NATIONAL PENSION SYSTEM TRUST

Information and

Cyber Security Policy, 2023

Vision

The information and cyber security policy of NPS Trust envisions for a secure and resilient information and cyber security framework at NPS Trust.

Executive Summary

a) The policy’s objective is to provide management direction and support for implementation of information and cyber security system to address security threats and implement strategies to mitigate IT security vulnerabilities, as well as strengthen cyber defense and build strong resilience, in accordance with NPS Trust’s requirements, relevant laws and regulations.

b) NPS Trust’s information and cyber security policy shall be a collection of statements, designed to guide employees’ behavior regarding the security and integrity of networks, programs, data, assets and IT systems from unauthorized access, cyberattacks and damages.

c) The policy shall identify the rules and procedures that all employees accessing and using the organization’s IT assets and resources must follow, in order to help protect the confidentiality, integrity and availability of information i.e., organization’s data and other valuable assets, and protect and defend theuse of cyber space from cyberattacks on a continuous basis.

d) NPS Trust shall establish a management framework to initiate and control the implementation and operation of information and cyber security within the organization.

e) Policy implementation shall strengthen cyber defense and build strong resilience with risk assessment, awareness, education and training on information and cyber security.

f) Policy shall emphasize on information and operational security, IT and related secure asset handling, access control, backup solutions with extended utilities and environment controls.

g) Policy shall determine the importance of Business Continuity Plan (BCP) in case of the natural or man-made disaster with redundancies and Business Continuity Management.

h) Appropriate contacts and coordination with relevant authorities and interest groups like NCIIPC, IDRBT, CERT-In, NTRO, etc., shall be maintained.

i) Policy shall recommend the compliance need with respect to legal, statutory, regulatory and contractual obligation. NPS Trust’s objectives, policies, process, procedures, and controls shall enable information and cyber security with resilience.

The policy shall be reviewed periodically to address any non-conformities or insights gained from any corrective actions.

Introduction

The present world is rapidly becoming more digitalized and hence, become reliant on data and increasingly more interconnected. In an interconnected world, information and associated process, systems, networks and personnel involved in the operation are valuable to an organization's business and consequently deserve or require protection against various hazards. The fast pace of adoption of technological innovations have increased exposure to cyber incidents underlining the need to have a robust information and cyber security framework. Cyber incidents and attacks have increased in frequency in recent past. Hence, it is essential that the financial system enhances cyber resiliency through the individual action of financial institutions and through increased coordination across participants, including the sharing of information and developing a set of commonly understood rigorous practices through adoption of information and cyber security plan and crisis management plan. The information technology sector which thrives on cyber space, plays a significant role in influencing and improving the lives of people through direct and indirect contribution to the delivery of various services. Such a focus necessitates creation of a suitable cyber security eco-system in the country, in tune with globally networked environment. Cyberspace is a complex environment consisting of interactions between people, software, services, and supported by worldwide distribution of information and communication technology (ICT) devices and networks.

The mission of India's National Cyber Security Policy -2013 is to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities, and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology, and cooperation. The NCSP mandates all government organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. The policy should aim to establish standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

1. NPS Trust shall establish an information and cyber security policy that:

a. Is appropriate to the purpose of the organization;
b. Includes information and cyber security objectives;
c. Includes a commitment to satisfy applicable requirements related to information and cyber security;
d. Includes a commitment to continuous improvement of the information and cyber security management system.

2. The information and cyber security policy shall:

a. Be available as documented information with simple explanation;
b. Be communicated within the organization; and
c. Be available to interested parties, as appropriate.

3. Context of the organization:

3.1 NPS Trust shall determine external and internal issues that are relevant to its purposeand that affect its ability to achieve the intended outcome(s) of its information cyber security management system.

3.2 NPS Trust shall determine:

a. The interested parties that are relevant to the information security management system;
b. The requirements of these interested parties relevant to information and cyber security, which may include legal and regulatory requirements and contractual obligations;
c. The boundaries and applicability of the information and cyber security management system to establish its scope.

4. Information security management system

NPS Trust shall establish, implement, maintain, and continually improve the information and cyber security management system in accordance with the requirements.

