as per the user password parameters outlined in the Access Control Policy. Similarly the work desk should be cleared of all the work related documents prior to leaving it unattended.
- For security and network maintenance purposes, authorized individuals within NIA may monitor equipment, systems and network traffic.
- NIA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

19.3 Information Classification and Labelling

- NIA's information shall be classified and labelled according to the criticality. And security controls should be applied basis on the classification category.
- Refer to the Information classification standard section in this policy for the detailed classification categories

19.4 Email Policy

- NIA's (New India Assurance) email system is a corporate resource and is to be used for as a medium for business-to-business and business-to-customer communication and transaction. This policy aims to ensure that NIA's email system is used exclusively for business purposes and that all emails sent or received by an NIA employee are secured against internal and external threats.

19.5 Security and proprietary information

- Password shall be kept secure and user account shall not be shared. Users are responsible for the security of their passwords and accounts. All the users shall adhere to the password management policy.
- All PCs (Personal Computer), laptops and workstations should be secured with a password-protected screensaver when unattended.

- Postings by employees/contractors using NIA email addresses to social media and newsgroups are expressly prohibited.
- Postings by employees / contractors from NIA email addresses to public forums shall be based on authorization and should contain a disclaimer stating that the views or opinions expressed by the individual are solely his own and in no way represent NIA's views/ stance/ opinion unless explicitly authorized.
- Employees and contractors must use extreme caution when opening e-mail attachments received from unknown senders, as they may contain viruses, e-mail bombs, or Trojan horse code.
- Any personal data processing device or information storage media like cartridge tapes, DAT (Digital Audio Tap), floppy disks, USB (Universal Serial Bus) devices, CD (Compact Disk) / DVD (Digital Versatile Disk), and Mobile Phones with camera and file storage capabilities must not be allowed to be brought inside Server Rooms / Disaster Recovery Site without approval from the IT Head/GM and CISO.
- Users will not bring & install or configure any personal media /software for use on NIA computer systems. Further, users would not be allowed to take official computer media out of NIA premises without appropriate clearances.

19.6 Clear Screen and Clear Desk Policy

- NIA employees, contractors and consultants shall follow a Clear Desk Policy for papers and removable storage media and a Clear Screen Policy for computing devices in order to reduce the risks of unauthorized access, loss of, and damage to information during and outside normal working hours.
- The relevant Information Security Manager shall communicate the Clear Desk and Clear Screen Policy to the employees and the contractors in their own areas and monitor their activities to ensure users compliance.
- Head/GM of Information Security and Compliance shall ensure that awareness training addresses Clear Desk and Clear Screen policies.
- At a minimum, the following guidelines shall be communicated to all employees and implemented to promote NIA's Clear Desk and Clear Screen policy:
- Paper and computer media shall be stored in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours
- Sensitive or critical business documentation shall be locked away (ideally in a cabinet or fire-resistant safe) when not required, especially when the office is vacated
- Personal computers are not to be left logged on when unattended and shall be protected by password protected screen savers;
- Printers, photocopiers and faxes shall be locked (or protected from unauthorized use in some other way) outside normal working hours;
- Sensitive or classified information, when printed, shall be cleared from printers immediately and shredded or securely disposed when not required.

19.7 Usage of firm-provided Devices

- Users should be allocated the Desktops/Laptops post appropriate hardening of the devices.
- Users shall only use the Desktops/Laptops owned and authorized by NIA and respectively assigned to them for official work purposes.
- Users shall not attempt to enable any vulnerable services on their systems. Users shall not disable the antivirus/anti malware softwares installed on their Laptops/ Desktops
- Users are not authorized to make any modification to the security configurations of the devices. In order to make any modifications, if required, users should log request with IT. Only IT team is authorized to make changes to the device configurations in consultation with the information security team if required
- All NIA employees, contactors, consultants and vendors who are assigned NIA-provided mobile devices (laptops, smart phones, iPads, tablets, etc.) shall comply with the following:
- Be responsible to ensure every effort at their disposal is taken to protect NIA’s mobile computing devices.
- Ensuring that the mobile device is used for business purposes only and that the usage complies with NIA’s Information and Cyber Security Policies and Procedures.
- Ensure that the device is never left unattended in an insecure place and is locked away wherever possible.
- Ensure that all ‘Confidential and above’ information contained on a mobile device shall be backed up as and when practical.
- Be responsible for updating the anti-virus software with necessary support from the IT department.
- Take safeguard measures when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside NIA premises, to avoid risk of disclosure to unauthorized personnel.
- In case of theft of mobile computing device, the undersigned shall report to the immediate reporting authority informing the details and lodging a report at the nearest Police Station where incident of device loss has occurred.

19.8 Access Controls

- All the users accessing the NIA internal network shall adhere to NIA information and cyber security policy and procedures
- Only authorized users shall connect to the NIA network (LAN (Local Area Network), wireless, remote etc.)
- All the users shall adhere to the defined password policy
- All remote access users are expected comply with NIA information and cyber security policy, and shall not perform any illegal activities, and may not use the access for outside business interests.
- All remote access connections to NIA network over the internet shall be secured

with encryption technologies such as SSL (Secure Sockets Layer) /TLS (Transport Layer Security) and VPN (Virtual Private Network).

- All hosts that are connected to NIA internal networks via remote access technologies must have up-to-date anti-virus software implemented.
- Only authorized users should connect to the NIA via remote access
- Remote access for troubleshooting using third-party free software or web applications shall be prohibited unless the requirement for the same is raised by the relevant user and is approved by the Chief Information Security officer

19.9 Unacceptable Use

Network and system activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NIA.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which NIA or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing account password to others or allowing use of account by others. This includes non-NIA employees when work is being done from home or other teleworking site.
- Using NIA’s computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any NIA account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Causing security violations, breaches or disruptions of network communication.
- Security breaches include, but are not limited to, accessing data of which the employee/ contractor is not an intended recipient or logging into a server or account that the employee/ contractor is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods,

packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless prior permission from Information Security Function is obtained.
- Executing any form of network monitoring which will intercept data not intended for the employee's or contractor's host, unless this activity is a part of the employee's / contractor's normal job/duty, is prohibited.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's / contractor's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, NIA employees/contractors to parties outside the organization.

Email

The policies for acceptable usage of NIA's (New India Assurance) email service are outlined in the 'Email Security Policy' in this document.

Internet Usage

The following activities are strictly prohibited, with no exceptions:

- Access to the Internet from NIA's personal computers is strictly for business purposes, and excessive or inappropriate personal use may be treated as a disciplinary offence.
- All material sent or received via the Company's computer and telecommunications networks is the property of NIA.
- NIA reserves the right to monitor Internet traffic for the purpose of preventing any activity that may be illegal, unauthorized or harmful to the Company, its employees / contractors, customers or business partners.
- Users should have no expectation of privacy for Internet access.
- Internet (Social media websites, chat portals etc.) and newsgroups are public forums where it is inappropriate to reveal confidential company information, customer data, trade secrets, and any other material covered by existing company policies and procedures. Users releasing protected information via a newsgroup etc. – whether or not the release is inadvertent – will be subject to disciplinary action.
- NIA retains the right to block access to any Internet web site.
- Only authorized persons are permitted to publish or act as spokespersons on behalf of NIA over the Internet or any other medium.
- NIA Internet access should not be used for:
    - Any profit related activity not sanctioned by NIA.

  - Obtaining unauthorized access to or knowingly modifying information held on Internet resources.

- Transmitting any NIA computer id or password information unless strongly encrypted and with Information Security approval.
- Accessing or downloading unauthorized, non-business related software including, but not limited to:
  - i. Software which could initiate unauthorized access to, or use of NIA computers, systems, networks or information.
  - ii. Software that might detect, identify or report any type of security weakness in NIA computers, systems or networks.
  - iii. Software that might cause harm or damage to NIA equipment, systems or networks.
  - iv. Software that infringes copyright legislation.
  - v. Games, games upgrades or related software.
- Downloading, transmitting, viewing or storing:-
  - i. Material which could be considered as defamatory, pornographic, vulgar or profane.
  - ii. Material that is insulting, defamatory or offensive to any individual or organization.
  - iii. Material which could harm NIA's status or reputation.
  - iv. Electronic harassment of any kind.
  - v. Publishing financial advice.
  - vi. Any activity which contravenes the current Data Protection Act.
  - vii. Any other use deemed unethical, illegal or unauthorized by NIA either now or in the future.
- All downloads from the Internet must be virus scanned immediately, regardless of originating site.
- Information Systems Internet use:
  - Application development using Internet facilities is restricted to management authorized employees and contractors.
  - No unapproved software downloaded from the Internet may be used in any production system or application and the integrity, continuity and full support of the product must be guaranteed.
  - The Internet must not be used as a storage or transport medium for NIA business critical applications except under secure conditions approved by the Company's Information Systems and Information Security departments.
  - Software patches or updates may only be downloaded from officially supported vendors, subject to current Information Systems test and approval procedures and adherence to the vendor's security and usage guidelines.

- All license fees and shareware costs for permitted software must be paid by the downloading department and authorized prior to download.
- NIA cannot guarantee the integrity, timeliness or availability of information transmitted or received via the Internet.

20. Email Policy

20.1 Objective

- NIA's (New India Assurance) email system is a corporate resource and is to be used for as a medium for business-to-business and business-to-customer communication and transaction. This policy aims to ensure that NIA's email system is used exclusively for business purposes and that all emails sent or received by an NIA employee are secured against internal and external threats.

20.2 Email Security

- All emails sent or received via the NIA corporate email system are the property of NIA and are subject to monitoring for information and Cyber security purposes.
- Access to emails should be created only after obtaining due approval for the specific individual.
- Employees should communicate their corporate email addresses to only people and organizations that are business partners of NIA.
- Each employee shall be aware that, with messages to Internet recipients, he/she represents NIA publicly.
- Employees should not give their corporate email address to friends and relatives who are personal associates and not business associates of NIA.
- All employees must ensure that the latest update of NIA's anti-virus software is running on their computer.
- Employees should not send any internal, confidential, or highly-sensitive information via email to external stakeholders. If in doubt as to whether to send certain information via email, users shall consult the Information Security Officer in their department or the Department Chief Manager.
- The following activities associated with usage of firm-provided email services are strictly prohibited, with no exceptions:
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters" or other "pyramid" schemes of any type.

