PAMAC

Banking on our Credentials

Policy - Acceptable Usage

Title	PAMAC Acceptable Usage Policy
Classification	Internal Use Only
Author	IT Head
Reviewer (suitability and adequacy)	AVP-Process improvements
Approver (suitability and adequacy)	CEO
Policy/Document Owner	Information security manager
Current Version	2.3
First Document Release Date	01.06.2017

Modification History:

S. No.	Description of Change	Date of Change	Version No.
1	Detailed documentation of existing policy	21.09.2017	2.2
2	Reviewed no changes done	27.12.2019	2.2
3	Policy reviewed no change	18.09.2020	2.2
4	Policy scope amended	18.08.2021	2.3
5	Reviewed no changes done	12.10.2022	2.3
6	Reviewed no changes done	26.02.2024	2.3

PAMAC

Banking on our Credentials

1 Overview

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at PAMAC . PAMAC provides necessary infrastructure to PAMACIANS ,to perform their day to day Operational activities and must use them responsibly to maintain the confidentiality, and refrain from physical damage. This document is a guideline that every member of PAMAC, shall comply in his/her day to day operations.

2 Scope

All employees, contractors, consultants, temporary and other workers at PAMAC, including all personnel affiliated with third parties must adhere to this policy. This policy applies to assets owned or leased by PAMAC, or to devices that connect to a PAMAC's network or reside at a PAMAC site. All the updated policies are uploaded online (Easy HR Portal), PAMACIANS are required to read, understand and adhere to the policies

3 Policy

PAMACIANS are responsible for exercising good judgment regarding appropriate use of PAMAC resources in accordance with PAMAC policies, standards, and guidelines. PAMAC resources may not be used for any unlawful or prohibited purpose.

3.1 Computer System, Accounts and Password

3.1.1 PAMACIANS are responsible for ensuring the protection of assigned PAMAC assets that includes the use of computer cable locks and other security devices.

3.1.2 All PCs, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

3.1.3 PAMACIANS are not allowed to connect any external Devices to the PAMAC network. For any exception to this, you should get approval from ISMS via your reporting manager. You should approach IT Team for further assistance, after you get approvals.

3.1.4 Usage of USB/flash memory is strictly prohibited in the organization. This is controlled with the antivirus end point security. In case of data file transfer, which cannot be made through other mediums, ensure formal approval is in place before such media can be used.

3.1.5 PAMACIANS are not allowed to share folders/files on network i.e. file/folder sharing should not be activated on any PCs, laptops, workstations and servers.

3.1.6 PAMACIANS are forbidden to use any messenger/chat applications such as (but not limited to) like MSN Messenger, Yahoo messenger, ICQ etc unless explicitly permitted.

3.1.7 PAMACIANS should not connect directly to the Internet via modem, GPRS or any other mean's except by Company issued devices such as laptops while on PAMAC premises

3.1.8 Using Notebook PCs in public places (conferences, training rooms etc) calls for additional physical security, usage of Laptop Locks is advised.

3.1.9 Laptop/note book have a continuous threat of theft as they are easily visible. Avoid

using laptop bags that suggest the laptop inside. If not keep in close custody. There has been incidents related to laptop thefts inside the car. Avoid getting tricked by incidents that drive your attention around the car when someone can open your door and pick up your laptop in a fraction of seconds.

3.1.10 Laptops left at PAMAC overnight must be properly secured or placed. Promptly report any theft of PAMAC assets to the IT and ISMS team.

3.1.11 Using PAMAC computing asset to actively engage in procuring or transmitting material that is in violation of law or business code or conduct sexual harassment or hostile workplace laws in the user's local jurisdiction is strictly prohibited.

3.1.12 Mobile device contain company information in the form of emails and documents, therefore they should always be protected physically as well as logically. Physical protection involves keeping the device in proximity to the individual. Logical protection involves keeping the devices protected by a password and session time out after 5 minutes. Access in Mobile device is provided basis matrix or access policy

3.1.13 In case the mobile device is lost report immediately to the issuing department or the security manager in order to stop further relay of messages. Also read manufacturer (Apple, Android, Nokia) driven guideline for secure remote destruction of content if the control is applicable.

3.1.14 PAMACIANS are responsible for the security of data, accounts and physical systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

3.1.15 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home. Do not share your access credential at work with any other employees.

3.1.16 PAMACIANS must maintain system-level and user-level passwords in accordance with the Password Policy.

3.2 Usage of Office Network & Communication Infrastructure

Office Network & Communication Infrastructure has been provided in order to ensure highest availability of systems and network services. The user has systems access includes business applications, Operating systems, Databases, and host of internal and external network related services. You are responsible for the security and appropriate use of above mentioned resources under your control.

