ই-মেইল পলিসি এর উপর মতামত প্রদানের জন্য অনুরোধ করা যাচ্ছে।

মতামত প্রদানের ঠিকানাঃ

ড. মোঃ ফজলুর রহমান
উপ-সচিব (পলিসি শাখা)
মোবাইল # ০১৭১৬১২৩৫৪১
ই-মেইল: fazlu@ictd.gov.bd

Email Policy
of
Government of Bangladesh
(Draft V.1)

Information and Communication Technology Division
Government of the People's Republic of Bangladesh

Document Information

Document Title	**Email Policy of the Government of Bangladesh**
Document Type	**Public**
Version	**1.0**
Commencement Date	**….. February 2017**
Last Update	**17 February 2017**
Pages	
Status	**Draft**

Table of Contents

1 Overview

To materialize the vision of Digital Bangladesh by 2021, the government of Bangladesh is implementing plenty of e-Governance activities in all potential sectors across the country. Towards this journey ICT became an essential tool for day to day activities of the government employees. Among those, Email is one of the mostly used means government employees use for communication within the organization, organization to organization and with different stakeholders of the government. Email service of global public email service provider like Yahoo, Gmail, Outlook, etc. is used by government employees to communicate and to share government information. However, this situation is changing and the awareness is growing within the government organization to have email services with its own internet domain name [e.g. cabinet.gov.bd]. Some of the government organization has email services hosted within their organization using their own servers and IT infrastructure whereas most of the government organization is using this services from Bangladesh Computer Council (BCC).BCC under ICT Division provides email services for the government organization from its National Data Center. More than 250 organizations are currently consuming email services from BCC. There is another good reason of hosting the email services in Bangladesh and that is to preserve government data within the geographical boundary of Bangladesh.

However there are cases found that even though organizations have email service under their own domain, their personnel still uses email services of Gmail, Yahoo or Outlook for official communication. Moreover there are lack of uniformity and guidance of acceptable email usage within the government organization. To mitigate this problem and to streamline every government email users under same rules and regulation, it has been realized that an email policy for government organization and employees should be developed.

This policy is intended to assist government organization having email services under their own domain as well as to give guidance to the government email users on acceptable usage of email.

2 Policy Governance and Implementation

Information and Communication Technology (ICT) Division on behalf of the Government of Bangladesh holds the ownership of this policy. ICT Division will also monitor and review the implementation of this policy across the government. As this is a live document and technology is changing over time, ICT Division holds the right to update this policy or any part of this policy as and when necessary in consultation with the stakeholders.

All government organization excluding those mentioned in 4.1 is responsible to implement and maintain the implementation of this policy. Any organization while implementing this policy can ask assistance to **emailpolicy@ictd.gov.bd**.

3 Objective

The objective of this policy is outlined as below:

- To ensure proper use of email system by all government organization and the users;
- To make the users aware of the acceptable and unacceptable use of email system;
- To bring uniform nomenclature in government email system;
- To provide guidance to the Email Service Provider (ESP) managing the email systems;
- To aware users on the perspective of compliance and legal.

4 Scope

This policy is applicable for all government, semi-government, autonomous, semi-autonomous, and statutory organization of Bangladesh excluding entities mentioned here in Clause 4.1.

4.1 Exception list of Entities

- Organization deals with National Security;
- Law Enforcing Agencies;
- Financial Institutes;
- Bangladesh Missions in abroad;

Organizations come under this exception list are exempted from this policy provided that they have ensured the following at least:

- The email servers are located in Bangladesh;
- The email domains are registered as cTLD (.bd) extension
- The email servers are managed by either BCC as the Email Service Provider or by the organization itself;
- The organization has its own acceptable and disclosure email usage policy;
- The organization has its own Backup, Retention and Information Security policy in compliance with the relevant laws of Bangladesh.

This policy is also applicable for the Service Provider providing email services for government organization. This policy is applicable to all users having email account under government domain regardless of devices they are using to access government email platform. Any

organization having internal email policy or acceptable email usage policy shall map their policy with this policy and ensure conformity with this policy.

5 Roles and Responsibilities

Separate entities are defined in this section to clearly identify major stakeholders and their roles for the successful implementation of this policy. Those are:

5.1 Email Service Provider

Bangladesh Computer Council (BCC) under ICT Division is the Email Service Provider for the government of Bangladesh. Apart from that any government organization having their own IT infrastructure to manage email services for their respective organization are also treated as Email Service Provider.

5.2 User Organization

Organization having email services from Email Service Provider are the User Organization. In some cases User Organization and Email Service Provider may be same.

5.3 Users

Email Users under the User Organization is treated as Users throughout this policy.

5.4 Focal Point

Focal Point is an individual or a team nominated to communicate regarding implementation of this policy and email services. Focal Point shall be from both Email Service Provider and User Organization.

