Electronic Mail and Internet Services Directive

Version: 2.0
Effective date: 01 July 2003
## Table of Contents

1. Purpose .................................................................................................................. 3
2. Who should know this Directive............................................................................. 3
3. Scope of applicability............................................................................................ 4
4. Definitions................................................................................................................ 4
5. Roles and responsibilities...................................................................................... 5
6. Directives................................................................................................................ 8
   6.1 Creation of e-mail and Internet Accounts.......................................................... 8
   6.2 Updating the version of the e-mail and Internet browser software.................... 9
   6.3 Ongoing management of e-mail and Internet accounts ...................................... 9
   6.4 Amendments of individual e-mail Addresses and Aliases.............................. 9
   6.5 Amendments of groups of e-mail Addresses and/or Aliases.......................... 10
   6.6 Suspension and Termination of e-mail and/or Internet Services..................... 10
   6.7 Temporary unavailability of e-mail and Internet Services.............................. 10
   6.8 Abuse of the e-mail and Internet Services....................................................... 11
   6.9 Coming into force of the Policy....................................................................... 11
   6.10 Temporary delegation of use of a mailbox...................................................... 11
   6.11 Occurrences of Spam and Counterfeit e-mail............................................... 11
7. Supporting Documents.......................................................................................... 12
8. References............................................................................................................... 12
9. Modification history............................................................................................... 12
10. Maintenance and review cycle............................................................................. 13

Appendix A - E-mail Etiquette .................................................................................. 14
Appendix B - Restrictions on use of e-mail and Internet Services............................ 15
   B.1. E-mail............................................................................................................... 15
   B.2. Internet............................................................................................................. 15
   B.3. Restrictions on Internet Access....................................................................... 16
   B.4. Restrictions to e-mail specific to combat Spam.............................................. 16

Appendix C - Management Information and Audits ................................................. 17
   C.1. Management Information............................................................................... 17
   C.2. Audits............................................................................................................... 17
       C.2.1 Audits requested by the CIMU................................................................. 17
       C.2.2 Audits requested by Heads of Department/Entity................................. 17

Appendix D - Sanctions on use of e-mail ................................................................. 19
   D.1. Personal Use.................................................................................................... 19
   D.2. Official Use..................................................................................................... 19
       D.2.1. Use of Official e-mail............................................................................... 19
       D.2.2. Filing of Official e-mail............................................................................ 20

Appendix E - Typical e-mail Address and Alias Names......................................... 21
   E.1. E-mail Address............................................................................................... 21
   E.2. System Specific e-mail Alias..................................................................... 21
   E.3. Generic e-mail............................................................................................... 21

Appendix F - Classification of e-mail messages...................................................... 22
   F.1. Encrypted communications.......................................................................... 22
   F.2. Non encrypted communications.................................................................. 22
       F.2.1. Confidential............................................................................................ 22
       F.2.2. Private................................................................................................... 22
       F.2.3. Personal................................................................................................ 22
       F.2.4. No Classification.................................................................................. 22
1. **Purpose**

The Government of Malta (Government) uses an e-mail system and provides access to the Internet via its communications backbone, the Malta Government Network (MAGNET). E-mail and the Internet is becoming the principal vehicle for text and graphics movement within the Public Service and with outside entities and individuals. E-mail and the Internet have the potential of an important vehicle for:

1. Widely distributed broadcast type communications.
2. Specialised activities such as the movement of business applications to and between workstations and the movement of corporate memory.
3. On-line discussions such as Internet newsgroups and virtual meetings.

The e-mail and Internet Services are provided to assist in the conduct of Government business operations and to support the Public Service and wider Public Sector in delivering a service of the highest quality to the public in general.

E-mail and Internet are used for the exchange of information and business decision-making but are subject to rules that are appropriate and similar to that in a paper based work environment. These new technology tools are so important that a need has arisen to ensure that risks are minimised from either intentional or unintentional misuses.

In particular, the e-mail system carries and stores important programme and policy data and information that is a critical part of activity and project audit trails. Reminding employees of the importance of the protection of corporate memory, while permitting electronic document destruction under certain circumstances, is therefore a matter of concern.

The purpose of this document is to bring the expectation, as officially documented and endorsed in the Policy, Standards and Directive in respect of Government e-mail and Internet Services, to the attention of those who need to know. Good practices will improve system performance, maintain network efficiency, assure a productive work environment, preserving important corporate information and support the Government’s migration to standardised e-mail and Internet Services management.

The Policy helps ensure that e-mail and Internet use does not infringe on the privacy or rights of employees, is not used for purposes prohibited under the Laws of Malta, and does not legally compromise the Government.

2. **Who should know this Directive**

Knowledge of this Directive should extend up and down the organisations concerned and be widespread within them.