3.2.1 Anti-Virus Protection : All hosts used by the employee that are connected to the PAMAC Internet/Intranet whether owned by the employee or PAMAC are equipped with E-scan or any other approved virus scanning software, you are supposed to make sure that the AVS is auto updated regularly with latest definition. You are not allowed to change the officially approved AVS on your system.

3.2.2 PAMACIANS are not allowed to use pirated software on PAMAC Network, installation of any copyrighted software for which PAMAC or the end user does not have an active

license is strictly prohibited. You should not save games, jokes, mp3s or any such information for entertainment purposes on PAMAC devices.

3.2.3 Scanning the network with the purpose of exploiting the weakness is strictly prohibited.

3.2.4 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 and approved by ISMS.

3.2.5 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet is strictly prohibited.

3.2.6 Employees are forbidden from using PAMAC electronic communication system for charitable endeavors, private business activities or amusement/entertainment purposes.

3.3 Electronic Communications

Email communication is a business necessity for all kind of communications whether internal or external. The usage of emails also brings several risks, as it is one of the most vulnerable mediums for several recognized and often unknown threats. PAMAC expects that the following security controls are exercised by individuals in order to prevent any security incident arising from usage of email.

3.3.1 ***Disclaimer:*** All Emails sent by employees should have a disclaimer stating that “the opinions expressed are strictly their own and not necessarily those of COMPANY, unless posting is in the course of business duties. The disclaimer should also state that Internet communication is unsafe and that the individual and the organization hold no liability in case the mail is being modified during the transmission”.

3.3.2 *Email from Unknown Sources:* Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, Malware, spy ware, or Trojan horse code. These threats have a potential to compromise systems and network and therefore user caution is an extremely important.

3.3.3 *Emails containing SPAM:* When employees receive unwanted and unsolicited email (also known as SPAM), they must refrain from responding directly to the sender. Instead, they should forward the message to the system administrator who will take steps to prevent further transmissions.

3.3.4 Employees must treat electronic mail messages and files as “Confidential” information. Electronic mail must be handled as a “Confidential” and direct communication between a sender and a recipient.

3.3.5 PAMAC electronic mail system is to be used only for business purposes. All messages sent by electronic mail are PAMAC records.

3.3.6 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).

3.3.7 Any form of harassment via email, telephone or SMS, whether through language, frequency, or size of messages.

3.3.8 Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender is prohibited.

3.3.9 While sending classified information as attachments, you are requires to zip the file and send the password through 'out of band' methods. Out of band refers to any medium than user for sending the primary medium. An example is mobile text, or a voice call.

3.4 Printer – Correct Usage

When a print command is given the user is required to be physically near the printer in order to protect output of confidential information. [This control is not applicable in case the printer provide authentication to the user for printing documents]. Printer access is provided on need basis as per defined policy.

3.5 Secure access of office premises

3.5.1 Office premises are secured with Access Control with Biometric device. Users are allowed to enter the premises with access control.

3.5.2 It is mandatory to use biometric device to access the office premises

3.5.3 In case, any issues with biometric report immediately to the issuing department.

3.5.4 All the employees are provided with the PAMAC identity cards for personal identification It is mandatory for PAMACians to wear the ID cards provided to them, on the premises

3.5.5 Identity cards provided to the PAMACians by PAMAC are the intellectual property of PAMAC, hence in case of loss/theft of ID cards, the PAMACian shall inform the loss of card to the relevant authority (HROPS and Admin) by calling or email.

3.6 Secure usage of cryptographic keys

Cryptographic keys (such RSA token) are to be used as an additional layer of authentication to access sensitive applications as per client requirement and Wherever applicable.

3.7 Clear Desk and Clear Screen Policy

3.7.1 All personnel are required to ensure that paper documents/files, other assets are kept in lock and key, when no longer in use;

3.7.2 All personnel are required to lock their screen (Pressing Windows + L or Control-ALT-DEL) when no longer working in their PC/notebook;

3.7.3 Group policy enforces screen lock every 300 seconds. If you are moving away from

your screen press Windows + L to lock your screen on windows machines and **Control + Shift + Eject** on Mac machines with an optical drive. (**Control + Shift + Power on a mac machine with no optical drive)**

3.7.4 All other admin interfaces – where group policy is not enforceable has admin driven 300 seconds screen lock

3.7.5 VPN Session, if any as per client, locks out also implement at 300 second interval.

3.8 Teleworking Policy

Teleworking Policy applies if the company has a policy of allowing work from home. In such cases additional security conditions applies such as but not limited to the follows:

3.8.1 Employee has the overall responsibility of protection physical and logical access to computing devices such as notebook, mobile and desktops.

3.8.2 Physical protection of computing device at teleworking site using locked physical areas to work

3.9 Social Media/ networking Policy

While using social networking sites such as (but not limited) twitter/facebook/linked-In, it is strictly prohibited to share any information related to PAMAC or Client or any other information related to data, its resources, information, clientele etc.

