	EMAIL POLICY	Page 1 of 14
	Doc # : IT/EML/03	Ed: 03 REV: 00 November 01, 2024


INFORMATION AND COMMUNICATION TECHNOLOGY DEPARTMENT




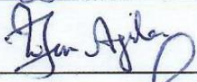
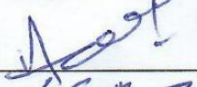
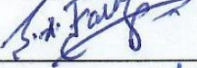
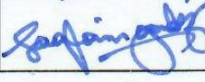
EMAIL POLICY & PROCEDURE
EMAIL POLICY & PROCEDURE

Edition – 3

November 2024


	EMAIL POLICY	Page 2 of 14
	Doc # : IT/EML/03	Ed: 03 REV: 00 November 01, 2024

Third Edition

	NAME	DESIGNATION	SIGNATURE	DATE
Prepared by:	Syed Mustafa Ali	Manager ICT		29/11/2024
Revised by:	Irfan Ayub	Dy. General Manager System Admin		2/12/2024
Reviewed by:	Adeel Yousfani	Dy. General Manager Cyber Security		
Reviewed by:	Syed Ahmed Faraz	General Manager IT Infrastructure		
Approved by:	Muhammad Saqlain Gardezi	Chief Information Officer		09.01.2025
Issue date: NOV - 2024		Effective Date: JAN - 2025		

Distribution List:


1. Chief Information Officer
2. General Manager –Infrastructure
3. General Manager – Quality Assurance & HSE
4. General Manager – Human Resource & Administration
5. PIA Intranet

	EMAIL POLICY	Page 3 of 14
	Doc # : IT/EML/03	Ed: 03 REV: 00 November 01, 2024

Revision Record

Edition Number	Revision Number	Issue Date	Effective Date	Inserted By & Date
3 rd Edition	Revision No. 0	Nov 01 ,2024	Jan, 2025	Irfan Ayub Syed Mustafa Ali (01 st Jan 2022)
2 nd Edition	Revision No. 1	Oct 25, 2007	Nov 01, 2007	Muhamad Imran Khan Irfan Ayub (25 th Oct, 2007)
1 st Edition	Revision No. 0	Feb 28 th , 2007	Mar 1 st , 2007	Manager Network Maintenance & Operations (28 th Feb, 2007)

List of Effective Pages (LEP)				
Chapter No.	Chapter Name	Page	Date	Revision
1	Introduction	7	Sep 21, 2020	0
2	Scope	7	Sep 21, 2020	0
3	Legal Risk	7	Feb 28, 2007	0
4	Legal Requirements To use PIAC email Services	7	Sep 21, 2020	0
5	Inappropriate use of corporate email	7	Sep 21, 2020	0
6	Best Practices	8	Sep 21, 2020	0
7	Personal Use	9	Dec 20, 2021	
8	Mail to the entire network	9	Sep 21, 2020	
9	Email usage	9	Sep 21, 2020	0
10	Email Attachment	10	Sep 21, 2020	0
11	Email Security	10	Dec 20, 2021	0
12	Confidential Information	10	Dec 20, 2021	0
13	Passwords	10	Dec 20, 2021	0
14	Encryption	11	Dec 20, 2021	
15	Inactive email accounts	11	Sep 21, 2020	
16	System Monitoring	11	Feb 28, 2007	0
17	Disclaimer	11	Sep 21, 2020	0
18	Email Forwarding	11	Sep 21, 2020	0
19	Account Creation	11	Sep 21, 2020	0
20	Password forgotten / Recovery	11	Nov 01, 2024	0
21	Quota Management	12	Sep 21, 2020	0
22	Data Purging & Record Retention	12	Dec 20, 2021	0
23	Data Backup	12	Dec 20, 2021	0
24	Data & Account Restore	12	Dec 20, 2021	0
25	Account Deletion	12	Dec 20, 2021	0
26	Help Desk Support	12	Dec 20, 2021	0
ANNEX-I	Email Account Creation Form	13	Sep 21, 2020	0
ANNEX-II	Email Account Restore Form	14	Dec 20, 2021	0

	EMAIL POLICY	Page 5 of 14
	Doc # : IT/EML/03	Ed: 03 REV: 00 November 01, 2024

FOREWORD

Following the implementation of the new Zimbra email system at PIACL, an update to the email policy has been deemed necessary. Due to the previous practice of local Lotus archiving on user machines, such archived emails will not be accessible on the server or in backups. This revised policy specifically addresses Zimbra's features and requirements.