- Use of unsolicited email originating from within NIA's networks of other Internet / Intranet / Extranet service providers on behalf of, or to advertise, any service hosted by NIA or connected via NIA's network.
- Posting the same or similar non-business-related messages to large numbers of users (spam).
- No attachment should be opened or stored from incoming email messages unless the employee can positively identify and confirm the sender's credentials.
- The permissible outgoing mail size shall not exceed 5 MB or as approved by Information Security Risk Management Team.
- No personal email should be sent or received unless there are extenuating circumstances such as a family emergency or crisis.
- No user (employee, contractor or consultant) may send or distribute email containing non-business related material such as jokes, spam, chain emails and related multimedia. This includes audio files, (e.g. WAV (Waveform Audio File Format)), video files, (e.g., AVI (Audio Video Interleaved)) or any form of such material.
- No user may send or distribute questionable email containing expletives or pornography.
- No user may send or distribute email containing derogatory, inflammatory, insulting or libelous information about any other NIA employee, customer, associate or any other person whatsoever.
- No user may conduct any business (whether personal or professional) via NIA's corporate email system other than legitimate NIA business.
- Any NIA employee receiving questionable material should immediately raise an incident for reporting such material to NIA's IT (Information Technology) team for appropriate action and then delete all local copies.
- NIA employees should be aware that all emails are being monitored to ensure that NIA's email policy is being adhered to.
- NIA employees found to be acting in contravention of the above policies will be warned by the appropriate Information Security Officer and asked not to repeat the offence. Employees who continue to disregard the above policy will face the action as per the Human Resource Security Policy if the offence is considered to be of a serious nature. Note that any offence associated with pornography or insulting behaviour will be automatically classified as being of a serious nature.
- All NIA employees, contractors, consultants and vendors having access to corporate emails shall adhere to additional guidelines documented in the 'Acceptable Use Policy'.

21. Human Resource Security Policy

21.1 Objective

- The objective of this Policy is to provide direction to NIA management on how to manage a competent workforce which understands aspects roles and responsibilities with respect to Information Security.

21.2 Prior to employment

Job description-roles and responsibilities

- All job responsibilities with respect to Information Security must be documented and must include general as well as specific responsibilities for implementing or maintaining security in NIA.
- Information security roles and responsibilities will be communicated to job candidates during the pre-employment process.
- All employees, contractors and third party service providers of NIA must understand their job roles and Information Security responsibilities.
- For contractors and third-party service providers, the contract agreement shall include clauses outlining such roles and responsibilities with respect to Information Security.

Background checks

- Background checks must be performed on all personnel including employees, contractors and third-party service providers.
- Further, personnel who are third party service providers must have undergone a background check by their respective organizations and the assurance of the same shall be provided to NIA. A provision for this shall be included in the contractual agreements.

Terms and conditions of employment

- All employees, contractors and third party users of NIA’s (New India Assurance) Information Assets must sign and agree terms and conditions of their employment contract. These terms and conditions shall state personnel’s responsibilities towards Information Security.
- In case of third-parties, a provision for this shall be included in the contractual agreements.

21.3 During employment

Management responsibilities

- The respective Department Chief Managers shall provide guidance to their department staff on understanding the information security expectations of their roles.

Confidentiality agreements

- All employees, consultants and contractors of NIA's (New India Assurance) information assets must sign the 'Agreement to Comply with ISPP (Information Security Policies and Procedures) and & third-party vendors should additionally sign a formal 'Non-disclosure agreement' respectively as indication of their acceptance to protect the confidential and sensitive information of the company.
- Users are required not to disclose company information derived as a result of their access to NIA's Information Systems to unauthorized parties.
- Appropriate disciplinary actions will be carried out against personnel in cases of breach of confidentiality agreements.

Information security training and awareness

- Information security training and awareness programs must be provided by Strategy and Governance Team to all the employees, third party contractors and relevant third party users of NIA's Information systems in order to create consciousness about the Information Security policies and processes as well as information security initiatives deployed.
- Contacts with special interest groups (such as ISACA (Information Systems Audit and Control Association), CERT (Computer Emergency Response Team), NCIIPC (National Critical Information Infrastructure Protection Centre), etc. shall be maintained.

Disciplinary process

- Disciplinary action shall be taken against employees, contractors or third party users who have violated the organizational Information Security policies and procedures. The disciplinary process shall ensure correct and fair treatment of employees, contractors and third party users who are suspected of having committed serious breaches of security.

21.4 Termination or change of employment

Employees, contractors and third party termination of employment

- NIA shall ensure that termination of employees, contractors and third party users are done in orderly manner and responsibilities are defined within NIA to ensure the same. The assets of NIA assigned to terminated individuals shall be taken back and all their access rights (both physical and logical) shall be removed immediately.
- NIA shall take into consideration the Information Security responsibilities of terminated or transferred employees, contractors and third party users and assess the appropriateness of their access when such occasions arise.
- No employee shall , while in service or post exit (Retirement/resignation/VRS etc), disclose any non-public NIA's information (internal, confidential, sensitive) to any other persons/company/portals etc unless authorized to do so by NIA in writing.

Return of assets

- All employees, contractors and third party users must return all of NIA’s assets in their possession upon termination of their employment, contract or agreement.

Removal of access rights

- Chief Managers from Human Resources, IT (Information Technology) Department and respective department (that the specific employee belongs to) must ensure that the access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

22. Third Party Security Policy

22.1 Objective

- The objective of this policy is to provide direction to NIA's management on how to manage and control third party relationships in a secure manner.

22.2 Prior to Engagement

Information Security Policy for Supplier Relationships

- Strategy and Governance Team shall ensure that all services to be provided by the third party organization are clearly identified and the relationship is managed through clearly identified point of contacts from both NIA and the vendor.
- A formal contract shall be entered between NIA and all third parties providing service to NIA or using NIA's information systems. The services to be provided by the outsourced party shall be covered by a Service Level Agreement ('SLA') that takes into consideration expected levels of service, security, monitoring, contingency and other stipulations as appropriate.
- Responsibility for identification and handling security incidents must be documented and agreed with the third party vendors.
- All third parties shall be required to provide information to NIA about related subcontractors and obtain NIA's permission for the subcontracting, prior to initiation of work by the subcontractor.
- Any sub-contracting arrangements should cover due diligence aspects
- Non-Disclosure Agreements shall be signed by vendors, third parties and contractors to protect NIA's information assets.

Addressing security in supplier agreements

- NIA shall ensure that the SLA (Service Level Agreement) / contracts/ agreements with third parties cover NIA's security and service delivery requirements. Security controls and service levels specified in the SLA shall be implemented, operated, and maintained by the third party for compliance to NIA's information security policies and procedures.
- The service level agreement (SLA) shall specify information security requirements and controls, service levels and liability of suppliers in case of SLA violations, non-mitigation of IS vulnerabilities, IS incidents etc. External party shall demonstrate compliance with all SLA requirements.
- Contracts/Agreements shall include information security requirements to ensure compliance to NIA's (New India Assurance) security policies and procedures, requirement for validation of security arrangements, right to Audit/ inspection, Handling termination of a relationship

Information and communication technology supply chain

- NIA shall work with suppliers to understand the information and communication technology supply chain and any matters that have an important impact on the products and services being provided.
- Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.
- NIA shall obtain assurance that critical components and their origin can be traced throughout the supply chain. Vendors must propagate the information security requirements throughout their supply chain, especially in case of sub-contracts for parts of service delivery or components purchased from other suppliers.
- In case NIA's vendors outsource aspects of product or service to other suppliers, NIA shall monitor and have increased scrutiny over security requirements management for critical components.

Identification and addressing risk related to external parties

- NIA shall carry out appropriate risk assessment and put in place adequate mitigating controls prior to granting them any kind of access to NIA's information and information processing facilities.

22.3 Third party service delivery management (During Engagement)

- NIA shall review confidentiality and non-disclosure agreements with third parties periodically and whenever the service terms and conditions are changed.
- Access management for third parties including granting access, review of user access rights shall be periodically assessed and changed as applicable.
- In case of third party including Call Centre operations, the Operating system has to be hardened to prevent data leakages.
- NIA shall perform external Party Internal Controls Review in which:
    - External parties requiring review of internal control shall be identified on a periodic basis
    - Review findings shall be communicated to external party and corrective action shall be monitored.

Monitoring and review of third party services

- NIA shall review the performance of the third-party based on the agreed service levels.
- Security controls and service levels, associated reports and records of third party service providers shall be independently assessed, reviewed and monitored. Vendor audits shall be performed at least annually to review the services offered by the third party.
- NIA shall conduct annual review meetings to ensure that the desired performance levels are maintained by the supplier.

Managing changes to third party services

- NIA shall ensure that changes to third party services including maintaining and improving existing information security policies procedures and controls, are appropriately managed taking account of the criticality of business systems and processes involved and re-assessment of risks.

22.4 Termination or Renewal of Agreement

- NIA shall apply consistent method for securely handling the termination of relationships with external parties which shall include:
- Designating individuals responsible for managing the termination
- Revocation of physical and logical access rights to the organization’s information
- Return, transfer or secure destruction of assets (e.g.' back-up media storage' documentation, hardware and data.)
- Coverage of license agreements and intellectual property rights
- In case of renewal, NIA shall revisit the security considerations in line with the Prior to engagement scenario.

