



COMPUTER & INFORMATION TECHNOLOGY CENTER

Email Policy

Document Controls

This document is reviewed every six months

Document Reference	PAAET-PLCY-EMAIL
Document Title	Email Policy
Document Owner	Abdullah AIDousari
ISO 27001:2013 reference	A13.2.3 - Electronic messaging
Security Classification	Internal -Unrestricted
Stored	http://sp13.paaet.edu/sites/TecDep
Next Review Date	8 th Dec, 2016
Document Status	Draft

Document Review and Approval History

Date	Version	Amended by	Reviewer/Approver	Remarks	RFC#
19 th April, 2016	Draft v1.0	Reena Varghese		Initial	
21 st April, 2016			Jessy Sakariah	Reviewed	
28 th April, 2016	Draft v1.1	Abdullah AIDousari		Edited	
8 th June, 2016	Final v1.2	Rabie Al-Mejbas	Rabie Al-Mejbas	Added email disclaimer statement and minor editing	

Document Distribution List

Sl.No.	Name and Department	Purpose
1	ISO team : <ul style="list-style-type: none"> • Rabie Al-Mejbas • Rajiv Prakash • Nadia AL Saleh • Shaikha AL Barak • Mai AlAbdulqader • Abdullah Aldousari 	Start implementing this policy on all documentations.
2	All CIC	To comply with the policy
3	Exchange Server Admins	To inforce and apply the policy

CONTENTS

CONFIDENTIALITY STATEMENT.....	4
1.0 INTRODUCTION.....	5
2.0 OBJECTIVE	5
3.0 SCOPE	5
4.0 POLICY	6
5.0 ENFORCEMENT	7
6.0 DEFINITIONS	7
7.0 REFERENCES	8
8.0 ASSOCIATED DOCUMENTS	8

CONFIDENTIALITY STATEMENT

This document includes confidential information related to the Computer and Information Technology Center (**CIC**) at the Public Authority for Applied Education and Training (**PAAET**), shall not be distributed to any persons other than those mentioned in the distribution list herein, and shall be used solely for **CIC**'s internal purpose.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise without the written permission of **CIC**, at **PAAET**.

All product names referenced herein are trademarks of their respective companies.

1.0 INTRODUCTION

Under the provisions of the ISMS, information resources are strategic assets of PAAET and information involved in electronic messaging should be appropriately protected.

Electronic email is often used as the primary communication and awareness method within an organization. At the same time, misuse of email can introduce many legal, privacy and security risks, thus it is important for users to understand the appropriate use of electronic communications.

Thus, this policy is established to achieve the following:

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To educate individuals using email with respect to their responsibilities associated with such use.
- To establish prudent and acceptable practices regarding the use of email.

Email services are provided by PAAET to support its primary role of education and research and associated functions related to this role.

This Policy is issued by CIC at PAAET. The owner of this document is responsible for maintain and updating this policy, and then final approval is obtained from the Technical Support Supervisor.

2.0 OBJECTIVE

This policy is intended to detail the rules of conduct for all members of PAAET who use email and related services.

3.0 SCOPE

This policy covers appropriate use of any email sent from PAAET email address and applies to all employees, contractors, vendors and students operating on behalf of PAAET.

Only authorized users of PAAET computer systems are entitled to use email facilities. All such email users of PAAET shall agree and abide by PAAET regulations.

4.0 POLICY

- All use of email must be consistent with PAAET policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- PAAET email account should be used primarily for PAAET business-related purposes.
- All PAAET data contained within an email message or an attachment must be secured.
- The PAAET email system shall not to be used for the following:
 1. Sending email that is intimidating or harassing.
 2. Using email for conducting personal business.
 3. Using email for purposes of political lobbying or campaigning.
 4. Violating copyright laws by inappropriately distributing protected works.
 5. The use of unauthorized e-mail software.
- Employees who receive any emails with this content from any PAAET employee should report the matter to their supervisor immediately.
- Users are prohibited from sending or forwarding confidential or sensitive PAAET information from PAAET email to a third party email system to conduct PAAET business, to create or memorialize any binding transactions, or to store or retain email on behalf of PAAET. Such communications and transactions should be conducted through proper channels using PAAET-approved documentation. Examples of third-party email systems and storage servers are Google, Yahoo, MSN Hotmail and email provided by other Internet Service Providers (ISP) such as Quality Net or KEMS etc.
- The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:
 1. Sending or forwarding chain letters.
 2. Sending unsolicited messages to large groups except to conduct PAAET business.
 3. Sending excessively large messages
 4. Sending or forwarding email that is likely to contain computer viruses.
- All user activity on PAAET Email systems is subject to logging and review.
- Disclaimer used by PAAET email system is as follows:

“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 have received this email in error, Please notify the sender immediately by email and delete this email 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 organization. Finally, the recipient should

check this email and any attachments for the presence of viruses. PAAET accepts no liability for any damage caused by any virus transmitted by this email.”

5.0 ENFORCEMENT

Access to the information technology environment in general, and electronic mail in particular, at PAAET is a privilege and must be treated as such by all users of these systems. Like any other facility, abuse of these privileges can be a matter of legal action or official PAAET disciplinary procedures.

Depending on the seriousness of an offense, violation of the policy can result in penalties ranging from written warning (i.e., do not do this anymore), to loss of access, to referral to PAAET authorities for disciplinary action.

In a case where unacceptable use severely affects performance or security, in order to sustain reasonable performance and secure services for the rest of the user community, CIC will immediately suspend an individual's access privileges.

6.0 DEFINITIONS

Names	Definitions
Email	A system for sending and receiving messages electronically over a computer network.
Copyright	Copyright is a legal right created by the law of a country that grants the creator of original work exclusive rights for its use and distribution for a period.
Asset	An asset is an item of economic value that is expected to yield a benefit to the owning entity in future periods
Email attachment	An attachment is a file that is sent along with an email message.
Chain letters	A letter, email, or other message sent to a number of people asking each recipient to send copies with the same request to a specified number of others

Unsolicited emails	Email spam, also known as junk email or unsolicited bulk email (UBE), is a subset of electronic spam involving nearly identical messages sent to numerous recipients by email.
Computer virus	A computer virus or a computer worm is a malicious software program that can self-replicate on computers or via computer networks
Email Disclaimer	An email disclaimer is a disclaimer, notice or warning to limit liability, which is, added in a text form to an outgoing email and so forms a distinct section, which is separate from the main message.

7.0 REFERENCES

ISO/IEC 27001:2013 – A.13.2.3 - Electronic messaging

8.0 ASSOCIATED DOCUMENTS

- 1) Information Security Policy