Email is the lifeblood of our daily operations, enabling efficient and convenient communication throughout the company. However, this powerful tool also carries inherent risks and responsibilities. We've established this email policy to provide clear guidelines for its appropriate use within the workplace. By following these guidelines, we can ensure that our email communication remains professional, secure, and effective.

By following the guidelines outlined in this policy, we can all contribute to maintaining our company's reputation, protecting sensitive information, and increasing our productivity. Please take the time to read through this policy carefully and familiarize yourself with its contents. If you have any questions or concerns, please do not hesitate to reach out to your supervisor or the I&CT department.

Thank you for your commitment to responsible email use and continued cooperation in maintaining a positive and respectful email culture at our company. This culture of clear, concise, and professional communication is essential for our teamwork and productivity.

PIACL (I&CT Department)


	EMAIL POLICY	Page 6 of 14
	Doc # : IT/EML/03	Ed: 03 REV: 00 November 01, 2024

Table of Content

1. INTRODUCTION

2. SCOPE

3. LEGAL RISKS

4. LEGAL REQUIREMENTS TO USE PIAC EMAIL SERVICES

5. INAPPROPRIATE USE OF CORPORATE EMAIL

6. BEST PRACTICES

- Writing emails
- Replying to emails
- Newsgroups
- Maintenance
- Mail Management

7. PERSONAL USE

8. MAIL TO THE ENTIRE NETWORK

9. EMAIL USAGE

10. EMAIL ATTACHMENT

11. EMAIL SECURITY

12. CONFIDENTIAL INFORMATION

13. PASSWORDS

14. ENCRYPTION

15. INACTIVE EMAIL ACCOUNTS

16. SYSTEM MONITORING

17. DISCLAIMER

18. EMAIL FORWARDING

19. ACCOUNT CREATION

20. PASSWORD FORGOTTEN / RECOVERY

21. QUOTA MANAGEMENT

22. DATA PURGING AND RECORD RETENTION

23. DATA BACKUP

24. DATA & ACCOUNT RESTORATION


25. ACCOUNT DELETION

26. HELP DESK SUPPORT

FORMS

i. EMAIL ACCOUNT CREATION FORM (ANNEX-I)

ii. EMAIL ACCOUNT RESTORATION FORM (ANNEX-II)

	EMAIL POLICY	Page 7 of 14
	Doc # : IT/EML/03	Ed: 03 REV: 00 November 01, 2024

1. **INTRODUCTION**

The purpose of this policy is to ensure the proper use of "PAKISTAN INTERNATIONAL AIRLINES CORPORATION LIMITED" email system and make users aware of what "PAKISTAN INTERNATIONAL AIRLINES CORPORATION LIMITED "deems as acceptable and unacceptable use of its email system. It is the responsibility of every email user to follow these guidelines, in letter and spirit to ensure optimum efficiency without compromising the security of official information. The "Information & Communication Technology Department" reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

2. **SCOPE**

This policy applies to all users of PIA information assets including PIA employees, permanent or contractual, on deputation, manpower deployed in PIA through contractors, vendors, business partners, and contractor personnel and functional units regardless of geographic location. All users are required to read, understand and comply with these policies, standards, and procedures. If any user does not fully understand anything in these documents, he/she should consult with his/her line/functional Manager, Human Resources Department or Information & Communication Technology Department.

3. **LEGAL RISKS**

Email is a business communication tool and users are obliged to use this tool in a responsible, effective, and lawful manner. Therefore, it is important that users shall be aware of the legal risks and consequences of the usage of email:

- 3.1. If you send emails with any libelous, defamatory, offensive, racist, or obscene remarks, you will be held liable.
- 3.2. If you unlawfully forward confidential information, you will be held liable.
- 3.3. If you unlawfully forward or copy messages without permission, you will be held liable for copyright infringement.
- 3.4. If you send an attachment that contains a virus, you can be held liable.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of email. If any user disregards, disobeys, violates, and/or breaches the rules set out in this email Policy, the user shall be fully responsible for its consequences under the applicable Disciplinary Policy and laws. The PIACL shall be fully indemnified and absolved from any consequence that a user may face under the applicable laws.