22.5 Business Continuity

- NIA shall establish alternative (contingency) arrangements to ensure that the business processes can continue in the event that the external party is not available (e.g. due to contract termination or a disaster or a dispute with the external supplier or the entry ceases its operations). This arrangement shall be based on the results of a risk assessment:
- NIA shall consider the following provisions for secure facilities for business processes to continue
- NIA to evaluate Escrow for information systems source code for and end of support / proprietary technologies (e.g.' application source code and cryptographic keys) using a trusted external party, such as a legal representative, lawyer or equivalent.
- Recovery arrangement to ensure continued availability of information stored at an external parties environment
- Alignment with the New India Assurance’s business continuity program

23. Cloud Security Policy

- The selection of cloud hosting model shall depend on the criticality of the information being hosted
- Wherever application/data/system hosting in a cloud is considered as an absolute requirement for commercial, business, regulatory, legal or other reasons, approvals should be obtained by the organization from their respective senior management.
- Business justification for considering the absolute requirement to host the data and system in Cloud. Classification of data to be hosted on Cloud Viz. Highly Confidential, Confidential, Public, Internal, etc.
- Appropriate access controls should be defined

23.1 Service Level Agreements

- Service Level Agreements should be defined to address sustainability, support for fail safe operations, Data Retrieval time, protection of IPR, etc. ,Security control measures to prevent, detect and react to breaches including data leakage and demonstration of the same, Unilateral contract termination/exit clause, Right to Audit for IRDAI /Law enforcement agencies and Cert-fin to access information / log,
- Service Provider’s contract shall include clauses to ensure confidentiality, integrity, availability and privacy of the data collected, processed, stored and disposed through cloud services.
- Contracts with service provider shall include but not limited to following in addition to the other contractual requirement:
    - SLA (Service Level Agreement)
    - Compliance to applicable laws & regulations
    - Data ownership
    - Authentication controls
    - Log retrievals
    - Patch Management
    - Configuration Management
    - Application/System Security Testing
    - Data Recovery plan
    - Data Deletion at separation or expiry of contract

23.2 Cloud Data Security

- Controls related to Operations Security shall be implemented for ensuring Secure Configuration, Application, OS (Operating System) , DB (Database), Web Server, Back-up & Recovery, Change Management, Capacity & Demand Management, Protection against Malicious Code and Monitoring, Auditing & Logging security requirements on cloud.

- Data-in-transition cloud shall be in encrypted form, as appropriate to the information classification.
- The Encryption techniques shall be implemented for cloud data hosting like Data in Transit and Data-at-rest for PII (Personally identifiable information).
- Any data related to NIA’s India operations & insured information must be hosted in India.
- Data retention and destruction schedules should be defined by NIA and service provider should be made responsible to destroy the data upon request, with special emphasis on destroying all data in all locations including slack in data structures and on the media. Organization should audit this practice, wherever applicable.
- Data retention controls should also ensure that the multiple copies of the data stored in different locations are also destroyed post the retention timeframe.

24. Virtualization

- NIA should identify and implement controls to ensure appropriate Provisioning and allocation of resources between different systems in virtualized machine and Securing information resides in the host and virtualized machines
- There should be centralized administration of virtualized systems
- Access Control shall be implemented and adequate process shall be in place to ensure no unauthorized virtual hosts or guests are created. Access from and to the host should be allowed through a firewall controls to restrict access to the necessary services only
- Adequate hardening guidelines should be identified and implemented
- Appropriate mechanism for monitoring the operations between the host and the guest should be put in place to ensure no unauthorized operations or no malicious operations or no resource monopoly happens between the VMs.
- Volumes or disk partitioning should be used and role-based access controls should be placed individually on each virtual machine.
- Virtual systems shall need to be regularly backed-up for error recovery and continuity of operations.

25. Access Control Policy

25.1 Objective

- To provide effective and consistent user identification, authentication and access control mechanisms for all information processing systems across NIA.

25.2 User access management

User registration and de-registration

- All users shall be granted access to the information systems through a formal user registration process including approval from authorized personnel before granting access.
- Unique user IDs (Identity Document) shall be assigned to individual who must maintain complete responsibility for actions performed using their accounts.
- Shared/functional accounts, not linked to a single individual, must be refrained from but may be permitted with documented business justification and adequate approvals.
- All users shall follow a formal de-registration process for revocation of access to all information systems which will include automated or timely intimation and revocation of access rights.
- On termination of employment, the unique account must be de-registered from the respective information system or service after revoking the role/ access-level.

User access provisioning

- NIA shall maintain a central record of all application, network and infrastructure systems access requests across the organization including approval and provisioning workflow in an automated tool, or in manual spreadsheet at minimum.
- Repository for all users accessing systems including third parties should be maintained.
- An approval must be sought from the Owner of the information service or system for its access.
- Appropriate role/ level of access must be granted to the user accounts on a need-to-know and need-to-use basis.
- For internal transfer or change of role, appropriate change to access-level must be performed in-line with current job responsibilities.
- On termination of employment, the access-level to the respective information system or service must be revoked/de-linked (Refer: Section 22.2.1: User registration and de-registration).

Privilege management

- Privileges associated with each type of information systems such as operating system, business applications, databases and network elements shall be identified and documented.
- Privileges shall be allocated to individuals based on the requirements of their job function and role, on authorization from appropriate personnel. Additional privileges more than what is required for the job function shall be allowed after obtaining appropriate approvals.

User password management

- All User passwords (Individual as well as Administrator) shall remain confidential and shall not be shared, posted or otherwise divulged in any manner.
- An initial password shall be provided to the users securely during the user creation process & the system shall be configured to force the users to change the initial password immediately after the first logon.
- The following password and account policy shall be enforced for all user and administrative accounts on operating systems, applications, databases and all other information protected by password controls:

Password Parameter	Configuration
► Minimum Password Length	► 8 characters
► Complexity	► Enabled (Alphanumeric with mandatory one capital alphabet and one special character)
► Validity	► Minimum: 1 day

	▸ Maximum: 90 days
▸ History	▸ Previous 3 passwords
▸ Account lockout	▸ Duration: 0 minutes ▸ Threshold: 5 invalid login attempts ▸ Reset Threshold After: 60 minutes
▸ Idle session after which user shall be forced to re-enter credentials	▸ 15 minutes

- Due to system limitations or business necessity if any of the password and account policy parameters cannot be followed, relevant exception shall be taken by the respective Department Chief Manager and the Head/GM of Information Security Risk Management Team. Review of user access rights
- Information Asset Owners (Application or Infrastructure) shall review the access rights or privileges assigned to the corresponding system bi-annually. Exception on this should be taken from the respective Department Chief Manager and the Head/GM of Information Security Risk Management Team

Removal or adjustment of access rights

- In case of internal transfers access shall be timely modified as required
- On termination of employment or contractual agreement, all access rights of an individual on NIA's information and information processing systems must be revoked on or before the Last Working Day.

25.3 User Responsibilities

Password Use

- Users shall be encouraged to create passwords that will prohibit easy guessing (i.e., passwords such as spouse's first name, favourite team, etc.
- Users shall be provided with the capability to change their password on the login interface (after authentication).
- User password resets will be performed as per the password policy, or if the user requests for the same.
- Vendor-supplied account passwords, encryption keys, and other access codes shall be promptly changed. Default passwords shipped with software, networking components shall be disabled as far as possible.
- Group accounts shall not be allowed to the extent possible so that individual accountability is maintained except for special cases with prior approval from Department Chief Manager. Where used, they shall be maintained solely within

the members of the group, and shall be subject to the same controls as personal passwords.

- Super user passwords shall be stored in a secure manner by the respective vendor managing the relevant system infrastructure. An owner must be defined for each super user account for maintenance and defining safeguard mechanisms for associated passwords, and must be agreed with NIA. Care should be taken to ensure continuity of super user account password in cases where the password is forgotten or the related person has left the organization without surrendering the passwords.
- Documented approval should be sought from the Head/GM of Technology Management Team at NIA for each usage of the super user account. The password shall be changed immediately after usage and stored in a secure manner.

Unattended User Equipment

- Each user shall secure their assigned assets using a system lock (such as OS (Operating System) account lock, etc.) and log off from applications when no longer needed.
- Physical assets not currently assigned to any individual or department shall be stored in a secure area.
- Head/GM of Strategy and Governance Team shall ensure that awareness training covers such areas of expected user actions and responsibility to information assets.

Clear Desk and Clear Screen Policy

(**Refer:** Acceptable Use Policy in this document)

25.4 Information system access control

Information access restriction

- Access to information and application system functions by users and support personnel shall be restricted to authorized users in accordance with the access control policy and procedures.
- All ‘Users’ shall be authenticated at a minimum by using User IDs (Identity Document) and passwords, before they can gain access to target systems to prevent Unauthorized access to the NIA’s (New India Assurance) information assets

Secure log-on procedures

- Access to all information systems at NIA shall be controlled by a secure log-on procedure. User credentials required for access to various information systems shall consist of a user ID (Identity Document) and password or other credential (such as digital certificates, token, etc.) that is unique to an individual.
- Users shall not have multiple accounts within the same computing environment.

User identification and authentication

- The host system shall authenticate each user prior to allowing access. Once verified, users shall automatically be directed to applications for which they have been authorized.

Password management system

- Restrictions shall be enforced at system authentication level to ensure adherence to password requirements.

Use of generic/ shared accounts

- Wherever feasible, generic accounts shall be refrained from and shall be created on NIA information systems only with valid business justification and relevant approvals.
- The owner of generic accounts shall maintain a list of all users who have access to the password and review the list on a quarterly basis.
- Sufficient automated controls shall be implemented to ensure logging of all activities performed by each user accessing the account along with the timestamp of activity.
- Wherever not feasible, a manual register shall be maintained by the account owner which shall be updated by the generic account users during usage of the account. This register shall record the exact timestamp and duration of activity for each user and a description of activities performed during the usage.
- The account owner shall review the automated and/or manual logs and review them for appropriateness on a monthly basis. The results including any discrepancies or risks identified shall be reported to the relevant System Owner in a timely manner.

Use of system utilities

- Wherever applicable, access to various system utility programs that might be capable of overriding system and application controls shall be controlled to ensure that the users do not obtain more information than what they require to perform their job function. Access to the utilities shall be limited to administrators only to assist end-users resolve problems.

Session time out

- Wherever technically feasible Operating Systems, Applications, Databases and Terminals or servers shall timeout and clear the screen automatically if the terminal is inactive for more than 15 minutes.

Limitation of connection time

- Connection times on high risk applications shall be restricted to only during business hours unless authorized.
- Periodic Access Review Access to all the Information systems should be reviewed on periodic basis
- All user-IDs (Identity Document) and their access right shall be reviewed by the respective functional business owner on a regular basis to avoid existence of

stray/orphan user accounts and ensuring that access rights are based on the need to know basis principle.

- The review shall include verification that the user's access rights and privileges are still in line with job requirements.
- Details of Business owner, approvers and their delegated authority shall be maintained and be re-certified and updated periodically.

26. Physical and Environmental Security Policy

26.1 Objective

- The purpose of this policy is to provide guidance on security NIA's (New India Assurance) information and information processing systems at its own and vendor premises effectively from physical risks.

