सत्यमेव जयते

national
health
authority

Pradhan Mantri Jan Arogya Yojana
Ayushman Bharat
PM-JAY

Acceptable Use Policy

PRADHAN MANTRI JAN AROGYA YOJANA (PM-JAY)

VERSION 1.0

30-AUGUST-2019

Table of Contents

Document Control

Type of Information	Document Data
Title	Acceptable Use policy
File number	S-12019/33/2019-NHA
Document Revision	1.0
Document Owner	National Health Authority

Revision History

Version	Date	Prepared By / Modified By	Significant Changes
1.0	30 August, 2019	Information security team, NHA	First document

Document Approver

Version	Approved By	Name	Email
1.0	IT Advisor, NHA and GM-IT, NHA	Kiran Anandampillai and Manu Shukla	kiranma@nhaindia.in manu@nhaindia.in

1. Introduction

National Health Authority (NHA) shall define, document, implement and maintain policies to control access to their information resources. To ensure a high level of efficiency and quality in day to day business operations, NHA provides various digital and information assets (such as desktop, laptop) and services (such as internet access, printer) to various users. NHA intentions for publishing an acceptable usage policy are not to impose restrictions that are contrary to its established culture of openness, trust and integrity. NHA is committed to protecting its personnel, employees and third parties from illegal or damaging actions by individuals, either accidental or deliberate.

Effective security is a team effort involving the participation and support of every personnel and associate who deals with information and/or information systems. It is the responsibility of every PM-JAY personnel to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the Acceptable use of NHA’s Information systems. These rules are in place to protect the PM-JAY personnel and NHA. Inappropriate use exposes PM-JAY and its personnel to risks including virus attacks, compromise or network systems and services, and legal issues.

3. Scope

This policy is applicable to all NHA personnel, temporary/contractual staffs, eco-system Partners/ vendors, third Party personnel, State Government (SHA) Employees, Hospitals, other stakeholders who are using or accessing NHA’s services and/or applications and all NHA information systems and assets within NHA computing environments including but not limited to data centers, business workplace facilities, and all other NHA facilities that house computing systems. It is mandatory for employees to comply with this policy while serving NHA’s business.

4. Policy

4.1. General Use

a. All NHA personnel should be aware that the data/information they access/create on the information systems remains the property of NHA.

b. All personnel are responsible for exercising good judgment regarding the use of NHA information systems and facilities for personal purposes.

c. For security and network maintenance purposes, authorized individuals within NHA ecosystem may monitor equipment, systems and network traffic at any time, as per NHA Information Security Policy.

d. NHA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

e. All user accounts and passwords shall be kept secure and not shared with anyone. Authorized users are responsible for the security of their passwords and accounts. System level passwords and user level passwords shall be changed as per access control standard.

4.2. Laptop/Desktop and Workstation Security

a. PM-JAY personnel are accountable for the NHA laptop/desktop and must protect it to minimize the possibility of loss or theft, unauthorized use, or tampering;

b. PM-JAY personnel must ensure that the laptop remains under their personal control at all times;

c. Laptops must be securely stored when not in use; they must not be left unattended in an unsecure area.

d. Laptops must not be left in an unattended car.

e. When a laptop is taken to a location such as hotel, the laptop must either remain with the person or be locked in the hotel room and suitably secured with a cable lock.

f. When taken home, the laptop must not be left in an obviously visible location and must be stored within the confines of a locked room/building. For added protection, a cable lock must also be used to secure the laptop.

g. All personal computers, laptops and workstations shall be secured by logging-off or locking the screen when the host is left unattended.

h. PM-JAY personnel shall refrain from using desktops/ laptops or any other IT resources provided to users for unofficial purpose.

4.3. Physical Security

a. All PM-JAY personnel shall display their ID cards all times within NHA premises and other information processing facilities.

b. PM-JAY personnel shall not tailgate to enter the access restricted premises and shall challenge/report any other personnel tailgating into the premises.

c. All personnel shall participate in safety/fire drills organized by NHA or building management.

d. Personnel shall ensure that visitor or third party users are always escorted to and from the reception areas.

e. All PM-JAY personnel shall use their access card / biometric access control to enter NHA information processing facility.