4. **LEGAL REQUIREMENTS TO USE PIAC EMAIL SERVICES**

It is prohibited to:


- 4.1. Send or forward emails containing libelous, defamatory, offensive, racist, or obscene remarks/material. If you receive an email of this nature, you must promptly notify your system administrator/supervisor.
- 4.2. Forward a message to other domains (in or out of the PIA network) without acquiring permission from the owner of the email.
- 4.3. Send unsolicited email messages.
- 4.4. Forge or attempt to forge email messages.
- 4.5. Disguise or attempt to disguise your identity when sending mail.
- 4.6. Send email messages using another person's email account. The account holders must be aware that in case of violation of this clause, they shall be personally responsible.
 - 4.6.1. Account Holders must furnish details of the person(s) who are authorized by them to use their email accounts to ICT Department.
- 4.7. Copy a message or attachment belonging to another user without permission of the originator.
- 4.8. Public emails like hotmail, gmail, yahoo, etc. should not be used for official purposes. In case of PIA email services' limitation, user must obtain permission from his/her line Manager. PIAC email users must are not allowed to set public email domain as forwarding email address.

5. **INAPPROPRIATE USE OF CORPORATE EMAIL**

By using the corporate email address, our employees must bear in mind that they represent our company in that sense alone, and should mind the image they project. This sensitivity must be manifested in all their communications, whether official or personal.

Our employees represent our company whenever they use their corporate email addresses. They must **NOT**:

- 5.1. Sign up for illegal, unreliable, disreputable, or suspect websites and services.
- 5.2. Send unauthorized marketing content or solicitation emails.
- 5.3. Register for a competitor's services unless authorized.
- 5.4. Send insulting or discriminatory messages and content.
- 5.5. Intentionally spam other people's emails, including their coworkers.
- 5.6. Our company has the right to monitor corporate emails.

	EMAIL POLICY	Page 8 of 14
	Doc # : IT/EML/03	Ed: 03 REV: 00 November 01, 2024

6. **BEST PRACTICIES**

"PAKISTAN INTERNATIONAL AIRLINES CORPORATION LIMITED " considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Users shall take the same care in drafting an email as they would for any other communication. Therefore "PAKISTAN INTERNATIONAL AIRLINES CORPORATION LIMITED " wishes users to adhere to the following guidelines:

6.1. **Writing emails:**

- 6.1.1. Write well-structured emails and use short, descriptive subjects.
- 6.1.2. "PAKISTAN INTERNATIONAL AIRLINES CORPORATION LIMITED " email style is informal. This means that sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. Messages can be ended with '**Best Regards**'. The use of Internet abbreviations and characters such as smiley, however, is not encouraged.
- 6.1.3. Signatures must include your name, job title, extension, and company name. A disclaimer will be added underneath your signature (see Disclaimer)
- 6.1.4. Users must spell-check all emails prior to transmission.
- 6.1.5. Do not send unnecessary attachments. Compressed attachment email size should not exceed 15 MB before sending them.
- 6.1.6. Do not write emails in capitals.
- 6.1.7. Do not use cc: or bcc: fields unless the cc: or bcc: the recipient is aware that you will be copying a mail to him/her and knows what action, if any, to take.
- 6.1.8. If you forward emails, state clearly what action you expect the recipient to take.
- 6.1.9. Only send emails in which the content could be displayed on a public notice board. If they cannot be displayed ethically in public in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password (see confidential).
- 6.1.10. Only mark emails as important if they really are important.

6.2. **Replying to emails:**

- 6.2.1. Emails shall be answered within office time, but users must endeavor to answer priority emails within 4 hours.
- 6.2.2. Priority emails include emails that may suffer business continuity, but not limited to, are emails from existing customers and business partners.
- 6.2.3. End users must ensure a timely response to avoid any financial or operational loss to PIAC.

6.3. **Newsgroups:**


- 6.3.1. Users should seek permission before joining any newsgroup from ICT Department through email. The request will be generated by the concerned supervisor or in charge and approved by the head of the Human Resource Department.