26.2 Physical Security Perimeter

- Physical protection can be achieved by creating several physical barriers around the building premises and information processing facilities. A security perimeter can be a wall, a card controlled entry gate or a manned reception desk.
- Offices where NIA information is stored shall be logically divided into different zones. Each zone shall have appropriate level of access restrictions and access authorization requirements. Areas containing critical IT (Information Technology) equipment (such as Data Centre) shall be designated as high security zones.

26.3 Physical Entry Controls

- Only employees and authorized individuals shall be allowed to enter NIA and vendor premises where NIA information assets are located. Visitors' entry into the premises shall be restricted by appropriate security validations like checking the identity of the visitor, security frisking of belongings and bags, etc.
- There shall be 24x7 guarding of premises by a security personnel or a designated security agency.
- The credentials of the security personnel posted at such premises shall be verified with the agency to mitigate risks of theft or vandalism. Contact information of the security agency shall be maintained by the NIA for easy identification in the eventuality of a mishap, and shall be verified with the security agency whenever required by NIA.
- All movement of physical material going in and out of premises shall be duly authorized and tracked.

26.4 Securing offices, room and facilities

- Depending on the sensitivity of information handled within, the physical security for offices, rooms and facilities shall be designed and applied.
- Access to Data Centers shall be restricted to only the Networks team personnel and other authorized individuals.

26.5 Protecting against External and Environmental Hazards

- NIA offices shall be fitted with appropriate fire-fighting devices at critical locations in order to arrest the fire and to avoid damage to the various resources of NIA. Fire drills shall be conducted annually.
- Appropriate safety measures shall be taken to avoid loss and damage due to water flooding or inappropriate drainage system within the premises of NIA.

26.6 Working in Secure areas

- The following guidelines for working in secure areas shall be followed:
- Authorized personnel should only be aware of the existence of, or activities within, a secure area on a need-to-know basis
- Unsupervised working in secure areas should be avoided for safety reasons and to prevent opportunities for malicious activities to take place
- Vacant secure areas (such as storage facilities) should be physically locked;
- Photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized by Departmental Chief Manager.
- Third party support service personnel shall be granted restricted access to secure areas.

26.7 Public access, delivery and loading areas

- Access points such as delivery areas and other points where unauthorized personnel may enter the premises shall be controlled and isolated from information processing facilities.

26.8 Equipment sitting and protection

- All electronic office equipment including faxes, printers, photocopiers etc., shall be physically secured.

Security of Desktops and Network hubs

- Desktops shall be adequately protected from fire, water and pollution damage and power supply fluctuations.
- Networks hubs shall be secured from fire, heat, dust, water and other damages.

Media handling and security

- Media shall be protected from physical damages like fire, moisture and magnetic interference.
- Media shall be disposed securely and safely when no longer required to minimize the risk of sensitive and confidential information being disclosed to unauthorized persons.

26.9 Supporting Utilities

- Equipment shall be protected from power failures and other electrical anomalies. A suitable electrical supply shall be provided that conforms to the equipment manufacturer’s specifications.
- Options to achieve continuity of power supplies include:
- Multiple feeds to avoid a single point of failure in the power supply
- Uninterruptible power supply (UPS)

- Back-up generator
- A UPS to support orderly close down or continuous running shall be implemented for equipment supporting critical business operations. UPS equipment shall be regularly checked to ensure it has adequate capacity and tested in accordance with the manufacturer’s recommendations.
- A back-up generator shall be considered if processing is to continue in case of a prolonged power failure. An adequate supply of fuel shall be available to ensure that the generator can perform for a prolonged period.
- Emergency lighting shall be provided in case of main power failure. Lightning protection shall be applied to all key information processing facilities.

26.10 Cabling Security

- Power and telecommunications cabling carrying data shall be protected from interception or damage.

26.11 Equipment Maintenance

- Equipment shall be checked on a quarterly basis and maintained to ensure its integrity and usability.

26.12 Security of equipment off-premises

- Security shall be applied to off-site equipment taking into account the different risks of moving organization’s assets outside its premises.

26.13 Secure disposal or Re-use of equipment

- IT hardware and equipment shall be disposed only after approval from the respective Department Chief Manager. Further, appropriate data and media destruction shall be performed prior to disposal. Disposal of retired hardware and media shall comply with prevalent environmental regulations.

  (Refer: Media Handling Policy)

26.14 Removal of Property

- Equipment, information or software shall not be taken off-site without prior authorization. The following controls shall be applied:
- Employees, third-party and contractors who have the authority to take the equipment off-site shall be clearly identified.
- Equipment shall be recorded as being removed off-site and recorded when returned.

26.15 Environment Controls

- Threats posed by environmental hazards to the NIA’s (New India Assurance) information systems shall be addressed by implementing appropriate controls to detect, correct and prevent identified environment threats like Fires, Water Leakages, Power Fluctuations, Pests, etc.

Cleanliness

- Data centers holding NIA information assets will be kept dust free and protected from any kind of spillage of water or other liquids.
- To ensure dust free environment, Data center hub room/ server room will be cleaned by designated housekeeping personnel under the supervision of an authorized individual on a regular basis
- Smoking, spiting, eating and drinking shall be strictly prohibited in the Data Center.
- To enable easy movement of cables, the server rack will be positioned in certain height from ground level.

Temperature and Humidity

- Temperature of the Data center will be maintained as per the OEM (Original Equipment Manufacturer) recommendations.
- The facility management team will keep a record of Data center hub room/ server temperature twice a day i.e. Morning and Evening.
- The precision air conditioning systems will be duly maintained as per the facility management team.

Fire detection and Prevention

- Cabling will be sheathed in fire resistant conduits.
- Smoke or Fire detectors will be installed to forewarn against fire.
- The fire detectors equipment will be maintained and supervised as per OEM (Original Equipment Manufacturer) recommendations.
- Appropriate portable fire extinguishers will be installed at easily accessible locations. These will be suitably serviced and tested at regular intervals.

Water leakage prevention

- Information assets will be housed in a dry environment with appropriate measures in place to prevent water leakage. Water leakage detection equipment can be installed for automated monitoring of water leakage.

Power Supply

- Centralized Uninterrupted Power Supplies (CUPS) shall be used and maintained. Critical electronic equipment will not be connected to raw power supply.

Cabling

- The power and data cabling shall be separated as per vendor recommended best practices.
- The cabling shall be structured to avoid clutters.

Pests and insects

- Pest and insect control mechanisms will be implemented to prevent damage to the information systems assets.

27. Information Technology Operations Security Policy

27.1 Objective

- The objective of this policy is to identify key security operational activities to be performed by the NIA.

27.2 Documented Operating Procedures

- Operating procedures for all IT processes shall be developed, maintained and published to enable the authorized users, network and system administrators to perform their daily operations.
- Where applicable, the procedures shall include and abide by the applicable laws and regulations.

27.3 Operational Change Management

- Changes to IT assets (including applications, servers, system software, network devices and security architecture) shall be performed in a controlled manner to ensure that the risks associated with such changes are managed to an acceptable level. This involves obtaining prior authorization, performing impact analysis, testing, obtaining approval before deployment, and maintaining up-to-date current and historical documentation for the entire process.
- Changes requiring testing shall be tested in a non-production environment before deployment and ineffective changes shall be rolled-back.
- All emergency changes requiring expedited response, which bypass the Policies and Procedures outlined, shall obtain necessary approvals from Department Chief Manager and consult with Information Security Manager before deployment.
- All changes shall be monitored and reviewed for successful implementation and documented, they shall
  - Be performed by skilled and competent individuals who are capable of making changes correctly and securely. Developer and Release Manager / Deployment team access should be segregated.
  - Be signed off by appropriate business owners.
  - Have a record of version control and capture what was changed when and by whom.
  - Have communication of details to relevant individuals and checks be performed to confirm that only intended changes have been made
  - Ensure that documents associated with computer systems and networks are updated.
- Digital records created are to be adequately preserved over time and remain accessible and functional, even over successive changes in technology.

27.4 Operational Patch Management

- NIA shall ensure that all patches are applied based on criticality and its potential impact to the systems following appropriate testing of the patches.
- The firm shall ensure that all patches are first deployed in dedicated test environments and their impact assessed thoroughly before deploying the patches in the production environment.
- The firm shall ensure that critical patches are prioritized and deployed based on their priority, depending on the potential impact to the systems and adequate testing of the patches performed in the test environment.
- The firm shall use a phased deployment approach for installation of patches across various segregated systems.
- The firm shall ensure that all new hardware devices and software technologies are patched to the current patch level, as defined by the operating system vendor and supported by the application, prior to the device being connected to the production network.
- The firm shall ensure that if a patch is unavailable for an identified vulnerability, adequate/ reasonable compensating control measures shall be implemented to protect the system/application from being exploited.
- The firm shall ensure that if it is identified that a patch affects certain critical business functions, then adequate mitigation measures shall be implemented to protect the system/application from being exploited and relevant exceptions from respective Department Chief Manager should be taken and informed to the Head/GM of Information Security Risk Management Team NIA shall ensure that all the necessary patches/ compensating controls to be deployed in the production environment will follow the firm's Change Management Procedure.

27.5 Operational Capacity Management

- NIA shall continuously monitor the utilization and make projections for future requirements of information processing resources and plan accordingly to ensure that adequate information processing resources are available to meet the business requirements of NIA.
- Capacity requirements must be identified taking into account the criticality of the concerned system.
- Detection systems must be configured to indicate any problems related to capacity management in due time for systematic resolution.

27.6 System acceptance

- Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system shall be carried out prior to acceptance.

27.7 Segregation of Duties in Operational Procedures

- All processes shall adopt the principle of segregation of duties. The initiation of an event shall be separated from its authorization.

- Where segregation of duties is not possible or practical, the process shall include compensating controls – such as monitoring of activities, maintenance and review of audit trails and management supervision.

27.8 Separation of Development, Test and Production environments

- Development, test, and production facilities and duties shall be logically or physically separated to reduce the risks of unauthorized changes to the production system.
- Transfer of information between the development, test and production environments shall be controlled.