- Head of Agent
- All Account Holders
- Head of Department / Entity
3. **Scope of applicability**

The provisions of this Directive apply to all Account Holders, Agents and Heads of Department / Entity, and covers all e-mail and Internet Services use within Government.

The Policy and accompanying Standards and Directives encompasses internal and external electronic communications, independently of which network or system they travel on.

4. **Definitions**

**Account Holder** – a person authorised to use e-mail and Internet Services within the Government.

**Agent** – a trusted organisation that has the mandate by Government to provide Information and Communications services.

**Attachment** – indicates textual, graphical, visual or executable files that are attached with an e-mail message.

**‘Bulk Mail’** – an e-mail message in which the list of recipients spans a wide band of e-mail users.

**Corporate information/record** – all information under the control of a government institution, regardless of physical mode or medium in which such information is stored. Excluded from the definition are materials held by libraries, which were not prepared or produced by or for the Government.

**Corporate memory** – means information, which Account Holders create, generate, collect and use to enable the department/entity to meet its operational, legal, tactical and/or strategic needs to meet legislative or policy requirements.

**Counterfeit** – e-mail that makes use of or contains invalid or forged headers, invalid or non-existent domain names or other means of deceptive addressing.

**Delegate** – an individual authorised by the Account Holder to access his/her e-mail account, using software permissions or a delegate password. The degree of access of the delegate must be under the control of the Account Holder.

**E-mail** – correspondence between e-mail users over a computer network.

**Head of Department/Entity** – the person at the workplace to whom the employee or Account Holder reports.

**Internet** – a global network connecting millions of computers.

**Knowledge Worker** – a government employee who gathers data and information for business purposes, analysis and assesses such data and information and adds value to such data and information; and distributes the value added information product to others.

**Log Out** – an operation that terminates access to an e-mail and/or Internet Service, thus preventing unauthorised access.

**Mailbox** – a functional unit that contains stored messages for a specific user.
Password – a character string that is used as authentication information.

Service Level Agreement (SLA) – a contractual obligation between parties, which stipulates and commits the Agent to a required level of service. An SLA should contain a numerically quantified level of service, support options, enforcement or penalty provisions for services not provided, a guaranteed level of system performance as relates to downtime or uptime.

Spamming – electronic junk mail or any unsolicited bulk e-mail received that is unrelated to work, personal interest and not otherwise justifiable. In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network resources. Spamming costs the sender very little to send - most of the costs are paid for by the recipient or the carriers rather than the sender.

User – any person who has been granted access to an e-mail and Internet account.

Virtual Meetings – are defined as Account Holders discussions occurring in real or delayed time using computers.

5. Roles and responsibilities

For the purpose of this Directive, the following roles and responsibilities have been identified:

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| 01. The Central Information Management Unit (under direction from the CIMU Head) | i. to define e-mail and Internet Services Policy and Directive.  
| | ii. to communicate the Policy, Standard and Directive.  
| | iii. to define e-mail and Internet software standards.  
| | iv. to establish and maintain naming conventions for e-mail addresses and aliases.  
| | v. to identify the Agent.  
| | vi. to audit the quality of the e-mail and Internet Service provision and subsequently define SLAs to regulate this service provision.  
| | vii. to audit the use of the e-mail and Internet Services on a general and regular basis.  
| | viii. to liaise with Heads of Department/Entity or their designated delegates on administrative matters related to the e-mail and Internet Services.  
| | ix. to pays for e-mail Service.  
| | x. to regulate, investigate and direct matters arising re Anti Spam and Counterfeit e-mails. |
02. The Agent (under direction from the Head of Agent)

i. to obtain e-mail and Internet software updates from the supplier.

ii. to control and co-ordinate the distribution of e-mail and Internet software updates on PCs/Laptops that may be used by Account Holders.

iii. to ensure that e-mail aliases and addresses conform to the; Typical e-mail Address and Alias Names as indicated in Appendix E.

iv. to administer, document and manage the e-mail and Internet systems and adhere to any SLAs regulating these services.

v. to administer and manage procedures must be documented and in position of being used in audits.

vi. to carry out audits on behalf of CIMU and Heads of Department/Entity to ensure compliance with policies and Directive according to the provisions in Appendix C.

vii. to maintain all technical information and the Internet addresses resident on e-mail accounts correct and to be able to reproduce any configuration information that may be required by CIMU.

viii. to invoice CIMU for e-mail Services.

ix. to maintain and publish a list of Internet Service Providers licensed in Malta and approved for the transfer of classified information.

x. to create, amend or delete e-mail and Internet accounts as requested by CIMU or Heads of Department/Entity or their designated delegates. This includes the transmission of this Directive to new Account Holders via e-mail.