6.4. **Maintenance:**

- 6.4.1. Delete any email messages that you do not need to have a copy of, and empty your 'deleted items'.

6.5. **Mail Management:**

- 6.5.1. Employees should compress large-size files before attaching them with the email. This will help to optimize the bandwidth and size of the email.
- 6.5.2. Employees should check their e-mail with a frequency appropriate to their jobs. Employees who will be absent for more than one day should make arrangements for a supervisor or co-worker to check for messages that need attention, OR, an automatic reply message (out of office) may be configured.
- 6.5.3. It is possible to receive a virus when receiving e-mail, and some viruses are embedded in attachments. If you receive a suspicious e-mail, then do not open it and forward it to abuse@piac.aero
- 6.5.4. Some computer features increase e-mail traffic, and employees should strive to keep message and attachment sizes as small as possible. Avoid the use of graphics in auto-signatures or other parts of the message or attachments. The use of stationary should be avoided, as well as moving graphics and/or audio objects as they consume more disk space, and network bandwidth, and detract from the message content.
- 6.5.5. Users must use proper official language in their emails.
- 6.5.6. Users must not
 - 6.5.6.1. discuss their opinions on religious/sectarian, or political matters,
 - 6.5.6.2. to propagate indiscipline in office matters,
 - 6.5.6.3. for the purposes of disrepute/ill repute of any individual or organization.

	EMAIL POLICY	Page 9 of 14
	Doc # : IT/EML/03	Ed: 03 REV: 00 November 01, 2024

7. **PERSONAL USE**

It is strictly forbidden to use "PAKISTAN INTERNATIONAL AIRLINES CORPORATION LIMITED " email system for anything other than legitimate business purposes. Therefore, personal emails, chain letters, junk mail, jokes and executables are prohibited. All messages distributed via the company's email system are "PAKISTAN INTERNATIONAL AIRLINES CORPORATION LIMITED " property.

8. **MAIL TO THE ENTIRE NETWORK**

- 8.1. Only General Managers and above are authorized to send MAIL ALL messages, message should route through General Manager ICT.
- 8.2. Message may contain attachments, including pdf files, graphics as well as animations and/or audio objects, subject to the consent of email administrators.
- 8.3. Messages from employee's associations/trade unions / welfare organizations/scouts should route through General Manager Public Relations
- 8.4. Message should clearly mention its recipients, sender, subject, and message body/email text


9. **E-MAIL USAGE**

The usage of the email system is subject to the following:

- 9.1. Usage of the E-mail system is limited to business needs.
- 9.2. Content of the email must be in formal language.

Message content restrictions include: -

- 9.3. PIA information resources shall not be used to transmit or receive statements that contain any material that is offensive, defamatory, or threatening to others.
- 9.4. The Systems should not be used to communicate statements, messages, or images consisting of pornographic material, ethnic slurs, racial epithets, or anything that may be construed as harassing, offensive, or insulting to others based on race, religion, national origin, color, marital status, citizenship status, age, disability, or physical appearance.
- 9.5. Any statements or comments made via email that could in any way be construed as an action of PIA must bear a disclaimer such as "These statements are solely my own opinion, and do not necessarily reflect the views of my employer." Even with this disclaimer, all practices regarding decency and appropriate conduct still apply.
- 9.6. Any use of Email from the network is easily traceable to PIA. Personnel must conduct these activities with the reputation of PIA in mind. Staff must exercise the same care in drafting Email, as they would for any other written communication that bears the PIA name.
- 9.7. PIA Email systems should not be used to produce or distribute "chain mail," operates a business, or makes solicitations for personal gain, political or religious causes, or outside organizations. Users must not forward or otherwise propagate, to individuals or groups, chain letters, pyramid schemes, or any other types of data that may unnecessarily consume system resources or otherwise interfere with the work of others.
- 9.8. To maintain the security of PIA's Email system, it is important to control access to the system. Users must not provide other unauthorized persons with their Email ID and personal password.
- 9.9. Users must use only their own PIA official Email account and must not allow anyone else access to their account. Impersonation is not permitted. Users must identify themselves by their real name; pseudonyms that are not readily attributable to actual users must not be allowed. Users must not represent themselves as another user. Each user must take precautions to prevent unauthorized use of the Email account. Forging of the header information in Email (including source address, a destination address, and timestamps) is not permitted.
- 9.10. Users must not publish or distribute internal mailing lists to non-staff members. PIA Systems should not be used to transmit or receive trade secrets, copyrighted materials, or proprietary or confidential information unless it is digitally signed and encrypted.
- 9.11. Any information regarded as confidential including legal or contractual agreements, technical information related to PIA's operations or security, etc. must not be communicated through Email unless it is digitally signed and encrypted.
- 9.12. Under no circumstances is information received through unsecured Email to be considered private or secure. Description Clear text information in transit may be vulnerable to interception. Secure communication through Email can be ensured only by using encryption and digital signatures.