27.9 Information Backup Policy

- All application and operating systems software, data (including databases), application and operating systems configuration information, hardware configuration information, software and log files (logs from various systems that need to be backed) essential to the continued operations of NIA shall be identified, documented and backed up as per defined frequency.
- Frequency, medium and storage location of the backup shall be identified and documented.
- The security controls over the backup of information and media shall be commensurate with the classification of the information backed up, contractual obligations and other applicable guidelines. Backup shall be retained in accordance with the requirements set out in the contractual obligations. Backup register shall be maintained by personnel performing backup and shall be updated regularly.
- In addition to the scheduled backups, backups shall be taken in case any of the following event occurs:
- Configuration changes
- Changes in Operating systems
- Both onsite and offsite backup shall be stored in safe custody in a fire-proof safe. If fire-proof safe is not available, alternate controls shall be put in place to protect those tapes from fire.
- All movement of tapes between offsite and onsite locations shall be tracked and recorded.

27.10 Recovery Policy

- Backed-up data shall be tested for valid restoration at least annually, after appropriate authorization to test the effectiveness of the backup and recovery procedure.

27.11 Monitoring, Auditing and Logging and Protection of Logs

- Security logs shall be enabled on all critical information assets. A centralized approach to logging & monitoring should be implemented.
- Security Logs generated by different systems and devices shall be collected such that linking (correlating) events generated across these systems and devices is possible and should be maintained for a minimum period of six months and meet other specific regulatory stipulations as applicable.
- Security logs shall be made available to the Law enforcement agencies, IRDAI (Insurance Regulatory and Development Authority) and Cert-Fin as and when required
- Logging shall be enabled to track critical system activities which shall include:
- User account management
- Privileged user activities
- Changes in OS (Operating System) configuration
- Multiple authentication failures/simultaneous logins
- Access to audit trail
- Monitoring reports should be published based on the management requirements. Periodic review of logs and monitoring reports for adequacy and contents should be performed.
- User activities, exceptions, and security events shall be logged and monitored. Logs may include the following and not limited to:
- System starting and finishing times
- System errors or faults and corrective action taken
- The identity of the person making the log entry
- The activities of users with high levels of access (privileged users such as system administrators and system operators) shall be logged and independently reviewed on a regular basis.
- The audit logs shall be retained based on the predefined record retention requirements.
- Logging facilities and log information shall be protected against tampering and unauthorized access.
- The clocks of all relevant information processing systems within NIA or security domain shall be configured to an accurate uniform time source using Network Time Protocol synchronization.

27.12 Security of system documentation

- System documentation shall be protected from un-authorized access. The teams shall have their individual access-controlled folders in the common work area.

- The system or application owner shall authorize or approve distribution lists for system documentation.

27.13 Protection against malware

- All servers, desktops, workstations, hand-held devices, gateways and any other access points to NIA's (New India Assurance) network shall be protected against malicious code. The most current available version of the anti-virus software package will be taken as the default standard. Automatic update features will be enabled on all newly-installed systems.
- All computers attached to the NIA network shall have standard, supported anti-virus software installed. This software shall be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date

  (**Refer:** Anti-virus Policy in this document)
- Anti-virus software shall be configured to scan any files received over the corporate network or via any form of storage medium for malware.
- Business Continuity Planning shall analyze critical business processes based on the impact of malware attacks to determine measures for recovery of software and data.
- Installation of unauthorized software shall not be allowed on all NIA information systems.
- Technical vulnerabilities that can be exploited by malware shall be identified and mitigated.
- Adequate user awareness measures shall be implemented for the same.

28. Network Security Policy

28.1 Objective

- The objective of this policy is to identify key communication security activities to be performed by the NIA.

28.2 Network security management

- Access to NIA networks shall be provided to users on a need-to-know basis based with proper authorization from the Department Chief Manager.
- The protection of information contained on the NIA's networks is therefore the responsibility of the management and the activity and content of user information on the NIA computer networks is within the scope of review by management.
- NIA shall implement network security systems and resources (Firewalls, IDS (Intrusion Detection System), IPS (Intrusion Prevention System), routers, etc.) to protect all business data, related application systems and operating systems software from unauthorized or illegal access at a level that is appropriate for the information or computing resources.

Network controls

- Connection capability shall be restricted through access-control lists in firewalls and switches.
- A legal message shall be displayed on the screen whenever a user logs on to the network through any terminal to warn the user on using NIA network for business use only. A message shall be displayed on all external network connections warning potential users that unauthorized use is prohibited (e.g. Unauthorized access to The New India Assurance Company network is prohibited).
- The use of personal communications equipment (modems, ISDN (Integrated Services Digital Network) cards, etc.) attached directly to personal computers with remote control software shall be prohibited, unless authorized by a designated authority.
- Network access shall be given to third parties after analyzing the risks involved in providing such access, in accordance with the Third Party Security Policy.
- Routing controls shall be implemented for networks to ensure that computer connections and information flows do not circumvent the access control requirements of the business applications.
- Network diagrams at all levels (WAN (Wide Area Network) and LAN (Local Area Network) segments) shall be maintained and updated regularly by Technology Management Team.
- Minimum Baseline Security Standards (MBSS) shall be developed all network equipment shall be configured to comply with MBSS, which follows industry's best practices like CIS, NIST, STIG, etc.
- All Connection between NIA's network and any third party network shall be established only after authorization from the Chief Information Security Officer.

Wireless network security

- All Wireless Access Points/ Base Stations/ Wireless Devices connected/deployed in NIA's corporate network shall be registered and approved by the NIA Head/GM of Technology Management Team.
- Wireless networks must be logically segregated from the wired corporate network as well as the data center or other critical segments in the network
- All wireless LAN (Local Area Network) hardware used shall be certified Wi-Fi devices that are configured to use the latest security features available.
- Physical security controls should be implemented to prevent the misuse, theft or alteration of Access Points / Base Stations, and shall be locked in an appropriate manner.
- Access Points / Base Stations shall be subjected to vulnerability assessments, penetration tests and audits.
- Security requirements for wireless networks shall be identified and documented, such as security features and service levels.
- NIA shall ensure that all access points will operate with the highest security settings available for the infrastructure at the specific location.
- Features of wireless networks related to information security such as authentication and encryption technologies shall be clearly documented and Technology Management Team must ensure that the selected measures are implemented across the firm.
- Wireless Intrusion Detection Systems (WIDS) and/ or Wireless Intrusion Prevention System (WIPS) shall be installed to identify rogue wireless devices and detect attack attempts and successful compromise. These devices shall be installed based on a risk assessment performed and associated threat profile of the premise under consideration.
- All wireless traffic shall be monitored by wired IDS (Intrusion Detection System) as traffic passes into the wired network.
- All wireless traffic shall use strong encryption like Advanced Encryption Standard (AES) with minimum Wi-Fi Protected Access (WPA2) authentication.
- Wireless networks shall use authentication protocols such as Extensible Authentication Protocol (EAP)/ Transport Layer Security (TLS) or Protected Extensible Authentication Protocol (PEAP).
- Access to wireless networks and devices shall be limited only to authorized users.
- Wireless clients shall use strong authentication credentials to mitigate the risk of unauthorized access from compromised credentials.
- Peer-to-peer wireless network like Bluetooth, infrared, etc. on wireless clients shall be disabled unless such functionality meets a documented business need.

Security of Network Services

- All network services in NIA shall be identified and documented.

- Security requirements for network services shall be identified and documented, such as security features and service levels.
- Physical and logical access to diagnostic and configuration ports shall be controlled. Network and network services access shall be annually reviewed in order to ensure that unauthorized network services are not used or authorized network services are not accessed by unauthorized personnel.
- Features of network services related to information security such as authentication and encryption technologies shall adhere to the Information Security Policy and Network Security Team must ensure that the selected measures have been implemented.

User authentication for external connections

- Remote user access to NIA’s networks shall be subject to appropriate user authentication methods and should be permitted only after due approval from the Department Chief Managers.
- 'Users' seeking to gain privileged access to the NIA’s IT (New India Assurance Information Technology) facilities via public or other external networks shall do so via two factor authentications.
- All remote users shall connect to centralized communications servers.
- Proactive control measures and response procedures shall be in place to reduce the likelihood and impact of attacks such as but not limited to Phishing and man-in-the middle attacks.

Internet Service Management

- Access to the Internet shall be provided to employees for legitimate business purposes.
- Internet access to third parties shall be provided only through a proxy and after the necessary authorization have been obtained.
- All Internet activity shall pass through a firewall and a proxy gateway server or equivalent to the Internet so that access controls and related security mechanisms can be applied.

Segregation in Networks

- Networks shall be logically or physically divided based on the criticality of the information stored in the networks. If the network is logically separated, the perimeter of each domain must be well defined and appropriate perimeter security devices shall be put in place. If the network is physically separated, controls shall be in place to protect physical access to the network points at all ends.
- The criteria for division of networks shall also consider the relative cost and performance impact of incorporating suitable technology.
- Internal network shall be segregated from the external network with different perimeter security controls on each of the networks.
- The connectivity between internal and external networks shall be tightly controlled.

- Web servers shall be physically separate from database servers, and shall reside on separate network segments.

28.3 Information Transfer

Information exchange policies and procedures

- To prevent loss, modification, destruction, or misuse of information, NIA shall protect and control exchange of critical business information assets and software with third parties and outside organization.
- Exchange agreements
- Formal agreements shall be established for the exchange of critical business information assets or software with external organizations. The department requiring this exchange shall be responsible for the formal agreements to maintain confidentiality and non-disclosure of information.
- These agreements shall include both physical and electronic exchanges, and shall reflect the sensitivity of the critical business information assets being exchanged and shall describe any protection requirements.
- These agreements shall specify management responsibilities, notification requirements, packaging and transmission standards, responsibilities and liabilities, data and software ownership, protection measures, and all encryption requirements.

Electronic messaging

- Information involved in electronic messaging shall be adequately protected to prevent loss, modification or misuse of information as per the ‘Email Policy’ in this document.

On-line transactions

- Information involved in online transactions shall be adequately protected from modification and misuse.
- Technologies like Digital Certificates or equivalent shall be used to ensure enhanced security features such as integrity authentication, non-repudiation of the online trading server and for all online trading transactions with remote users, business partners and regulatory agencies.
- Encryption shall be used to ensure confidentiality for online transactions
- At log-in time, every user must be given information reflecting the last login time and date. Also, details of any unsuccessful log-on attempts since the last successful log-on must be displayed, wherever possible. This would provide end-users with the information needed to determine whether an unauthorized party has used their User ID.
- A warning banner must be displayed at login to all individuals gaining access either intentionally or unintentionally. This must advise users that the system is for authorized personnel only and its use may be monitored. The System Administrator and the legal department must verify the possible legal issues related to the text put in the banner.