5. Leadership and commitment

NPS Trust shall demonstrate leadership and commitment with respect to the informationand cyber security management system by:

a. Ensuring the information and cyber security policy and the objectives are compatible with the strategic direction of the organization;
b. Ensuring the integration of the information and cyber security management system requirements into the organization’s processes;
c. Ensuring that the resources needed for the information and cyber security management system are available;
d. Communicating the importance of effective information and cyber security management and of conforming to the information and cyber security management system requirements;
e. Ensuring that the information and cyber security management system achieves its intended outcome(s);
f. Directing and supporting employees to contribute to the effectiveness of the information and cyber security management system;
g. Promoting continual improvement; and
h. Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

6. Organizational roles, responsibilities, and authorities

NPS Trust shall ensure that the responsibilities and authorities for roles relevant to information and cyber security are assigned and communicated for reporting on the performance of the information security management system within the organization.

7. Information and cyber risk assessment

NPS Trust shall define and apply the information and cyber security risk assessment process that establishes and maintains information security risk acceptance criteria and criteria for performing information security risk assessments to ensure that repeated information security risk assessments produce consistent, valid, and comparable results. The aim shall be to identify, analyse and evaluate the information and cyber security risks. NPS Trust shall retain documented information about the information security risk assessment process.

8. Awareness

The employees of NPS Trust shall be aware of:

a. The information and cyber security policy;
b. Their contribution to the effectiveness of the information and cyber security management system, including the benefits of improved information and cyber security performance; and
c. The implications of not conforming to the information and cyber security management system requirements.

9. Documented information

NPS Trust's information and cyber security management system shall include documented information necessary for its effective implementation. Creating and updating documented information of NPS Trust shall be ensured appropriately.

For the control of documented information, NPS Trust shall address the following activities, as applicable:

a. Distribution, access, retrieval, and use;
b. Storage and preservation, including the preservation of legibility;
c. Control of changes (e.g., version control); and
d. Retention and disposition.

NPS Trust shall ensure that outsourced processes are determined and controlled.

NPS Trust shall evaluate the information and cyber security performance and the effectiveness of the information and cyber security management system. NPS Trust shall monitor, measure, analyze and evaluate the process and controls.

The internal audit shall be conducted at planned intervals, preferably twice a year, to provide information on whether the information and cyber security management system conforms to the policy and is effectively implemented and maintained.

10. Periodical review of policy

The information and cyber security policy should be reviewed at planned intervals, preferably once a year, to ensure its continued suitability, adequacy, and effectiveness.

10.1 Non-conformity and corrective action

NPS Trust shall review the existing information and cyber security management system in order to address any non-conformity with the policy in order to take suitable corrective action, if necessary and shall document the same.

10.2 Continual improvement

NPS Trust shall continually strive to improve the suitability, adequacy and effectiveness of the information and cyber security.

11. Management framework for information and cyber security management

11.1 Internal organization

NPS Trust shall establish a management framework to initiate and control the implementation and operation of information and cyber security within theorganization.

a. Role and responsibilities

All information and cyber security responsibilities shall be defined and allocated.

b. Segregation of duties

Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the NPS Trust’s IT and related assets.

c. Contact with authorities

Appropriate contacts and coordination with relevant authorities like NCIIPC, IDRBT, CERT-In, NTRO, etc., shall be maintained.

d. Contact with special interest groups

Coordination with special interest groups or other specialist security forums and professional associations viz CISO’s forum, product specialist etc., shall be maintained.

11.2 Mobile devices and teleworking

NPS Trust shall ensure the security of teleworking and secure use of mobile devices.

A policy and supporting security measures shall be adopted to manage the risks associated with using mobile devices and to protect information accessed, processed, and stored at teleworking sites.

12. Human resource security

12.1 Prior to employment

a. NPS Trust shall ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are engaged, prior to employment;

b. Background verification checks of all employees shall be carried out in accordance with relevant laws, regulations, and ethics. Employees are to be assessed as per the perceived risks;

c. The contractual agreements of NPS Trust with employees and contractors shall state the employees and the organization's responsibilities for information and cyber security.

12.2 During employment

NPS Trust shall ensure that employees and contractors are aware of and fulfil their responsibilities as per the information and cyber security policy.

a. Management responsibilities

NPS Trust shall ensure all employees and contractors adhere to information and cyber security policy in accordance with the established policies and procedures of the organization.

b. Information and cyber security awareness, education, and training

All employees of the organization and, where relevant, contractors shall receive appropriate awareness education, training and regular updates on organizational policies and procedures, as relevant to their job function.

c. Disciplinary process

There shall be a formal and communicated disciplinary process in place to act against employees who commit an information and cyber security breach.

