Ministry of Information Technology
& Telecommunication

DIGITAL PAKISTAN

Email Usage Standard Operating Procedure

Document Control

Prepared / Updated By	Reviewed By	Approved By	Owner	Version	Date of Approval
			MOITT	**1.0**	

Change History

SN	Version	Changes Description
1	**1.0**	**Final Version**

Table of Contents

1 Abbreviations

IS: Information Security

IT: Information Technology

2 Introduction

Official email accounts are provided Government employees to assist and facilitate business communications. It is provided for legitimate business use in the course of employees' assigned duties only.

Email is perhaps the most important means of communication throughout the business world. Messages can be transferred quickly and conveniently across our internal network and globally via the public Internet. However, there are risks associated with conducting business via email. Email is not inherently secure, particularly outside our own internal network. Messages can be intercepted, stored, read, modified and forwarded to anyone, and sometimes go missing. Casual comments may be misinterpreted and lead to contractual or other legal issues.

1. Email users shall be responsible for avoiding practices that could compromise information security
2. Corporate email services are provided to serve operational and administrative purposes in connection with the business
3. All emails processed by the departmental IT systems are considered to be the property of the organization/department.

3 Scope

This policy applies to all employees, consultants, vendors or visitors who use provided email facility of the department/organization.

4 Prohibited email usage

1. User shall not send confidential/ sensitive information over the internet unless it is necessary. It is recommended that the sender must get approval by the reporting officer and if possible, share file/ information in protected format (password protected)
2. Official email shall not be used for the creation or distribution of any disruptive or offensive messages, including but not limited to offensive comments about race, gender, personal appearance, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this type of content, the matter should be reported immediately to IT Support/ Service Desk.
3. Users shall not use official email to commit to a third party; for example, through purchase or sales contracts, job offers or price quotations, unless users are explicitly authorized by management to do so

4. Users shall not use official email to work for private or charity unconnected with legitimate business.
5. Users shall refrain to communicate using official email in ways that could be interpreted as representing or being official public statements on behalf of the department/organization, unless user is a spokesperson explicitly authorized by management to make such statements.
6. Users shall not send any message from anyone else's account or in their name (including the use of false 'from:' addresses). If authorized by the manager, a secretary may send email on the manager's behalf but should sign the email in their own name per pro ('for and on behalf of') the manager
7. Users shall not use official email for any other illegal, unethical or unauthorized purpose.
8. User shall not unnecessarily disclose potentially sensitive information in "out of office" messages.
9. Except when specifically authorized by management or where necessary for IT system administration purposes, employees shall not intercept, divert, modify, delete, save or disclose emails
10. Users shall not use Gmail, Hotmail, Yahoo or similar external/third-party email services (commonly known as "webmail") for official purposes.
11. Do not use auto-forward facility for corporate email to external/third party email systems.
12. Users shall be reasonable about the number and size of emails users send and save. Periodically clear out their mailbox, deleting old emails that are no longer required and filing messages that need to be kept under appropriate email folders.
13. The email accounts of all out-going employees shall be removed after taking backup of all their emails. Their emails shall be handed over to the departmental head. In case a departmental head resigns, their emails shall be handed over to a person authorized. Such email accounts may be kept active for a period of six months.

5 Responsibilities

IT Department is responsible for maintaining this policy and advising generally on information security controls. Working in conjunction with other corporate functions, it is also recommended for awareness activities to raise awareness and understanding of the responsibilities identified in this policy

Users should have no expectations of privacy: all emails traversing the corporate systems and networks are subject to automated scanning and may be quarantined and/or reviewed by authorized employees

1. Users shall apply their professional discretion when using email, for example abiding by the generally accepted rules of email etiquette (see the Email security guidelines for more). Review emails carefully before sending, especially formal communications with external parties

2. The organization/department's concerned team is responsible for building, configuring, operating and maintaining the corporate email facilities (including anti-spam, anti-malware and other email security controls) in accordance with this policy. The use of email is an extremely valuable business tool. However, misuse of such a facility can have a detrimental effect on other users and potentially the public profile of the organization.

3. Emails on the corporate IT systems are required to be automatically scanned for malicious software, spam and unencrypted proprietary or personal information. Unfortunately, the scanning process may not be 100% effective (e.g. compressed and encrypted attachments may not be fully scanned), therefore undesirable/unsavoury emails are sometimes delivered to users. Delete such emails and report them as security incidents to IT Help/Service Desk

4. The granting organization/department maintains the right to access user email accounts in the pursuit of an appropriately authorized investigation.

5. IT Help/Service Desk is responsible for assisting users with secure use of email facilities, and acts as a focal point for reporting email security incidents.

6. All employees shall be responsible for complying with this and other corporate policies at all times. This policy also applies to third party employees acting in a similar capacity whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of acceptable behaviour) to comply with information security policies.

7. Internal Audit shall assess compliance with this and other corporate policies at any time

6 Email ID Creation

- Email ID creation for Employees including Consultants/Contractors & Outsourced will follow the standard procedures, according to the requirement
  - **Designation/Job Role@domain**
- For creation of Groups following sample may be followed. Below is the example according to IT, it may differ from department to department.
  - For Support: support@organization domain
- For creation of department account following sample may be followed, and that account will be under direct responsibility of Department Manager, below is the example according to server room, it may differ from department to department

- SR+D(Department)@moitt.gov.pk

7 Disclaimer

Below or related Disclaimer shall be used in each email after Email Signatures.

"This Email and its attachments, if any, are confidential and may contain legally privileged information. If you are not the intended recipient, please notify the sender immediately and delete this Email and its attachments, if any, from your system. You should not copy this Email, disclose its contents to any other person, or use it for any purpose. Statements and opinions expressed in this Email are those of the sender, and do not necessarily reflect those of the organization. The organization accepts no liability for damage caused by any virus transmitted by this Email."

8 Enforcement

Since data security and integrity along with resource protection is critical to the smooth operations, employees and concerned personnel that do not adhere to this policy and found to have violated this policy may be subject to disciplinary action

9 Exception to Policy

1. It is imperative that all employees comply with all Information Security policies. However, there are circumstances that fall outside the ability to comply with and/or conform to a policy. In such instances, an exception must be documented and approved. This defines the requirements to formally authorize exceptions where control cost is much greater than the risk represented from non-compliance to information security policies.

2. Requests for exception must include:

   a. A valid business justification.

   b. A risk analysis, compensating controls to manage risk, and technical reasons for the exception.

   c. Requests for exception that create significant risks without compensating controls will not be approved. Requests for exceptions must be periodically reviewed to ensure that assumptions or business conditions have not changes.

References:

ISO 27001
• A.8.1.3 Acceptable Use of Assets