3.10 Usage of classified documents

Any document identified as confidential or internal use only should be strictly handled based on the documented procedure. In case sensitive documents needs to be transferred or destroyed, this should be done under the formal approval of the document owner or the head of department.

3.11 Incident Reporting

A security weakness /incident may be a result of compromise to Confidentiality, Integrity, and availability, Non-repudiation and/or Legal or Contractual Non-conformity. The impact of any security incident may result in serious consequences to the business and therefore an adherence to this policy is to avoid any such serious incident.

3.11.1 Employees should be well aware of Incident reporting procedures and understand areas, which may or may not be reported.

3.11.2 Employees must promptly report all information security alerts, warnings, suspected vulnerabilities, weaknesses, and the like to the Information Security Manger using the incident reporting Form/Procedure.

3.11.3 Users should not be found any exploiting any identified weakness.

Areas that can be reported are as follows (not exhaustive):

Any event or weakness that can jeopardize the confidentiality, integrity and/ availability' of information assets is worthy of reporting. This can include physical controls, technology controls, personnel behaviors related to information assets, and procedural controls.

An example of each of these is give below:
Physical controls can cover all aspects of physical security such as weak doors, access control systems, entry and exit areas, and associated processes.

Technical controls can cover strengths and weakness such as password complexity (less than 6), lack of antivirus, email attachments, accidental or deliberate mass mails etc;

Personnel controls such as unauthorized access attempts, violation of Company policy, violation of internet usage policy etc.

Administrative controls such as asset not identified, document classification, no documentation, no change and access definition etc.

Note that an employee can report his/her head of department/reporting manager. Alternatively one can also approach the information security manager / IT manager by phone extn 2260 / 2267 or email to security@pamac.com

3.12 Bring Your Own Device:

No PAMACian is allowed to carry any digital device in the office premise except their mobiles. (wherever approved by ISMS Team and HOD). Mobiles are not allowed to connect to the network or systems or to be used as hotspot for any internal or external communication. This is controlled by AVS Policies and wherever any deviation is required, necessary approval process is to be followed up.

3.13 Suurvilance or Audit

All Company owned infrastructure is owned by PAMAC, and will be audited by ISMS Team or any appropriate authority authorized by PAMAC management without any prior notice to employee or respective unit.

3.14 Intellectual Property/ownership

PAMAC owns all hosted infrastructure including information stored, processed, and transmitted in the Company offices. No employee can claim the content or intellectual property of the assets/hosted infrastructure as their own.

PAMAC

Banking on our Credentials

4 Consequence Management/Disciplinary action Procedure (DAP)

Disciplinary action is an action towards the non-compliance to the stated objective in this policy. Any act deliberate or accidental, wherein the motive of the end-user is found to be malicious, shall lead to invocation of disciplinary action policy..

5 Question/clarifications/improvements

If you have any questions, clarifications or improvements please do not hesitate to call Ganesh Sawant at [Extn.2260] or write an email at security@pamac.com

[Note: All attempts have been made to provide accurate information. However please do not hesitate to write back to us if any area needs further elaboration or edition at ganesh.sawant@pamac.com]

Employee Access Matrix:-

Allowed Assets		**Laptop /Desktop**	**Internet**	**Dongle**	**Email**	**Antivirus**	**RES**	**Calculs**	**Pamaconline**
Sr. No.	Category								
1	Director / COO	Yes	Cat 1	Yes	Yes:- Full	Cat 1	Yes	Yes	Yes
2	Sr. Vice President	Yes	Cat 1	Yes	Yes:- Full	Cat 1	Yes	Yes	Yes
3	Vice President	Yes	Cat 1	Yes	Yes:- Full	Cat 1	Yes	Yes	Yes
4	Associate Vice President	Yes	Cat 1	Yes	Yes:- Full	Cat 1	Yes	Yes	Yes
5	Sr. Manager	Desktop / Laptop	Cat 1	On Approval	Yes:- Full	Cat 1	Yes	Yes	Yes
6	Manager	Desktop / Laptop	CAT 2	On Approval	Yes:- Full	CAT 2	Yes	Yes	Yes
7	Assistant Manager	Desktop / Laptop	CAT 2	No	Yes:- Restricted	CAT 2	Yes	Yes	Yes
8	Team Leader/SME	Desktop	CAT 2	No	Yes:- Restricted	CAT 2	Yes	Yes	Yes
9	Sr. Executive/MT*	Desktop	Cat 5	No	Yes:- Restricted	Cat 5	Yes	Yes	Yes
10	Executive	Desktop	Cat 5	No	Yes:- Restricted	Cat 5	Yes	Yes	Yes
11	Jr. Executive	Desktop	Cat 5	No	Yes:- Restricted	Cat 5	Yes	Yes	Yes
12	Trainee	Desktop	Cat 5	NO	Yes:- Restricted	Cat 5	Yes	Yes	Yes