12.3 Termination and change of employment

NPS Trust shall protect the organization’s interests as part of the process of changing or terminating employment. Information and cyber security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor, and enforced.

13. Communications security

13.1 Network security management

NPS Trust shall ensure the protection of information in networks and its supporting information processing facilities.

a. Networks shall be managed and controlled to protect information in systems and applications.
b. Security mechanisms, service levels and management requirements of all network services shall be identified and included in all network services agreements, whether in-house or outsourced.
c. Groups of information services, users and information systems shall be segregated on networks.

13.2 Information transfer

NPS Trust shall maintain the security of information transferred within an organizationand with any external entity as under:

a. Formal transfer policies, procedures and controls shall be in place to protect the transfer of information using all types of communication facilities.
b. Agreements on information transfer shall address the secure transfer of business information between the organization and external parties.
c. Information involved in electronic messaging shall be appropriately protected.

d. Requirements for confidentiality or non-disclosure agreements reflecting the organization’s needs for the protection of information shall be identified, regularly reviewed, and documented.

14. System acquisition, development, and maintenance

14.1 Security requirements of information and cyber security systems

NPS Trust shall ensure the following:

a. The information and cyber security related requirements to be included in the requirements for new information systems or enhancements to existing information systems.

b. Information involved in application services passing over public networks to be protected from fraudulent activities, contract disputes and unauthorized disclosures and modifications.

c. information involved in application service transactions to be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

14.2 Security in development and support processes

NPS Trust shall ensure that information and cyber security is designed and implemented,within the development lifecycle of information systems.

a. Norms for the development of software and systems to be established and applied to developments in the information and cyber security framework within the Authority.

b. Changes to systems within the development lifecycle to be controlled using formal change control procedures.

c. When operating platforms are changed, business critical applications to be reviewed and tested to ensure that there is no adverse impact on organizational operations or security.

d. Modifications to software packages shall be minimal, limited to changes that are necessary and all changes shall be strictly controlled.

e. Security engineering principles for engineering secure systems to be established, documented, maintained, and applied to any information and cyber security system implementation efforts.
f. Establish secure development environments for system development and integration efforts that cover the entire system development lifecycle.
g. The activity of outsourced system development shall be supervised and monitored.
h. Testing of security functionality shall be carried out during system development.
i. Acceptance of testing programs and related criteria shall be established for new information systems, upgrades, and new versions.

14.3 Test data

To ensure the protection of data used for testing, test data shall be selected carefully, protected, and controlled.

15. Supplier relationships

15.1 Information and cyber security in supplier relationships

NPS Trust shall ensure protection of the organization’s assets that is accessible by suppliers.

a. All relevant information and cyber security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for the organization’s information.
b. Agreements with suppliers shall include requirements to address the information and cyber security risks associated with information and communications technology services and product supply chain.

15.2 Supplier service delivery management

NPS Trust shall maintain an agreed level of information and cyber security of services delivered by the suppliers.

a. Regularly monitor, review and audit supplier agreements.
b. The provision of services by suppliers, including maintaining and improving the information and cyber security policies, procedures and controls,

shall be managed, taking account of the criticality of business information, system and processes involved and re-assessment of risks.

16. Information and cyber security incident management

16.1 Information and cyber security incident management

An Information and cyber security incident is either an adverse event in an information system or a network that poses a threat to computer or network security in respectof availability, integrity and confidentiality of information. Examples of adverse eventsare:

- Theft and burglary
- Natural disasters, e.g., floods, typhoons, rainstorms
- Possible hazards from the surroundings
- Data line failure
- System crashes
- Packet flooding
- Unauthorized access or use of system resources
- Unauthorized use of another user's account
- Unauthorized use of system privileges
- Web defacement
- System penetration / intrusion
- Massive virus attacks

However, adverse events such as natural disaster, hardware/software breakdown, data line failure and power disruption etc. should be addressed by a system maintenance and disaster recovery plan instead of an information and cyber security incident plan.

16.2 Management of information and cyber security incidents and improvements

NPS Trust shall ensure a consistent and effective approach to the management of information and cyber security incidents, including communication on security events and weaknesses.

a. Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information and cyber security incidents.
b. Information and cyber security events shall be reported through appropriate management channels as quickly as possible.
c. Employees and contractors using the organization’s information systems and services shall be required to note and report any observed or suspected information and cyber security weaknesses in systems or services.
d. Information and cyber security events shall be assessed and it shall be decided if they are to be classified as information and cyber security incidents.
e. Information and cyber security incidents shall be responded to in accordance with the documented procedures.
f. Knowledge gained from analysing and resolving information and cyber security incidents shall be used to reduce the likelihood or impact of future incidents.
g. Authority shall define and apply procedures for the identification, collection, acquisition, and preservation of information, which can serve as evidence.