	EMAIL POLICY	Page 10 of 14
	Doc # : IT/EML/03	Ed: 03 REV: 00 November 01, 2024

- 9.13. Attachments from unknown or untrusted sources must not be opened. All email attachments, regardless of the source or content, must be scanned for viruses and other destructive programs before being opened or stored on any PIA computer system. Personnel must perform a virus scan on all material that is transmitted to other users via email prior to sending it.
- 9.14. Users must not send unsolicited bulk mail messages (also known as “junk mail” or “spam”). This practice includes, but is not limited to, bulk mailing of commercial advertising and religious or political tracts. Malicious email, including but not limited to bulk mailing, is prohibited.
- 9.15. All communications and information transmitted, received, or archived in PIA’s computer system is the property of the company. PIA may exercise its right to monitor employees’ email activity. Company has the right to access and monitor official emails at any time, for any reason, with or without prior notice. Access and monitoring permission shall be granted by Chief Human Resource Officer.
- 9.16. Sharing of email box is not allowed. Please refer to point 11.11

10. E-MAIL ATTACHMENTS

The maximum attachment limit is 15MB for all users. Users must adhere to attachment restrictions. Attachments, greater than 15MB, must use compression utility or other tools to limit the attachment size. A few file extensions are restricted and cannot be used as attachments for example exe, bat, dll, etc.

11. EMAIL SECURITY

Email is a very sensitive medium that can compromise company’s reputation, legality, and security of data and equipment due to cyber-attacks, viruses, and other malware. To prevent this, employees must:

- 11.1. Remember passwords rather than writing them down, which can risk unauthorized access.
- 11.2. Select strong passwords that are hard to guess. Ideally, choose a password with at least eight characters in a combination of lower- and upper-case letters, symbols, and numbers.
- 11.3. Change passwords every 90 days.
- 11.4. Avoid opening attachments and links for content that is not well understood or looks suspicious.
- 11.5. Cross-check emails and names of unknown senders to ascertain their legitimacy. Cross-check the sender’s email address and reply email address before sending any email.
- 11.6. Be suspicious of clickbait titles and delete such emails if possible.
- 11.7. Be wary of inconsistencies or stylistic red flags like too many mistakes, capital letters, or excessive exclamation marks.
- 11.8. Keep anti-virus programs updated.
- 11.9. Cross-check with the ICT department on email address email.support@piac.aero if they are unsure about the safety of any email.
- 11.10. Avoid sharing passwords to any other person.
- 11.11. **Sharing of email box, if mandatory requirement:**
If sharing of the email box is required, then it will be used with separate email ids.

12. CONFIDENTIAL INFORMATION


Confidential Information must not be shared without prior permission of the concerned supervisor.

13. PASSWORDS

This is with the reference to **PIA IT Policy 6.13 – Passwords** which states that **6.13.1 Passwords should not be obvious or easy to guess and must be kept confidential. Passwords must:**

- Not be same as User ID.
- Not contain words like PIA, PIAC.
- Be minimum eight (08) characters long and contain (01) upper case letter and one (01) numeric and one (01) special character.
- Have zero (01) day minimum age.
- Have ninety (90) days maximum age.
- Not be same as last two (02) passwords.
- Be blocked after ten (10) failed sign-in attempts and unlocked after 30 minutes.

- 6.13.2 User profiles and passwords will not be disclosed to anybody other than the profile holder.
- 6.13.3 The Passwords of privileged or administrators’ accounts should be stored in a secure electronic vault.