- The warning banner must not include any system or application identifiers like the type of host hardware or operating system present on the host, information about the organization, the network configuration or other internal matters, which may provide valuable information to a would-be intruder.

Data Transmission

- Any information from NIA's environment travelling over third-party networks or public networks shall be encrypted, wherever feasible. Appropriate encryption algorithms shall be used to maintain the integrity and confidentiality of the data.
- Appropriate labelling of information must be performed to promote the sensitivity of information being shared.

29. Software and Systems Security Policy

29.1 Objective

- This policy establishes guidelines for building security into information systems including infrastructure, business applications and support applications. This policy also outlines controls to be incorporated when securing NIA's (New India Assurance) information systems.

29.2 Security requirements of information systems

Security requirements analysis and specification

- Security requirements in an information system shall be identified and documented during the requirements gathering and analysis phase of acquisition, development or change of information systems. These requirements shall be justified and agreed with business process owners. Security requirements such as the following must be identified but not limited to:
    - User authentication requirements
    - Access authorization and privileged-access management
    - Protection of information assets
    - Logging and monitoring
    - Encryption of data in storage
- Systems security requirements shall reflect the business value of the information assets involved and the potential damage that may be caused due to absence of sufficient security.

Securing applications on public networks

- Information involved in application processing must be secured from fraudulent activity and unauthorized disclosure/modification when transferred over public networks.
- Secure end-user authentication and authorization must be ensured over public networks for any application-related access provisioning.
- Appropriate measures must be deployed to secure online payment transactions using certified verification and settlement techniques.

29.3 Protecting application transactions

Input data validation

- Input controls shall be designed into applications and database systems to validate the correctness and appropriateness of data input fields.

Control of internal processing

- Processing controls shall be designed into applications and database systems to detect corruption of information whether resulting from processing errors or deliberate acts.
- Electronic signatures and encryption techniques must be used to ensure confidentiality and integrity of transactions is maintained and privacy of communicating parties is retained. Controls need to be deployed in accordance with the criticality and level of risk associated with the underlying transactions.
- Transaction information must be protected and stored on a medium not exposed to public networks.

Output data validation

- Output controls shall be designed into applications to validate the correct and appropriate processing of stored information.

29.4 Security of System Files

Control of operational software

- Installation of unauthorized software on operational systems must be controlled using preventive and monitoring mechanisms. Software installation should be carried out only using the operational change management procedure with adequate approvals.

Access control to program source code

- Program source code available with NIA shall be stored under restriction and only authorized personnel shall have access to the same.

29.5 Security in development and support processes

Secure Development Policy

- Security of development environment must be maintained by ensuring security requirements are addressed in software development methodology and use of secure coding guidelines. Secure coding standards like OWASP, NIST, CERT, CWE, MITRE, etc. must be mandated for use wherever possible and must be verified by testing and code review process.
- Information security must also be addressed in version control of source code and maintaining secure application repositories with proper access control and authorization measures.
- Security checkpoints must be identified to ensure annual checks are performed to meet security requirements.
- Development team must develop capability to proactively detect, document and fix technical vulnerabilities in the application development methodology.
- If software development is outsourced to a third-party, NIA shall ensure that secure development policy is adhered to for development of NIA infrastructure.

Secure coding guidelines

- The goal of secure coding is to build security measures in all NIA information systems to reduce vulnerabilities throughout the architecture and minimize risks arising from single point of failures. All NIA information systems shall be compliant with the below guidelines. Any exceptions shall be reported to the Head/GM of Technology Management Team for approval.
- Credentials required for authentication of application users and administrators to ensure individual ownership must not reside in the main body of the program source code. Credentials shall also not be stored under the document root of web servers.
- Applications shall not print, display or reveal user credentials through any mechanism.
- Successful authentications, failed authentication attempts and failed attempts to escalate privileges or exceed authorization shall be recorded in the audit log including timestamp, user ID (Identity Document), source address of login and description of the event.
- Service or functional accounts created for applications shall only have access to configuration data and other required resources.
- Database accounts shall have access only to the database, tables and actions required by the relevant applications.
- User accounts shall have appropriate access within applications to only the tasks required by their functional roles.
- Only super user accounts shall have access to all applications functions and shall be setup in accordance with the NIA Access Control Policy.
- ‘Home grown’ session management or custom session keys shall be prohibited. The application shall accept only those session IDs (Identity Document) created by itself. Sessions must not be based on credentials that may be forged such as source IP (Internet Protocol), name of DNS (Domain Name Server), HTTP (Hyper Text Transfer Protocol) headers, etc.
- Session IDs (Identity Document) shall be generated after a user has authenticated into the application and shall be replaced whenever the user’s role changes. Sessions must expire to log out the user after a fixed amount of inactivity as defined in the NIA Access Control Policy. Upon session termination, all user credentials must be removed from the application memory, cache, temporary files or other memory store.
- Sessions shall be managed by the application in a way that it can withstand replay-attacks.
- Inputs received from external entities from the application front-end must be validated using rules before they are used by the application.
- Cryptographic algorithms used in applications shall be approved with the Head/GM of Technology Management Team and shall comply with the requirements enlisted in NIA (Identity Document) Cryptography Policy.
- Effective error handling must be employed for error/ exception handling across the application. All applications shall fail in a safe/ secure mode.

- Debugging information, stack traces, file system information, server or database identification, credentials, system error codes or any other form of information useful in exploiting the application shall not be revealed to the end-user.

System change control procedures

- Formal procedures shall be followed for change management. All proposed system changes shall be authorized and reviewed to verify that they do not compromise security of either the system or the operating environment.
- All the changes should have a defined implementation plan which includes but is not limited to Implementation steps, Downtime requirements/Project plan, Test plan and Roll back Plan

Technical review of applications after operating system changes

- Business critical applications shall be reviewed and tested prior to installation of OS (Operating System) patches or updates in a test environment in order to ensure that there is no adverse impact on information security aspects of the application due to the changes in the operating system.

Restrictions on changes to software packages

- Modifications to software packages shall be discouraged. As far as possible, and practicable, vendor-supplied software packages shall be used without modification.
- All necessary modifications (including configuration changes, changes to reports, etc.) to software packages shall be made in accordance with formal change management procedures.

Secure system engineering principles

- Security should be designed into all layers of engineering architecture (application, data and technology). Secure engineering areas of secure authentication techniques, session control and data validation must be considered across all information processing system development.
- Robust input validation controls, processing and output controls needs to be built in to the application. Validations should be included on all critical pages so that attacks are minimized and no manipulation can be allowed to change data at source
- Critical Applications to provide for, logging unsuccessful logon attempts, access to sensitive options in the application, e.g., master record changes, granting of access rights, use of system utilities, changes in system configuration, etc.
- The audit trails need to be stored as per a defined period as per any internal/regulatory/statutory requirements and it should be ensured that they are not tampered.
- The developed security engineering principles should be applied to third party information systems through the contractual agreements between the organization and the vendor to have assurance of vendor’s compliance to its secure engineering principles.

Secure development environment

- NIA shall maintain a secure development environment comprising of adequate controls associated with system development and integration.
- Sensitivity of processed data, internal and external requirements, security policies and controls, trustworthy personnel, management of segregation of duties, and security in various operational procedures must be incorporated on premise and across vendor development locations to maintain high standards of secure development.

Information leakage

- Controls shall be implemented and monitored to prevent information leakage for critical business applications.

Outsourced software development

- All outsourced software development activities shall be supervised and monitored by NIA in an ongoing manner for compliance to NIA's (New India Assurance) information security requirements.
- NIA shall obtain application integrity statements in writing from the application system vendors providing for reasonable level of assurance about the application being free of malware at the time of sale, free of any obvious bugs, and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done).

System security testing

- Testing of security functionality shall be performed along with functional testing by the development team during system acceptance testing to ensure secure development principles are designed, implemented and operating effectively.

System acceptance testing

- System acceptance testing must be performed for any change to all information systems and must involve detailed testing of integrated systems to ensure completeness and appropriate synchronization of functionality.

29.6 Protection of test data

- Test data should be selected based on predefined criteria.
- Personally identifiable data or confidential data should not be used for testing purposes.
- Separate authorization must be procured for each attempt to move operational information to test environment.

29.7 Technical vulnerability management

Control of technical vulnerabilities

- NIA shall ensure that technical vulnerabilities on the information systems being used are identified, based on the criticality of the systems.

- Further, NIA shall ensure that the organization's exposure to such vulnerabilities is evaluated, and appropriate measures are taken to address the associated risk.
- Systematic vulnerability assessment and penetration testing activities must be conducted by Information Security Risk Management Team for critical infrastructure annually to ensure technical vulnerabilities are recorded across NIA’s (New India Assurance) information systems and appropriately addressed. External consultants may be employed for such activities and the program must be followed-up with Information Security Risk Management Team for compliance.

30. Application Security Policy

30.1 Objective

- The objective of this policy is to build guideline for secure input, processing, storage and output of data used by all the applications deployed at NIA.

30.2 Applications Security

Ownership and Responsibility of Applications

- Each application shall have a designated owner who will be responsible for the confidentiality, integrity and availability of the application and the associated data

Access Request

- User access to applications shall be based on the principle of least privilege and a need to know as per the NIA Access Control Policy.
- Access to each application including servers, databases and the application itself shall be authorized by the respective application owner.
- Application owner shall maintain a list of authorized users along with their role i.e. End User, Super User, Admin User, Database User etc.
- Application owner shall maintain an access control matrix which includes a list of users’ roles and their corresponding access rights
- Adequate segregation of duties shall be maintained by the application owners to minimize the risk of negligent or deliberate system misuse

Data Security

- All the data communication, validation and processing within the application and with other applications shall be configured in a secure manner.
- Application shall have adequate input data validation, processing and output data validation features.
- Application owner shall ensure that the data being used by application is stored, transmitted and processed in a secure manner to comply with the regulatory and/or internal requirements. Additional measures shall be implemented in case the application deals with customer, cardholder or Personally Identifiable Information.
- Where data is being exchanged using an interface control, application owner shall ensure that adequate security controls are in place

Audit Trails and Logging

- Application owner shall ensure that the application is able to log the transactions and administrative actions, which are adequate to serve as a reference in case of any investigation for misuse of the application and/or debugging the errors in the application.