4.4. Network and System Activities

The following activities are strictly prohibited, with no exceptions. Employees may be exempted from these restrictions if user have exception approval or during the course of their legitimate job responsibilities (such as systems administration staff may have a need to disable the network access of a host if that host is disrupting production services)

a. Port scanning or security scanning, unless prior notification to IT/ security department is made.

b. Connecting external devices or wireless access points to NHA network through data/LAN cable to gain unauthorized access.

c. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

d. Interfering with or denying service to any user other than the employee's host.

e. 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.

f. Introduction of malicious programs into the network, server or systems (such as viruses, worms, Trojan horses, e-mail bombs, etc.).

g. Making copies of system configuration files for users' own, unauthorized personal use or to provide to other people/users for unauthorized use.

h. Downloading, installing or running security programs or utilities which reveal weaknesses in the security of a system.

i. Connecting unauthorized devices like personal USBs, personal laptops, personal handheld devices, personal portable modems, personal tablets etc. to official systems or networks.

j. Revealing account password to others or allowing use of personal user account by others.

k. Using a NHA computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

l. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

4.5. Copyright Infringement

a. PM-JAY supports the rights of copyright owners and does not tolerate reckless or deliberate copyright infringement.

b. Users shall not violate 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 NHA.

c. PM-JAY personnel shall not indulge in 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 NHA or the end user does not have an active license.

d. PM-JAY personnel shall refrain from exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.

e. Users shall not transmit, distribute, download, copy, cache, host, or otherwise store any information, data, material, or work that infringes the intellectual property rights of others.

f. Installation of unlicensed software is strictly prohibited. Disciplinary action shall be taken if unlicensed software is found on PC/laptop or any other NHA owned asset.

4.6. Password Security

a. End users shall ensure confidentiality of their passwords.

b. Minimum requirements for passwords shall be adhered as per password policy.

c. Users shall ensure that authentication credentials are changed periodically or in case of compromise.

d. Compromise of password shall be reported immediately to SecurityIncident@nhaindia.in

4.7. Internet Usage

a. PM-JAY personnel shall not download inappropriate material such as picture files, music files, or video files for personal use;

b. PM-JAY personnel shall not store any NHA information/data on any online storage website or on cloud unless there is an authorized business requirement.

c. PM-JAY personnel shall not engage in uploading and downloading large files not related to business from the internet or unofficial e-mails;

d. PM-JAY personnel shall refrain from surfing sites having objectionable content like pornography, violence, weapons etc.;

e. PM-JAY personnel shall not store, send or distribute confidential information, copyright material or other content which is subject to third party intellectual property rights, unless users have a lawful right to do so;

f. Sending or distributing unsolicited advertising, bulk electronic messages or overloading any network or system is strictly prohibited;

g. PM-JAY personnel shall not access, monitor or use any data, systems or networks, including another person's private information, without authority or attempt to probe, scan or test the vulnerability of any data, system or network;

h. Employees shall not obtain unauthorized access to or knowingly modifying information held on Internet resources;

i. Internet access is provided to users for the performance and fulfilment of job responsibilities. Users shall access the Internet for business purposes and restrict non-business activities over the Internet.

j. All access to Internet shall be authenticated and shall be restricted to business related sites. NHA has the right to filter and prohibit access to certain websites at its own discretion.

k. Users will be held responsible for any misuse of Internet access originating from their account. NHA reserves the right to monitor users’ internet access and usage details, and to take any disciplinary or legal action upon violation of this policy.

4.8. Document and Storage Media Security

All documents containing sensitive information shall be marked as "confidential", both in electronic and print format. Care shall be taken to ensure confidentiality while these documents are transmitted by email, fax or other communication media or during printing and photocopying of documents.

4.9. E-mail/Instant Messaging and Communications Activities

a. 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)

b. Any form of harassment via email, instant messaging, telephone or paging, whether through language, frequency, or size of messages

c. Unauthorized use, or forging, of email header information

d. Sending /viewing/forwarding racial, sexually threatening, defamatory or harassing e-mails/instant messages

e. 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

f. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type

g. Use of unsolicited email originating from within NHA's networks.

4.10. Blogging and Social Media

a. Blogging by personnel, whether using NHA’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of NHA’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate NHA's policy, is not detrimental to NHA's best interests, and does not interfere with a personnel's regular work duties.

b. NHA's acceptable use policy also applies to blogging. As such, Personnel are prohibited from revealing any confidential or proprietary information, trade secrets or any other information classified by NHA's Information security policy when engaged in blogging.

c. Personnel shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of NHA and/or any of its personnel.

d. Personnel may also not attribute personal statements, opinions or beliefs to NHA when engaged in blogging. If personnel are expressing his or her beliefs and/or opinions in blogs, the personnel may not, expressly or implicitly, represent themselves as a personnel or representative of NHA. Personnel assume any and all risk associated with blogging.

4.11. Hardware and Software

a. To prevent the introduction of malicious code and protect the integrity of NHA assets, all hardware and software shall be obtained by raising request through NHA IT Help Desk.

b. All PM-JAY personnel shall abide by the software copyright law and shall not obtain, install, replicate, transfer or use software except as permitted under the licensing agreements.

c. To protect the integrity of NHA assets, PM-JAY personnel shall not use the personally owned software on NHA assets.

