COMPUTER & INFORMATION TECHNOLOGY CENTER

Information Transfer Policy

Document Controls

This document is reviewed every six months

Document Reference	PAAET-PLCY- INFORMATION TRANSFER
Document Title	Information Transfer Policy
Document Owner	Nadia AlSaleh
ISO 27001:2013 reference	A.13.2.1 – Information transfer policies and procedures
Security Classification	Internal Unrestricted
Stored	http://sp13.paaet.edu/sites/TecDep
Next Review Date	8th June 2017
Document Status	Final

Document Review and Approval History

Date	Version	Amended by	Reviewer/Approver	Remarks	RFC#
8th June 2016	Draft v1.0	Reena Varghese		Initial draft	
6th Jan 2017	Final	Nadia AlSaleh	Rabie Al-Mejbas	Final Draft	

Document Distribution List

Sl.No.	Name and Department	Purpose
	All CIC staff and contractors	To ensure that all users read the policy of Information Transfer and comply with it.

CONTENTS

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.

1.0 INTRODUCTION:

There are many occasions when information is transferred between departments, to third-party service providers, to other public bodies, commercial organizations, and individuals. This is done using a wide variety of media and methods, in electronic and paper format.

In every transfer, there is a risk that the information may be lost, misappropriated, or accidentally released. For legal reasons such as confidentiality or data protection, and to maintain the trust of our service users and partners it is essential that the transfer is performed in a way that adequately protects the information.

This policy outlines the responsibilities attached and the minimum-security requirements for transfer. For the purpose of this document, Information refers to both textual information (e.g. word-processed documents, reports and spreadsheets), and raw unformatted data (e.g. backup tapes), in any format and on any medium.

2.0 OBJECTIVE

This policy states the minimum-security requirements for physical transfer of information into, across, and out of the organization, in any format.

3.0 SCOPE

This policy applies to all employees of the PAAET CIC and any Third party that processes the organization information.

4.0 POLICY

1. PAAET CIC recognizes its responsibility to process its information correctly and in line with all legal, regulatory, and internal policy requirements.
2. It is the Sender's responsibility to assess risks in what they are intending to do and ensure that all associated risks are adequately understood and covered, and that the transfer is properly authorized.
3. PAAET CIC staff shall not assume that because someone asks for information that they are authorized or legally entitled to have it. If in doubt, staff shall check with their supervisor/manager.

4. Once the sender is sure that, the transfer is legal and necessary then he/she must decide what kind of information is being dealt with. This will determine what level of security is appropriate.
5. The sender must consider the various methods / media of transfer available and whether they are appropriate.
6. Before any information is transferred, one must:
    a. Obtain and document the approval of the Information Owner for transfer for example in the case of using e-mail for transfer the owner is notified by putting him/her in the CC.
    b. Ensure that the transfer is necessary and is legal
    c. Remove or blackout anything that is not essential for the recipient's purpose, different communities shall be established for different recipients & different purpose.
7. Confidential information that affects the business interests of a third party, or for which the sender does not hold copyright e.g. bank details, salary details, contracts, agreements shall be dealt with great care.
8. Unauthorized release of confidential information can leave PAAET CIC staff open to legal sanction or litigation.
9. Public information shall be transferred in the most cost-effective method available by:
10. Seeking the permission of the Department that produced or owns this information before making any transfer, even if the transfer appears harmless.
11. For all transfers of personal information it is essential that the identity and authorization of the recipient has been appropriately authenticated by the sender.
12. It is essential that CIC has in place systems to ensure that bulk transfers of personal information are appropriately controlled, implementing appropriate security measures around these transfers.
13. All new bulk transfers must be authorized by the Head of Section / Service. He / she will decide whether to authorize the transfer of this information after careful consideration of the content, format, and method of transfer.
14. PAAET IT shall maintain a log of all routine and ad-hoc transfers of bulk personal information (based on information flows review). For ex. (Active Directory, Applications).
15. Electronic mail should be used in accordance with the Email Policy.
16. Staff shall avoid distribution of chain emails and any other.
17. Personal e-mail accounts (e.g. Hotmail accounts, Gmail) must not be used for transferring official / confidential information.
18. All CIC staff and contractors shall ensure that the name and e-mail address of the recipient are correct.