xi. to carry out necessary operations as directed by CIMU in relation to Anti Spam and Counterfeit e-mail matters.
03. Heads of Department / Entity

i. to encourage the use of e-mail and Internet within their department/organisation, especially to Knowledge Workers.

ii. to ensure that the e-mail and Internet Services are provided to staff members who would be able to perform their duties better with these services.

iii. to inform the Agent of any new Account Holders that are to be provided with e-mail and/or Internet Services, and of any e-mail accounts that are to be amended or deleted (e.g. deleting an account in the case of a staff movement or resignation).

iv. to ensure that all e-mail and Internet Account Holders within the department are trained in the use of e-mail and Internet.

v. to ensure that any ‘bulk mail’ is only sent in cases were it is directly contributory to the business of the Department or Entity.

vi. to audit the use of the e-mail and Internet Services, with assistance from the Agent, on an individual Account Holder basis.

vii. to liaise with CIMU in the selection of an appropriate acronym/title for the e-mail address of their organisation.

viii. to liaise with CIMU on any changes that have to be effected in e-mail addresses in the case of a change in organisation name, as soon as possible after the official change of name.

04. Account Holder

ix. to adhere to this Directive when using e-mail and Internet Services. Specific guidelines as to best practices in etiquette are attached in Appendix A.

x. to communicate with other public officers via e-mail whenever possible, even when initiating correspondence.

xi. not to use e-mail and Internet for prohibited purposes and abide by the Restrictions defined in Appendix B attached with this document.

xii. to keep the passwords for their e-mail and/or Internet Services secret and secure.

xiii. to exit and log out of their e-mail account and/or Internet Service if they are to leave their computer unattended.

xiv. to maintain their electronic mailbox according to procedures communicated by the Agent.

xv. to maintain any personal details correct.
xvi. to ensure that the Agent installs the latest approved version of the e-mail and Internet software products on their computers.

xvii. to ensure that all official e-mails are actioned according to department policy and that personal e-mails are deleted in the event that they are to terminate employment with the department or that they are going to relinquish the direct control of any electronic mailbox. Sanctions on use of e-mail are indicated in Appendix D.

viii. to tag all electronic communications according to the Classification of e-mail as indicated in Appendix F.

ix. to use e-mail for personal purpose in exceptional circumstances only. Sanctions on use of e-mail are indicated in Appendix D.

x. to report to CIMU any occurrence of Spam and Counterfeit e-mail.

6. Directives

6.1 Creation of e-mail and Internet Accounts

Heads of Department / Entity or their designated delegates shall:

1. Formally submit a request to the Agent to create e-mail and/or Internet accounts as necessary, using proper forms as directed by the Agent.

2. Ensure that the prospective Account Holder is aware of the Policy and Directives on e-mail and Internet Services.

The Agent shall:

1. Create the e-mail and/or Internet accounts within the defined timeframe as per SLA from receipt of a proper request from the Head of Department or his/her designated delegate.

2. Conform to the typical e-mail Address and Alias Names as indicated in Appendix E.

3. Transmit a copy of the Policy and this Directive to new Account Holders via e-mail.

4. Issue periodical invoice to CIMU in accordance to the contract.
6.2 Updating the version of the e-mail and Internet browser software

The Agent shall:

1. Ensure that CIMU is informed of all new versions of the e-mail and/or Internet software.

2. Obtain and install updated versions of the e-mail and Internet software within the defined timeframe as per SLA on all computers that may be connected to the Malta Government Network for authorised use of the e-mail and Internet Services.

3. Alert the relevant Head of Department if the e-mail and Internet software cannot be updated within the required timeframe and inform him/her of the date when the service will be provided.

4. Issue periodical invoice to CIMU in accordance to the contract.

The Central Information Management Unit shall:

1. Assess the merits or otherwise of upgrading the e-mail and Internet software and issue instructions to the Agent accordingly.

2. Subsequently update the relevant Standards.

Account Holders shall:

1. Make suitable arrangements with the Agent to have the current version of the e-mail and/or Internet software installed. When technically possible, the upgrade will be carried out automatically via the Logon Script or other electronic interfaces.

6.3 Ongoing management of e-mail and Internet accounts

Account Holders shall:

1. Adhere to procedures communicated by the Agent for the management of their e-mail and/or Internet accounts.

The Agent shall:

1. Take corrective action within the defined timeframe as per SLA from receipt of a registered call from the appropriate authority within a department regarding a technical fault or breakdown in the e-mail or Internet Service.

2. Alert Account Holders if a technical fault cannot be resolved in the required timeframe and inform the Account Holder of the required action, how the fault is to be resolved and by when.

6.4 Amendments of individual e-mail Addresses and Aliases

Typically such directive would be applicable in instances were a change of Account Holder surname is required.