	EMAIL POLICY	Page 11 of 14
	Doc # : IT/EML/03	Ed: 03 REV: 00 November 01, 2024

Users are required to change their password upon first login. Maintaining password confidentiality is the sole responsibility of the email account holder. Any email transmitted using an account is the responsibility of the account holder. Passwords must not be shared with other individuals or groups.

Multi-Factor Authentication (MFA):

Multi-Factor Authentication (MFA) is mandatory for high-value users to enhance security. High-value users include individuals with access to sensitive data, financial systems, or administrative privileges.

14. ENCRYPTION

Encryption email requests must be initiated and forwarded to email.support@piac.aero by the line manager. Further, **refer to IT Policy Security Measures 7.7.2 (a),(b) & (c)**

7.7.2 (a) Message Confidentiality: Sensitive information to be transmitted via a public network must be encrypted using an approved encryption mechanism

7.7.2 (b) Message Authentication: Sensitive information to be transmitted via a public network must be “electronically signed” by the authorized Personnel. Such electronic signatures shall be assigned by PIACL and shall have a hash significantly different from other electronic signatures.

7.7.2 (c) Electronic Signatures Authentication: Such electronic signatures shall be assigned by PIACL and shall have a hash significantly different from other electronic signatures. Forgery of electronic signature shall be dealt with in accordance with applicable law.

15. INACTIVE EMAIL ACCOUNTS

All email accounts maintained on email servers are the property of "PAKISTAN INTERNATIONAL AIRLINES CORPORATION LIMITED ". Email accounts not used for 45 days will be deactivated and will be activated upon formal request through concerned DGM to email.support@piac.aero. **Refer to IT Policy 6.3.7** “All user accounts which are inactive or dormant for 45 days shall be disabled. The reactivation of account request shall be passed through line-manager.”

16. SYSTEM MONITORING

Users cannot claim any right of privacy in anything they create, store, send or receive on the PIA's email system. "PAKISTAN INTERNATIONAL AIRLINES CORPORATION LIMITED " can but is not obliged to, monitor emails without prior notification. If there is evidence that users are not adhering to the guidelines set out in this policy, the "PAKISTAN INTERNATIONAL AIRLINES CORPORATION LIMITED " reserves the right to take disciplinary action, including termination and/or legal action.

17. DISCLAIMER

The following disclaimer will be added to each outgoing email:

"This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not an intended recipient, as indicated above, please notify us immediately and delete it from your system. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the company. *Please consider the environment before printing this email*"

18. EMAIL FORWARDING


PIACL email accounts and emails are the property of PIACL, applying forward on email accounts to any domain is prohibited and falls under information leakage. Forwarder will be applied on individual accounts by email system admins only. Requester is required to acquire formal approval from the concerned competent authority i.e. GM, Chief Engineer, or Chief Pilot or above, and the same approval will be forwarded to system admins.

19. ACCOUNT CREATION

Request for the creation of a new e-mail account at the head office should be generated by at least a GM, Chief Engineer or Chief Pilot. Request for the creation of a new e-mail account at out stations should be generated by UU for sales offices and KK for airport-related functionaries. Email account creation requests should reach account.create@piac.aero in the prescribed form in **ANNEX-I** of this policy. Once the email account is created, the requestor will be informed by the concerned GM, CE, or CP.

20. PASSWORD FORGOTTEN / RECOVERY

To enhance security, any request for a password reset should follow a formal procedure. An email with the subject 'Forgot Password' must be sent to forgot.password@piac.aero by the section in-charge, including the user's email address, name, and employee number. The requester must also provide a registered mobile number or official extension. Once received, the system administrator will verify the request with a confirmation call and respond to the in-charge with a new

	EMAIL POLICY	Page 12 of 14
	Doc # : IT/EML/03	Ed: 03 REV: 00 November 01, 2024

password via email. The in-charge will then relay the new password to the user. No verbal or informal requests will be entertained.

21. **QUOTA MANAGEMENT**

Each normal user of the email account holder is provisioned with 500 MB of server space for storing messages and up to 5 GB for executives & critical users. If someone requires more storage special request from the concerned Chief must be acquired and forwarded to the Email Administration Team. GM I&CT has the final authority to accept or reject the quota enhancement request after evaluating the impact on the system and storage.