19. Email message must contain disclaimers and clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
20. The Sender shall check with the recipient that his / her e-mail system will not filter out or quarantine any attachments transferred by email.
21. The sender must check at an appropriate time that the email and any attachments sent to the recipient has been transferred successfully, and report any issues to Head of section/manager.
22. Ensure that the information within the e-mail is stored in the agreed format for the record type i.e. in line with professional record keeping guidelines.
23. No FTP transfer is allowed in PAAET.
24. Any removable devices used for information transfer should be scanned for viruses and malware.
25. On occasions, when information may need to be transferred in person, careful consideration must be given to all the potential security and confidentiality risks involved. Actions taken to mitigate such risks should be agreed upon and documented.
26. Staff shall ensure the following if certain circumstances demand the transfer of information via Fax.
    a. The sender must check that the Fax number is correct and that the receiver is awaiting transmission.
    b. For any confidential information, the number must be double-checked by a colleague before transmission and telephone contact must be maintained throughout transmission.
    c. Both sender and receiver must have an agreed process to avoid their copy being left on the Fax machine and a clear requirement to securely destroy the message when no longer required.
    d. The sender must check at an appropriate time that the transfer has been successful, and report any issues to his / her direct supervisor/manager.
27. Confidential information shall not be stored or transferred using SMS or other way on mobile phones.

5.0 ROLES AND RESPONSIBILITIES

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are:

Sender (PAAET CIC Staff)

The Sender is responsible for ensuring the following requirements of this Policy are met.

- Assessing the confidentiality of information to be sent.
- Ensuring that the identity and authorization of the recipient has been formally confirmed and documented.
- Obtaining the consent of the Data Owner for the transfer of information.
- Ensuring that the information is sent and tracked in an appropriate manner.

IT Auditor

The IT Auditor in the Internal Audit section will monitor and audit departments to ensure compliance with all statutory and regulatory obligations, and internal policies.

Section Heads and Supervisors

Departmental managers are responsible for ensuring that this Policy is communicated and implemented within their area of responsibility, and for ensuring that any issues such as resourcing or funding are communicated back to their strategic directors in a timely manner.

Individual employees

Individual employees will be responsible for familiarizing themselves with this Policy and ensuring that any information transfer for which they are responsible is done in a compliant manner.

Individual employees must report any suspected or actual security breaches related to data transfer in line with the PAAET Incident Management Policy.

6.0 EXCEPTIONS

Exceptions from this policy may be granted by Chief Security Officer, CIC Manager, or Technical Support Supervisor, on a case-by-case basis, after:

- Demonstration of sufficient business need and
- Completion of a risk assessment by information security team.

7.0 ENFORCEMENT

- The Information Security team shall verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

8.0 REFERENCES

1) ISO/IEC 27001:2013 - A.13.2.1 – Information transfer policies and procedures

9.0 ASSOCIATED DOCUMENTS

1) Information Security Policy

10.0 DEFINITIONS

Requester	Any individual, department, service, service provider or any third-party that requests for information from a department / service belonging to organization.
Sender	The Sender is the individual acting for the organization that initiates a Data Transfer. He or she must have the authority and sufficient knowledge of the nature of the data to determine whether it should be sent and that it is sent securely. Where the final actual task is delegated to administrative, untrained or inexperienced staff, the original Sender remains responsible for ensuring the Transfer complies with this policy.
Bulk Transfer	The transfer of electronic or paper data that is “batched up” to be sent out of a location and/or organization.
Encryption	The process of converting information into a form unintelligible to anyone except holders of a specific key or password.
Removable Media	Is a term used to describe any kind of portable data storage device that can be connected to and removed from a computer e.g. floppy discs, CDs/DVDs, USB flash memory sticks or pens, PDAs, tablets, and smart phones.
Information Owner	Every major type of information must be assigned an owner within the organization who will be responsible for it throughout its lifecycle. This Owner may work in any department but must have sufficient ability, authority, and experience to understand the contents and approve the processing of the record. Record owners must be formally documented.