4.12. Clear Desk and clear Screen

A clear desk program for papers and removable storage media and a clear screen program for information processing facilities shall be adopted in order to reduce the risks of unauthorized access, loss of and damage to information during and outside working hours. The purpose of clear desk and clear screen policy is to ensure that no sensitive/confidential information is left unattended at any workstation, meeting room, or any other area within the NHA office premises and to improve the cleanliness standards therein.

a. All sensitive information shall be kept in a secured office location e.g. storage in a locked drawer, file cabinet etc.

b. All documents when printed or scanned shall be cleared from printers or scanners immediately.

c. All incoming and outgoing mail points and unattended facsimile (fax) machines shall be protected from unauthorized physical and logical access.

d. Unauthorized use of photocopier and other reproduction technologies (e.g. scanners, digital cameras etc.) shall be prevented.

e. Personal computers, computer terminals and printers shall be logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended.

f. Password-protected screen savers shall be activated within defined timelines.

g. Users shall turn off personal computers or log off all network resources at the end of each day.

4.13. Security Violations

a. Any security violations shall entail disciplinary action.

b. PM-JAY personnel shall not access, read, copy, divulge or destroy any type of information not in his/her scope of work, belonging to other employees or NHA without the consent of the information owner.

c. PM-JAY personnel with access to privileged information shall not divulge that information to other employees or third parties.

d. Failure of any PM-JAY personnel to comply with the confidentiality conditions stated above shall give NHA the right to take action as deemed appropriate, including legal action.

e. NHA's network resources shall not be used to conduct any malicious activities such as electronic fraud or hacking. Prohibited behaviors include but are not limited to:

- Unauthorized monitoring of network or network user activity (snooping).
- Hacking into information systems.
- Developing or deploying malicious code (malware or viruses).
- Misrepresentation with intent to mislead (assuming another person's identity or using another person's credentials).
- Sending messages using a fictitious name or a name belonging to another firm.
- Sending messages or data from fictitious or misleading email, IP, or other electronic address (spoofing).

f. If a user learns of any such activities occurring at NHA, then contact the NHA IS team (NHA-IS-Team@nhaindia.in).

4.14. PM-JAY personnel Responsibility

a. All personnel shall report any security weaknesses, incidents, possible misuse or violation of any NHA policies to SecurityIncident@nhaindia.in (email planned for the future).

b. PM-JAY personnel shall not attempt to access data, information, applications or programs contained on NHA's information systems for which they do not have authorization or approval from the owner

c. PM-JAY personnel shall contact the IT helpdesk Team and ensure that latest version of the antivirus software is installed on their desktop / laptop and that the virus definitions are updated;

d. PM-JAY personnel shall not purposely engage in activity which may intend to:

- Harass other employees/third parties in the PM-JAY/NHA ecosystem;
- Degrade the performance of PM-JAY/NHA systems;
- Deprive an authorized user's access to NHA resource/ information systems;
- Obtain extra resources, beyond those allocated;
- Circumvent NHA's computer security measures or gain access to NHA's information systems without having obtained proper approval and without proper authorization for doing so.

e. PM-JAY personnel shall not change the configuration of, remove, de-activate or otherwise tamper with any anti-virus program and other software that has been installed on systems used by them;

f. Where the mobile device policy allows use of privately-owned devices (e.g. Bring Your Own Device – BYOD), the related security measures shall be considered including separation of private and business use of the devices. PM-JAY personnel shall take reasonable measures to ensure the physical security of the device and security of the business information on the device. NHA shall wipe complete information from the device in case of loss or personnel separating from the organization.

5. Annexure A: Glossary

Terms	Definition
Information Asset	Any component of the system – hardware, software or network – that is intrinsic to the company.
Users (End Users)	All persons with access to NHA computing and storage resources, including but not limited to full time or part time employees, contractors, consultants, temporaries, visitors, business partners, clients, and vendors.
PM-JAY personnel	All employees, temporary/contractual staffs, eco-system Partners/ vendors, third Party personnel, State Government (SHA) employees, Hospitals, other stakeholders who are using or accessing NHA's services and/or applications and all NHA information systems and assets.
Blogging	A blog (a truncation of the expression "weblog") is a discussion or informational website published on the World Wide Web consisting of discrete, often informal diary-style text entries ("posts").
Malware	Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, etc. intended to damage a computer, mobile device, computer system, or computer network, or to take partial control over its operation

Phishing	Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Spam	Spam is generally email advertising for some product sent to a mailing list or newsgroup.

6. Appendix

NHA Information Security Policy