Things to remember:

- I. When you reach or exceed your quota, you will not be able to receive any new e-mail messages until you free up space in your e-mail account. Once your quota is met or exceeded, the system will immediately return all messages to the sender.
- II. Messages will resume being delivered to you once you have freed up space in your account. Any messages sent to you while your account was over quota were returned to the sender and must be resent for you to receive them.

22. **DATA PURGING AND RECORD RETENTION**

The total retention period is 05 Years. No record will be available after 05 years.

23. **DATA BACKUP**

The PIA Email Accounts are backed up on a regular basis by the backup team as a way of recovering from a systematic loss impacting the entire email system. Following be more precise

- Five (05) years online
- Five (05) years offline

24. **DATA & ACCOUNT RESTORATION**

Offline data, mentioned in point 23, can be restored upon the email request of the account owner through the concerned In charge or DGM. The user must specify the restore period. Offline data, pertaining to retired, terminated, resigned, or deceased employees, the concerned General Manager may request through email at email.support@piac.aero to restore offline data.

Closed email accounts will be restored in read-only mode upon the approval of CHRO through the concerned chief to email.support@piac.aero.

25. **ACCOUNT DELETION**

This has reference to "Information Technology Policy Article -6. 'Information / Data Security Policy - 6.3 User Access' that states *where users with access to sensitive information / data are terminated or have resigned or suspended from PIACL service, concerned supervisor and HR is responsible for removal of that staff access rights in the systems to prevent unauthorized transactions.*" Therefore, HR Department **will** inform ICT department on an email account.revoke@piac.aero to **revoke/disable** the rights on email, subsequently, the account will be disabled/deleted.

26. **HELP DESK SUPPORT:**

26.1. **T1 Support (khicpk@piac.aero)**

- 26.1.1. Email Client Installation/Configuration (Desktop Client, Thunder Bird, Outlook).
- 26.1.2. Troubleshooting Client Issue.
- 26.1.3. Reset Password

26.2. **T2 Support (email.support@piac.aero)**

- 26.2.1. Create New Email Account
- 26.2.2. Quota Extend
- 26.2.3. Account Configuration
- 26.2.4. Mobile Device Configuration



Information & Communication

ANNEX-I

Form No:ICT/NW-20/001

EMAIL ACCOUNT CREATION FORM (ANNEX-I)

First Name		Section	
Middle Name		Department	
Last Name		Loc	
Staff No.		City	
Designation		Country	
		Tel/Contact No	
Suggested Email Account		GM / CE Email id	

Justification :

User Status: Permanent ☐ Contract ☐ Daily Wages ☐ Vendor / Auditor ☐

Declaration

I have read and understood PIA ICT & Email policies and shall use email accounts accordingly.

Signature	Date	Concerned GM / CE
-----------	------	-------------------

For ICT use only

Dy. General Manager ICT	Date	APPROVED / REJECT
-------------------------	------	-------------------

Quota	<input type="text"/>	GB	MB	Created ID	<input type="text"/>
Performed By Pno.	<input type="text"/>			Date / Time	<input type="text"/>

Signature
Asst Manager ICT

Signature
Manager ICT



ANNEX-II		Form No:ICT/NW-20/005	
EMAIL ACCOUNT RESTORATION FORM			
Serial No.	<input type="text"/>	Section	<input type="text"/>
Name	<input type="text"/>	Department	<input type="text"/>
Staff No.	<input type="text"/>	Extension	<input type="text"/>
Designation	<input type="text"/>	Station	<input type="text"/>
Email Account	<input type="text"/>		

Justification :

User Status: Permanent ☐ Contract ☐ Daily Wages ☐ Vendor / Auditor ☐

Declaration
I have read and understood PIA ICT & Email policies and shall use email accounts accordingly.

Signature _____	Date _____	Concerned General Manager _____
<u>For ICT use only</u>		

Dy. General Manager ICT _____	Date _____	APPROVE / REJECT
-------------------------------	------------	-------------------------

Retrieved <input type="text" value="YES / NO"/>	Reason :	<div></div>
Performed By <input type="text"/>		
Pno. <input type="text"/>		
Date / Time <input type="text"/>		

Signature _____	Signature _____
Manager ICT	DGM ICT