To implement this policy successfully each of the defined roles is mapped with certain tasks and responsibilities. The tasks are to be implemented within a period defined as below:

- Short Term (3 months)
- Mid Term (12 months)
- Long Term (24 months)

On the other hand, responsibilities mapped with each role are continuous tasks or day to day activities that has to be complete by each role.

6 Action Plan

The following sections states the action plan for ESP, User Organizations, Focal Points and Users

6.1 Email Service Provider (ESP)

Sl.	Resposibility	Task	Duration
1	ESP shall implement the required infrastructure to provide email services for the government organization. But prior to that, ESP should make a Technical feature list and Requirement document of the mail server system and approve it before operational level.		LT
2	ESP shall implement uniform email security policy (guideline) for all the government organization		LT
3	ESP shall assist government organization to migrate their existing email accounts and data if it seems technically feasible and possible by ESP		LT
4	ESP shall formulate and implement backup policy for email services		LT
5	ESP shall provide disaster recovery support of email services for critical organization		LT
6	Apart from organization specific email services, ESP shall also implement common email services for all government employees under country top level (**.bd**/.বাংলা) domain which will be managed and supervised by ESP.		LT

Sl.	Resposibility	Task	Duration
7	ESP shall provide admin access to the organization as required and as per the signed SLA between ESP and User Organization		
8	ESP shall provide day to day support to create/modify account, password retrieval where admin access is not given to the organization. However, the email platform should have the DIY functionality.		
9	ESP shall implement spam guard for the email services provided to government organizations		
10	ESP shall implement Data Leakage Prevention for the email services		
11	ESP shall develop manuals for effective usage of government email		
12	ESP shall develop manual for using digital signature and encryption feature in email system		
13	ESP shall create data retention policy (guideline) of deactivated email accounts of the users as per the document retention directives by relevant laws		
14	ESP can deactivate any account, email domain or email feature if the account or domain or feature deemed as threat that can compromise or lead to a situation of compromise of data or service.		
15	ESP can deactivate any account or domain if any misuse activities has been reported by local or international CERTs.		
16	ESP shall notify the focal point of the organization when an account or		

Sl.	Resposibility	Task	Duration
	domain has been disabled.		
17	ESP shall provide designation based email id under organization domain and name based email id under common government email domain (mail.gov.bd/ডাক.বাংলা)		
18	ESP shall make Service Catalog and Service Level Agreement available in its website regarding Email Services mentioned under this policy and as catered by ESP in their service catalog		
19	ESP shall maintain active email server logs for 3 months and archived logs for 365 days		
20	ESP may disclose the logs of mail server and data of mail account for scrutiny by the LEA as per the ICT Act and relevant laws. ESP shall not act on any request from any organization to provide e-mail data and logs.		
21	ESP shall not Redirect emails coming into any deactivated email accounts to any government or third party email account		
22	ESP shall create necessary User Interface for different types of devices available today and keep provision for upcoming access mode/devices.		
23	ESP shall also define & deliver necessary email client software for different types of devices for those users who would like to preserve offline mails on their respective devices.		
24	ESP shall ensure 2FA or multiFA feature on UIX.		

6.2 User Organization

Sl.	Action Items	Type (Task/Responsibility)	Duration
1	User organization shall disseminate this policy to all email user under that organization		
2	User organization may formulate their own email usage policy provided that their own email policy is aligned with this policy		
3	User organization shall provide periodical awareness and training session on email security and on this policy for organization employees		
4	User Organization shall also create awareness on ICT Act for their employees		
5	User Organization shall use newsletter, bulletin, banner, boards to create awareness among the employees on email security		
6	User Organization shall not allow its users to use personal email for official communication and official email for personal affairs		
7	User organization shall ensure use of email must be consistent with government policies and procedures of ethical conduct, safety, compliance with applicable laws and proper practices.		
8	User organization must classify their data and develop acceptable practices to share data as per the Information Security Policy Guideline of Bangladesh. Any data classified as top secret, secret, confidential and restricted must be used in email with		

Sl.	Action Items	Type (Task/Responsibility)	Duration
	proper permission from the competent authority of the organization and as per acceptable practices to share data.		
9	If any User Organization wants to use SSL certificate in their email domain they shall provide the SSL certificate to ESP and with the assistance of ESP SSL certificate shall be deployed for the organization.		
10	User organization shall ensure that the government email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin by their employees.		
11	User organization should maintain a strict user nomenclature system as defined by the policy		

6.3 Users

Sl.	Action Items	Type (Task/Responsibility)	Duration
1	User must use government email system only for government purpose, personal use with government email system is prohibited		
2	User must periodically (at least once in every 6 months) change their email account password to ensure the protection of their email account		
3	Users shall change their account		