16.3 Handling of Information and cyber security Incident

Security incident handling is a set of continuous processes governing the activities that take place before, during and after a security incident occurs. Security incident handling begins with planning and preparing the right resources, then developing the proper procedures to be followed, such as the escalation and security incident response procedures. When a security incident is detected, a security incident response is set in motion by the responsible parties, following predefined procedures. When the incident is over, follow up action is taken to evaluate the incident, strengthen security protection and prevent its recurrence.

16.4 Information and cyber security incident management

Security incident management is the process of identifying, managing, recording, and analyzing security threats or incidents in real-time.

16.5 Preparing for Information and cyber security Incident Management

The ISO/IEC Standard 27035 outlines a five-step process for security incident management, viz.:

a. Prepare for handling incidents;
b. Identify potential security incidents through monitoring and report all incidents;
c. Assess identified incidents to determine the appropriate next steps for mitigating the risk;
d. Respond to the incident by containing, investigating, and resolving it; and
e. Learn and document key takeaways from every incident.

16.6 Security Incident Handling for staff members of NPS Trust

NPS Trust shall document the steps for employees, for incident handling, if they encounter a security incident, such as when virus-scanning software alerts that computer infected with a virus.

17. Information and Operational Security

Information and cyber security policy should address the requirements created by regulations, legislation and contracts, the current and projected information and cyber security threat environment. The policy should be supported by topic-specific policies, which further mandate the implementation of information and cyber security controls.

17.1 Preparedness for Informational and Operational Security at NPS Trust

a. NPS Trust shall ensure that information and information processing facilities are protected against malware. Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

b. A backup policy shall be established to define the organization’s requirements for backup of information, software, and systems.

c. Formal information transfer policies, procedures and controls should be in place to protect the transfer of information using all types of communication facilities.

d. NPS Trust shall define and enforce strict policy on types of software a user is allowed or mandated to install.

e. Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g., what software is installed on what systems) and the person(s) within the organization.

f. If products are acquired from a third party, a formal testing and acquisition process should be followed. Contracts with the supplier should address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls shall be reconsidered prior to purchasing the product. Criteria for accepting products should be defined in terms of their functionality, to assure that the identified security requirements are met.

g. Information and cyber security considerations for application services passing over public networks should include the following:

   i. Authorization processes associated with approval of content, issue resolution, or to sign key transactional documents;
   ii. The protection requirements of any confidential information;
   iii. Selecting the most appropriate settlement form of payment by the Finance and Accounts Department to guard against any possible fraud;
   iv. Ensuring that the storage of confidential documents is not publicly accessible e.g., on a storage platform on the organizational

intranet, and not retained and exposed on a storage medium directly accessible from the Internet; and

v. Official organizational email IDs shall be assigned to all staff barring outsourced and usage of other email services such as Gmail etc. be avoided.

h. Sensitive or critical official information, whether physical or electronic should be properly secured (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.

i. Computers and terminals should be logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism when not in use.

j. Ensuring uninterrupted power supply as frequent and sudden power outages or fluctuations can lead to motherboard crashes and may lead to data corruption. Power backup system such as UPS shall be installed.

k. When using mobile devices, special care should be taken to ensure that business information is not compromised.

l. Password management systems should be interactive and should ensure secure passwords.

m. To protect the organization's interests as part of the process of changing or terminating employment, the communication of termination responsibilities should include on-going information, cyber security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement.

n. Operating procedures shall be documented and made available to all users who need them. Documented procedures shall be prepared for operational activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, backup, media handling, and mail handling management.

o. All storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

p. The date and time of entry and departure of visitors shall be recorded, and supervised.

q. An information and cyber security awareness program shall be held regularly to make employees aware of their responsibilities and the means by which those responsibilities are discharged.

18. Information and cyber security aspects of Business Continuity Management

18.1 Business Continuity Management (BCM)

BCM is a management process that identifies risk, threats and vulnerabilities that could impact an entity's continued operations and provides a framework for building organizational resilience and the capability for an effective response. Business continuity plan sets out in detail as to how a particular strategy will be implemented in order to meet the defined requirements.