Web Applications

- Application owner shall ensure that web applications being accessed over the internet/intranet have adequate security controls configured to avoid misuse of these applications.

Risk Assessment

- Application owners shall ensure that annual risk assessment exercise is conducted for each application.
- Such Risk assessment exercises shall at a minimum include the following aspects:
    - Asset Identification and Classification
    - Compliance to Information and Cyber Security Policy
    - Threat and Vulnerability Assessment
    - Penetration Testing
- Application owners shall consult the Information Security Officer to develop and implement risk treatment plans for the identified risks.

31. Platform/Infrastructure Security Policy

31.1 Minimum Baseline Security Standards

- The configuration shall be based on Minimum Baseline Security Standards (MBSS). NIA shall develop baseline MBSS based on OEM's recommendations and industry best practices like CIS, NIST, OWASP, CERT, STIG, etc. MBSS should be prepared for the following list (but not limited to) of components
- Operating Systems (Servers & End points – Laptop, Desktops)
- Web Server software (Tomcat, IIS, Apache HTTP (Hyper Text Transfer Protocol), IBM HTTP and Oracle HTTP, etc.)
- Application Server software (Weblogic, etc.)
- Database Servers (Oracle, MS-SQL, MySQL, PostgreSQL,etc.)
- Network Components (Routers, Wireless Access Points, etc.)
- Security Devices (Firewalls, VPNs (Virtual Private Network), IDS (Intrusion Detection System), IPS (Intrusion Prevention System), etc.)
- Wireless
- MBSS (Minimum Baseline Security Standard) should be reviewed for currency on a periodic basis by Information Security Team. The exceptions to configurations as recommended in MBSSs owning to certain business requirements/limitations should be approved through formal exception process after adequate risk assessment.
- The IT infrastructure should be subject to configuration review (vulnerability assessment/penetration tests) against defined MBSSs on a periodic basis.
- Regular scheduled assessments, such as internal and external vulnerability scans should be conducted for the IT (Information Technology) Infrastructure including but not limited to software, applications, server, network, database, operating system, wireless devices, and other network equipment.
- Frequency of conducting vulnerability assessment shall depend upon the criticality of the Information Asset (application, software, database, operating system, network devices and wireless networks). All Internet facing applications shall undergo vulnerability assessments before deployment in the production environment.

32. Database Security Policy

32.1 Objective

- Databases are crucial component of information systems wherein data is stored, transmitted and processed. To ensure that confidentiality, integrity and availability of data residing on the NIA databases, effective security measures must be implemented.

32.2 Protection of databases

- Database administrators shall document procedures for performing administration activities such as installation and patching of software and firmware, manage storage and processing utilization, maintain data structures, changes in configuration, backup and restoration and troubleshooting errors encountered in usual operations, etc.
- NIA shall ensure that the number of users having administrator privileges at database level shall be restricted to minimum.
- Database administrators must ensure that users' access to the database is given on a need-to-know basis consistent with their job functions and relevant authorization.
- Database administrators must ensure that all accesses are managed using the procedures defined as part of NIA's Access Control Policy.
- The use of Privileged Identity Management solution shall be considered for granting secure access to databases, and logging of all events and activities performed by database users and administrators.
- NIA shall ensure that all the databases shall be upgraded to the latest or last supported versions provided by the database vendor. However, in case of dependency of compatibility with applications, exceptions by the respective Department Chief Manager and the Head/GM of Information Security Risk Management Team should be taken.
- All information, software and log files on firm databases essential for the continued operations of NIA shall be identified, documented and backed up as per defined frequency.
- NIA shall ensure that suitable documented backup/recovery procedures shall be in place, which shall cover type of backups to be performed, respective teams and their responsibilities, periodicity of backups, location for offsite storage of backup media, and restoration testing.
- The off-site location for secure storage of backup media shall have appropriate environmental and physical security controls similar to those at the primary data center site.
- NIA shall ensure that security patches shall be applied across all databases as soon as they are made available and tested before being deployed to production network
- NIA shall ensure that access to stored procedures on databases is controlled to authorized individuals using appropriate access control mechanisms.

- NIA shall ensure that databases shall be configured as per Minimum Baseline Security Standards (hardening standards) maintained by the firm for the respective database technology.
- NIA shall ensure that vulnerability scanning of databases shall be carried out on an annual basis for identification and treatment of various vulnerabilities.
- NIA shall ensure that logging of all activities shall be enabled on databases which must be reviewed on a quarterly basis for identification of unauthorized activities.
- NIA shall ensure that all changes to the databases shall be performed in line with NIA's defined change management process.
- Database owners shall ensure that all operational activities are being performed by database custodians in accordance with the policies and procedures defined in NIA's Information Security Management System.
- Direct back-end updates to database should not be allowed except during exigencies, with a clear business need and after due authorization as per the relevant policy.

33. Anti-virus Policy

33.1 Objective

- The objective of this policy is to ensure adequate protection of NIA information systems and resources against malwares and viruses.

33.2 Anti-virus and anti-malware security

- All desktops, laptops, server machines and other IT (Information Technology) infrastructure at NIA shall have an anti-malware/ anti-virus software installed which is updated with the latest signatures/patches.
- NIA shall ensure that the mobile devices and laptops are updated with the latest anti-virus and anti-malware signatures.
- All portable firm devices such as tablets, mobile devices and laptops should be checked for viruses and malware before being connected to NIA's (New India Assurance) corporate network.
- NIA should perform an assessment of the specifications and features of various anti-virus products and mandate the use of approved software across all firm devices.
- A centralized anti-virus server engine should be setup in the firm's data center which shall automatically push updates to all client software agents installed on end-point devices as soon as they are connected to NIA corporate network.
- NIA shall ensure that the antivirus software deployed on the NIA endpoints scan the devices for viruses, trojans and malicious software that could compromise the confidentiality, integrity or availability of NIA's critical business information.
- Users, both employees and vendors, shall be educated for the effects and implications of viruses new signatures shall be applied as soon as they are released by vendor.
- Users shall be educated to communicate any issues regarding connectivity to anti-virus server engine or potential compromise of device with viruses or malware to the NIA IT team NIA end-users shall connect their firm-provided devices to the corporate network as frequently as possible or at least once every quarter to ensure timely download of all anti-virus patches and update of their end-point software firmware.
- The anti-virus and anti-malware software shall be kept enabled on all firm devices at all times.
- The anti-virus and anti-malware software installed on all NIA end-points shall be configured to scan all portable devices connected to them such as portable hard-drives, USB (Universal Serial Bus) flash-drives, etc.
- The anti-virus and anti-malware software installed on all NIA end-points shall be configured appropriately to ensure that the end-user cannot manipulate virus and malware scan settings and other software permissions on the system.
- Backup of anti-malware/ anti-virus application/server configuration and log files shall be taken as per a defined frequency.

- Any critical change regarding the anti-malware/ anti-virus application and configuration settings shall follow the organization’s Change Management procedure.
- Service Level Agreements shall be maintained with the vendor for software upgrade and technical support for the anti-malware/anti-virus software.

33.3 Data Migration Policy

33.4 Objective

- NIA has and shall continue to upgrade/modify its technological infrastructure which hosts a range of information owned by NIA v. As the infrastructure undergoes a change, such information also needs to be migrated to the new systems and be transformed in line with the new system requirements.
- The objective of this policy is to safeguard information and NIA’s business operations while performing migration of data across varied technology platforms.

33.5 Data migration

- The Business Department from which the data migration requirements originate shall develop a plan with detailed information stating the pre and post migration activities along with responsibilities and timelines.
- Explicit sign off from the Department Chief Manager shall be obtained after completion of each stage of migration activity.
- End-users are responsible for cleaning and sensitization of information resources before a migration.
- Data conversion shall be validated by a department designated person or an appointed auditor to ensure completeness and integrity of data.
- IT (Information Technology) team or other designated personnel shall ensure the integrity of data during a migration activity.
- Audit logs shall be maintained and monitored for data mappings and transformations.
- NIA shall perform a post-migration validation to verify that the data has been migrated as intended, and that the access-rights and folder permissions for the data have been replicated as well at the target storage location.
- NIA shall ensure that the migrated data is tested and validated to be accurate, and that the entire data migration process meets the policy requirements outlined during planning stage.
- NIA shall ensure adequate controls are implemented to ensure data integrity and confidentiality during/after data migration and its completeness shall be verified.
- The IT Team or relevant vendor personnel shall at a minimum, consider the following aspects during the data migration:
  - Confidentiality of the data being migrated
  - Integrity of the data being migrated
  - Completeness and Accuracy of the data being migrated

  - Consistency of the data – Pre and Post Migration
  - Availability and Continuity of the data – Pre and Post Migration
- The Department Head/GM shall maintain the last copy of data before conversion from the old platform and first copy of data after conversion to new platform separately in the archive for future reference.

34. Cryptography Policy

34.1 Objective

- To ensure that NIA's (New India Assurance) critical information is protected from unauthorized disclosure and misuse by use of appropriate encryption mechanisms.

34.2 Policy statement

Determination of encryption requirements

- The information assets and applications that require encryption controls shall be identified.
- Cryptographic controls shall be used and documented, where required, for securing sensitive information residing within NIA premises, or being transferred over NIA/ vendor networks.

Product selection and deployment

- Encryption algorithms suitable for NIA's business and information security needs shall be identified and a list shall be maintained by Head/GM of Technology Management Team for all approved encryption algorithms, along with the acceptable key length for each.
- It shall be ensured that only the approved encryption software and cryptographic products are being used in NIA information systems.
- The type and strength of the encryption algorithm to be used in a given situation shall be based on the criticality of the business information handled.
- Access to encryption software and encryption keys shall be restricted and shall be made available only to authorized personnel.
- Digital signatures/certificates shall be acquired from the Certificate Authority (CA) licensed by the Controller of Certifying Authorities (CCA) India.

Defining roles and responsibilities

- The owners and custodians for the encryption software and keys shall be clearly defined in the Asset Registers for all encryption software being used by NIA.
- Split knowledge and dual control should be implemented for encryption keys, in order to prevent their unauthorized substitution, revocation or misuse.