Sl.	Action Items	Type (Task/Responsibility)	Duration
	password after the first login to their account		
4	User shall not share their account or password to anyone within or outside the organization		
5	User shall not add any non-government and third party email account in official email groups		
6	User must protect their device (Mobile, Laptop, Notebook, Tab etc.) from compromise or lost where email client is installed or email account has been configured as sync. In such cases user must notify to their focal point.		
7	User shall not register government email account to any non-government websites including Social Media websites which are not directly involved with organization issues.		
8	Users are prohibited from automatically forwarding government email to a third party email system. Individual messages which are forwarded by the user must not contain information classified as Top Secret, Secret, Confidential and Restricted.		
9	Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, Dropbox, Outlook etc. to conduct government activities or transaction.		
10	Employees who receive any emails containing the content of disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual		

Sl.	Action Items	Type (Task/Responsibility)	Duration
	orientation, pornography, religious beliefs and practice, political beliefs, or national origin from any government employee should report the matter to their Focal Point.		
11	User shall not use the feature of auto-save password for government email account		
12	Users shall not download e-mails from government e-mail account, configured on the GoB mail server, by configuring POP or IMAP on third party email client (Outlook, Thunderbird etc.) unless as directed by ESP		

6.4 Focal Point

Sl.	To do Items	Type (Task/Responsibility)	Duration
1	Focal Point shall communicate with ESP regarding email services		
2	Focal Point having admin access cannot share admin access with any third party. User may delegate admin access to user within their organization for email administration		
3	Focal Point shall modify admin password periodically (at least every 2 months)		
4	Focal point having admin access shall create groups with their organization email accounts to disseminate mass email messages		
5	Focal point shall not add third party email accounts in the official email groups		

Sl.	To do Items	Type (Task/Responsibility)	Duration
6	Focal point shall disseminate awareness related newsletter, bulletin, information to all users within the organization		
7	Focal Point of the organization shall ensure the latest operating system, anti-virus and application patches are available on all the end points (desktop/laptop/mobile devices)		
8	Focal point having admin access shall keep records of the email creation/modification and password reset request		

7 Usage of Digital Signature Certificate

As per the ICT Act 2006, email information shall be treated as official document and record when Digital Signature Certificate (DSC) is used by the users and organization along with their email account. It is recommended to use DSC by the email users to ensure the authenticity, confidentiality, integrity, and non-repudiation. Office of the Controller of Certifying Authorities (CCA) along with their licensed CAs (Certified Authority) will assist each user organization towards the use of DSC in email system.

8 Policy Compliance

Internal compliance/audit team of BCC and User Organization shall periodically verify the implementation of this policy in ESP and in the User Organization. Focal point of each organization shall ensure the applicable usage of email as per this policy by the users. User organization shall conduct training and awareness activities on applicable usage of email for their users.

9 Monitoring & Improvement

ICT Division on behalf of the government of Bangladesh shall monitor the activities mentioned in this policy. ICT Division shall organize quarterly monitoring and review meeting with the focal

points of the user organization and ESP. ICT division in consultation with the stakeholders can do the modification of this policy whenever it deems necessary.

10 Appendix C: Acronyms and Abbreviations

2 FA	2 Factor Authentication
BCC	Bangladesh Computer Council
CA	Certified Authority
cTLD	Country Top Level Domain
DIY	Do It Yourself
ESP	Email Service Provider
GoB	Government of Bangladesh
ICT	Information and Communication Technology
IMAP	Internet Message Access Protocol
IT	Information Technology
LEA	Legislative Enterprise Architecture
LT	Long Term
Multi FA	Multi Factor Authentication
POP	Post Office Protocol
SLA	Service Level Agreement
SSL	Secured Socket Layer
UIX	User Interface XML

11 Definition

Guideline: A description that clarifies what should be done and how, to achieve the objectives set out in policies information processing facilities any information processing system, service or infrastructure, or the physical locations housing them

Information: Digitally processed data or digitized information of an agency or an individual.

Information System: An electronic information system that processes data electronically through the use of information technology - including but is not limited to: computer systems, servers, workstations, terminals, storage media, communication devices, network resources and Internet.

Integrity: When authorized persons are allowed to make changes to the information stored or processed by Information Systems in any aspects.

IS Policy: A documented list of management instructions that describes in detail the proper use and management of computer and network resources with the objective to protect these resources as well as the information stored or processed by Information Systems from any unauthorized disclosure, modifications or destruction.

Information security: Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved

Policy: Overall intention and direction as formally expressed by management

Third party: That person or body that is recognized as being independent of the parties involved, as concerns the issue in question

Threat: A potential cause of an unwanted incident, which may result in harm to a system or organization