The information and cyber security continuity shall be embedded in the organization’s business continuity management systems.

a. NPS Trust shall determine its requirements for information and cyber security and the continuity of information and cyber security management in adverse situations – i.e., during a crisis or disaster.
b. NPS Trust shall establish, document, implement and maintain processes, procedures, and controls to ensure the required level of continuity for information and cyber security during adverse situations.
c. NPS Trust shall verify the established and implemented information and cyber security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

18.2 Redundancies

Information-processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

18.3 Business Continuity Plan (BCP)

18.3.1 NPS Trust shall establish documented procedures in order to respond, recover,resume, and restore to a pre-defined level of operation following disruption.

The plan shall ensure that employees and assets are protected and are able to restore function quickly in the event of a disaster. It shall be conceived in advance and involve input from key stakeholders and employees. BCP shall define all risks that can affect the organization’s operations, making it an important part of the organization's risk management strategy. Risks may include natural disasters—fire, flood, or weather-related events—and cyber-attacks.

The plan shall include:

a. Determining how those risks will affect operations;
b. Implementing safeguards and procedures to mitigate the risks;
c. Testing procedures to ensure they work; and
d. Reviewing the process to make sure that it is up to date.

BCPs are different from a disaster recovery plan, which focuses on the recovery of a company's IT system after a crisis.

18.3.2. Developing a Business Continuity Plan

Steps to develop BCP shall include:

a. **Business Impact Analysis**: Identify functions and related resources that are time-sensitive.
b. **Recovery**: Identify and implement steps to recover critical business functions.

c. **Organization**: Creation of team to focus on business continuity. This team shall devise a plan to manage the disruption.
d. **Training**: The team shall be trained and tested. Members of the teamshould also complete practicing exercises associated with BCP.

NPS Trust shall keep a checklist to include key details such as emergency contact information, a list of resources the business continuity team may need, where the backup data and other required information is housed or stored, and other important personnel details.Along with testing the business continuity team, the NPS Trust shall also test the BCP itself. It shallbe tested several times to ensure it can be applied to many different risk scenarios. This will help identify any weaknesses in the plan which can then be identified and corrected.

19. Asset management

19.1 Responsibility for assets:

NPS Trust shall identify the organizational assets and define appropriate protection responsibilities.

a. Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

b. Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented ,and implemented.

c. All employees and external party users shall return all organizational assets in their possession upon termination of their employment, contract or agreement.

19.2 Information classification:

a. Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

b. An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

c. Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.

20. Access control

An access control policy shall be established, documented, and reviewed based on business, information, and cyber security requirements.

a. Users shall only be provided with access to the network and network services that they have been specifically authorized to use.

b. A formal user registration and de-registration process shall be implemented to enable assignment of access rights.

c. A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.

d. The allocation and use of privileged access rights shall be restricted and controlled. The allocation of secret authentication information shall be controlled through a formal management process.

e. The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract, or agreement, or adjusted upon change.

f. Users shall be made accountable for safeguarding their authentication information.

g. Access to information and application system functions shall be restricted in accordance with the access control policy.

h. Password management systems shall be interactive and shall ensure secure passwords.

21. Compliance

NPS Trust shall avoid breaches of legal, statutory, regulatory, or contractual obligations related to information and cyber security and of any security requirements.

22. Conclusion

Information and cyber security policy is a foundation of a good security program for any organization. Information and cyber security shall be achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software & hardware functions. These controls need to be established, implemented, monitored, reviewed, and improved on a continuous basis to ensure that the specific security and business objectives of the organization are met. NPS Trust shall take a holistic and coordinated view of the organization’s information and cyber security risks in order to implement a comprehensive suite of information and cyber security controls under the overall framework of a coherent management system.

The information and cyber security policy can be effective only if employees adhere to it. Identifying appropriate controls requires careful planning and attention to detail. A successful information and cyber security policy requires support from all employees in the organization, participation from stakeholders, suppliers, and specialists/advisors.

Successful implementation of the policy would help the organization to report cyber incidents proactively and minimize and contain the damage. The continuous surveillance would arm the existing capabilities of information and cyber security framework leading to development of an effective and robust security thereby ensuring that the organization’s assets are reasonably safe and protected against any cyber threats.

This policy shall be operationalized by way of detailed standard operating procedures (SOPs) and internal circulars and plans of action at various levels of the organization as may be appropriate, to address the challenging requirement of information and cyber security.

****