Encryption key management

- To ensure secure management of encryption keys, wherever possible, only individuals that are not directly involved with the operational use of the keys shall be allowed to create the keys.
- Master keys for symmetric key/asymmetric key pair generation must be secured in a manner such that no one individual party is privy to the entire master key, wherever applicable

- The encryption keys shall be stored and archived in a secure manner to minimize the chances of their unauthorized access and misuse.
- Key backup process shall enable key recovery, but should not compromise key confidentiality and integrity. Request for recovery of keys/key pairs shall be made via a formal process that includes approval from competent authority.
- Only secure communication channels shall be used for distribution of encryption keys and the keys shall never be transmitted in an un-encrypted format.
- The encryption keys that are lost or compromised shall be revoked as per defined revocation procedures; and all stakeholders shall be promptly notified.
- Credentials of requesters shall be verified before sharing encryption keys and for ascertaining the authenticity of the counterparty before establishing a trusted path.
- Reviews shall be conducted on an annual basis to ensure that controls exist for protecting encryption keys. The reviews shall verify adherence to the guidelines for generation, change, distribution, revocation, destruction, certification, storage, archiving and usage of encryption keys.

Encryption Key Retention

- Data encryption keys – symmetric/asymmetric keys used for encryption shall be available as long as any information protected (encrypted) by the keys needs to be decrypted.
- Digital certificate verification – a public key shall be available as long as any information signed with the associated private key is maintained.
- Master key used to derive other keys – master keys shall be available as long as there is a requirement to recreate derived keys in the future.
- Keys used to generate hash algorithms – keys used to generate hash algorithms shall be available as long as there is a requirement to prove or otherwise the validity of a previously generated hash value.

35. Information Security Incident Management Policy

35.1 Objective

- To define procedures for effectively managing incidents related to Information Security, and reporting and escalation of information security events and weakness associated with information systems in a timely manner allowing timely corrective action to be taken.
- The goal is to restore normal service operation quickly and efficiently, to minimize the adverse impact on DC (Data Center) and DR (Disaster Recovery) operations, and to ensure that the best possible levels of service, quality, and availability are maintained.

Management of information security incidents and improvements

- NIA shall establish management responsibilities and procedures to handle information security incidents in a quick, effective and orderly manner.
- A knowledge base of the incidents occurred should be maintained along with the lessons learned and steps for resolution

Reporting information security events and weaknesses

- An Incident is defined as the occurrence of any exceptional situation that could compromise the Confidentiality, Integrity or Availability of Information and Information Systems of NIA. It is related to exceptional situations or a situation that warrants intervention of senior management, which has the potential to cause injury or significant property damage.
- Security weaknesses (vulnerability in the information system, which could be exploited to compromise the Confidentiality, Integrity or Availability of the system), software malfunctions (any abnormality or deviation in the functioning of a software application) and violations of NIA’s (New India Assurance) information security policies and procedures shall also be reported using the incident management procedure.
- NIA shall implement procedures for detecting & reporting security events through appropriate channels as quickly as possible.
- All employees, contractors and third party users of information systems shall be required to note and report any observed or suspected security weaknesses in systems.

Managing incidents

- The Information and Cyber security incident classification criteria shall be documented. Security incidents shall be classified based on the criticality and Severity. NIA should develop and maintain a comprehensive Cyber crisis management plan for Incident and Cyber Crisis.
- NIA shall implement procedures for responding to incidents related to exceptional situations in day-to-day administration of the IT (Information Technology) and information security related areas.

- The incidents shall be reported in time to the appropriate authorities and corrective actions shall be taken immediately to avoid the recurrence of such events in future.
- All contractors and third parties shall also be made aware of the procedures for reporting different types of incidents (like security breach, threat, weakness, or malfunction) that might have an impact on the security of NIA's (New India Assurance) assets.
- All reported incidents shall be logged, analyzed and classified according to predefined criteria.
- Escalations and actions shall be as per the classification of incidents.
- If need be, NIA may coordinate response and share information about incidents with external organizations
- Knowledge gained from analyzing and responding to security incidents must be documented and shared with appropriate stakeholders. This information must be easily accessible and reusable across the organization to manage repeat incidents or incidents of similar nature in the future.
- Incidents, classified as High or Critical, should be reported to CISO, CIO (Chief Information Officer), CRO (Chief Risk Officer) and other relevant stakeholders including CERT-in & CERT-Fin.

Contacts with Authorities

- Appropriate contacts with relevant authorities shall be maintained to escalate to the respective authorities as required.

Collection of evidence

- NIA shall define procedures for identification, collection, acquisition and preservation of incident management information, which can serve as evidence for purposes of disciplinary and legal action.

36. Business Continuity Management Policy

- A business continuity management process shall be implemented to minimize the impact of and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls.

36.1 Information Security Requirements

- Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
- A single framework shall be defined to ensure that business continuity plans for identified critical business processes are consistent with the organization’s information security policy and identifies priorities for testing and maintenance.
- A Business Continuity Governance Structure shall be developed to implement, exercise, oversee and improve business continuity controls at NIA.
- Adequate BCP (Business Continuity Planning) training programs and awareness sessions should be conducted

36.2 Business Impact Analysis

- NIA shall identify all business-critical processes in the organization that can cause significant financial and non-financial impact to the firm.
- Business Impact Analysis (BIA) should be performed for the identified critical business processes to identify parameters such as Recovery Time Objective, Recovery Point Objective and Maximum Tolerable Period of Disruption for each identified process.
- A risk assessment shall be performed to assess the impact of various internal and external threats on the critical business processes to identify areas of significant importance.
- Based on the results of the BIA, Business Continuity Plans and IT (Information Technology) Disaster Recovery Plans shall be developed by Process and IT Application Owners respectively outlining the people, process and technology requirements. Functional Recovery Strategies shall outline the measures, protocols, people involved and their responsibilities to ensure their continuity of the business processes in case of a disaster.
- NIA shall identify an Emergency Command Center to centrally coordinate management response in the event of a disaster.

36.3 Testing, maintain and reassessing of Business Continuity plans

- The Business Continuity Plans defined at NIA shall be reviewed and updated annually.

- A test schedule shall be maintained to indicate how and when each element of the plan shall be tested. Business Continuity Plans for all critical business processes shall be tested at least annually.

36.4 Availability of information processing facilities

- NIA shall identify business requirements for availability of information systems as part of the Business Continuity Plans.
- Where availability cannot be guaranteed using existing architecture, redundant architectures or components must be considered to act as a fail-safe control.

37. Audit and Compliance Policy

37.1 Compliance with legal, regulatory and contractual requirements

- Identification of applicable legislation
- All applicable statutory, regulatory and contractual requirements, pertaining to IT/Information Security shall be identified and documented explicitly by the Head/GM (General Manager) of Information Security Risk Management Team. Where applicable, the policy and procedures shall include and abide by the applicable laws.
- Specific controls to meet these requirements shall be identified and implemented. This shall include but not be limited to the IT Act 2000 (Information Technology Act 2000) and any other laws or acts applicable to NIA.

37.2 Intellectual Property Rights

- The terms and conditions and license requirements of the copyrighted software or any other proprietary information used within NIA shall be complied with.

37.3 Protection of Organizational Records

- NIA's (New India Assurance) important records relating to information security shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

37.4 Data protection and privacy of personal information

- Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses for each business.

37.5 Regulation of cryptographic controls

- NIA shall ensure that cryptographic controls used by the firm are compliant with relevant contractual agreements as well as legislation and regulations.

37.6 Compliance with Security Policies and standards and Technical Compliance

- Department Chief Managers and office in-charge shall ensure that security procedures within their area of responsibility are performed correctly in accordance with security policies and standards.

Independent Technical Compliance Review and Reporting

- Information processing resources and associated documentation shall be reviewed on an annual basis to verify that they are compliant with the security policies and standards. Findings and recommendations in the report shall be directed to the relevant department personnel for implementation.

37.7 Information Systems Audit Considerations

- Internal Audit team of NIA shall have a separate IS audit plan covering IT/Technology infrastructure and applications. The audit plan and the reports shall be presented to the Audit Committee of the Board
- Internal audit team shall conduct audit for third party /vendors handling critical data on planned and ad hoc basis to measure the effectiveness of the third party security controls implemented.
- NIA shall conduct annual audits by competent party to ensure compliance with the information security policies, procedures, standards and guidelines.
- Such audits should test the effectiveness of technical and operational security control measures implemented in IT networks and systems.
- Audits performed shall include cyber security assessment of NIA information systems to comply with regulatory requirements.
- Procedures shall be followed for planning and reporting audits and audit findings and ensuring the implementation of a prompt and accurate remedial action.
- Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
- VA and PT exercises shall be conducted annually for critical infrastructure by an independent function within NIA or an external agency.
- All instances of non-compliance related to Information security shall be communicated and discussed with relevant line management and CISO.

38. List of abbreviations

Abbreviations	Meaning
NIA	New India Assurance
CISO	Chief Information Security Officer
CIO	Chief Information Officer
CRO	Chief Risk Officer
MISC	Management Information Security Committee
DC	Data Center
DR	Disaster Recovery
HR	Human Resource
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IP	Internet Protocol
ISPP	Information Security Policies and Procedures
ISRMT	Information Security Risk Management Team
IT	Information Technology
SGT	Strategy and Governance Team
TMT	Technology Management Team
VPN	Virtual Private Network
ISDN	Integrated Services Digital Network
LAN	Local Area Network
WAN	Wide Area Network
HTTP	Hyper Text Transfer Protocol
IT	Information Technology
OEM	Original Equipment Manufacturer
ID	Identity Document
IRDAI	Insurance Regulatory and Development Authority
USB	Universal Serial Bus
GM	General Manager

CCMP	Comprehensive Cyber crisis Management Plan
DLP	Data Loss Prevention
HR	Human Resource
IRM	Information Risk Management
ISC	Information Security Committee
NDA	Non -Disclosure Agreement
OEM	Original Equipment Manufacturer
PII	Personally identifiable information

Appendix 1 – Templates

Sr. No.	Name of record	Template
1	Information Security Policy Exception Form	NIA ISMS- L4- 1.1 - Information Security I
2	Agreement to comply with the ISPP of NIA	NIA ISMS- L4- 1.2 - Agreement to Comply
3	Non-Disclosure Agreement	NIA ISMS- L3- Non-Disclosure Agree