The Head of Department or his/her designated delegate shall:

1. Formally submit a request to the Agent with relevant details to amend an individual e-mail account as necessary.
The Agent shall:
1. Amend the individual e-mail account as soon as possible and not later than two working days from receipt of the formal request from the Head of Department or his/her designated delegate

6.5 Amendments of groups of e-mail Addresses and/or Aliases

Typically such directive would be applicable in instances were a change in department name is required.

The Head of Department or his/her designated delegate shall:
1. Formally submit a request to the Agent through CIMU to amend details of whole groups of accounts as necessary, as soon as possible after the relevant change occurs.

The Agent shall:
1. Amend those affected e-mail accounts as soon as possible and not later than one working week from receipt of the formal request from CIMU.

6.6 Suspension and Termination of e-mail and/or Internet Services

The use of such directive is in cases; of disciplinary action, on the transfer of an Account Holder from one Department/entity to another, termination of employment or when the services are no longer required.

The Head of Department or his/her designated delegate shall:
1. Formally submit a request to the Agent to suspend and/or terminate the e-mail and/or Internet Services of specified Account Holders as necessary.

The Agent shall:
1. Suspend and/or terminate the e-mail and/or Internet Service within the defined timeframe as per SLA upon receipt of the formal request from the Head of Department or his/her designated delegate.

6.7 Temporary unavailability of e-mail and Internet Services

The Agent shall:
1. Inform Account Holders about routine downtime of the e-mail and Internet Services and endeavour to alert Account Holders at least 24 hours in advance of extraordinary circumstances, which will cause a temporary unavailability of the services.

2. Keep Heads of Department/Entity informed on progress to resolve any extraordinary downtime affecting the e-mail and Internet Services every 4 hours.
6.8 Abuse of the e-mail and Internet Services

In cases where the Head of Department or his / her designated delegate deem that the use of the e-mail or Internet Services is abusive the following action shall be taken by:

The Head of Department or his/her designated delegate shall:
1. Inform the Account Holder that his / her use of the service is deemed to be abusive.
2. Request the Agent to assist in carrying out a compliance audit. Depending on the extent of the audits, the department may be charged for the audit service.
3. In the event that the Account Holder persists in the abusive behaviour, request the Agent to deny the Account Holder access to the relevant service, in order not to jeopardise the integrity of the system or the interests of the Government.

The Account Holder shall:
1. Immediately refrain from his/her abuse of the Government e-mail and / or Internet Service on receiving a communication from his / her Head of Department that his / her use of the service is deemed to be abusive.

The Agent shall:
1. Carry out a compliance audit at the request of the Head of Department or his / her designated delegate.

The Central Information Management Unit shall:
1. Liaise with Heads of Department / Entity and / or their designated delegates and with the Agent as necessary until a satisfactory outcome is achieved.

6.9 Coming into force of the Policy

This paragraph has been left intentionally blank.

6.10 Temporary delegation of use of a mailbox

The Account Holder shall:
1. Ensure that the delegated person is aware of the responsibilities of an Account Holder.

6.11 Occurrences of Spam and Counterfeit e-mail

The Account Holder shall:
1. Forward to CIMU a copy of the offending mail for an immediate investigation once Spam is received. To ensure prompt handling of the complaint, please include the following:
   a. The subject line should read: "SPAM: (subject of offending mail)."
   b. The e-mail address of the sender in the body of your mail.
   c. A copy of the offending mail, including complete headers.
7. Supporting Documents

In Support to this Directive, the following Policy and Standards refer:

01. CIMU P 0010:2003 Electronic mail and Internet Services Policy
02. CIMU S 0010:2003 Electronic mail and Internet Services Standard

8. References

1. Acts and Regulation

2. CIMU Policies, Standards and Directives ([http://www.cimu.gov.mt])
   a. CIMU S 0001:2003 Office Automation Software Standard
   b. CIMU P 0014:2002 Web Filtering Policy
   c. Generic e-mail Accounts Policy
   d. Internet Domain Name Policy (in progress)

9. Modification history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>01.04.2002</td>
<td>Initial Release</td>
</tr>
<tr>
<td>2.0</td>
<td>01.07.2003</td>
<td>First Scheduled Review – Minor changes to the document format.</td>
</tr>
</tbody>
</table>


10. **Maintenance and review cycle**

    Maintenance and review of this directive is set for six months after the initial release as indicated in the effective date. Subsequent review to this directive shall be based on a twelve month cycle.


**Signature and stamp**

Joseph R. Grima

**Permanent Secretary, Office of the Prime Minister**
Appendix A - E-mail Etiquette

1. Do not use UPPER CASE for an entire message. It is harder to read and is considered as “shouting”. If emphasis is required for part of a message bold or italics may be used to good effect.

2. Be careful about the tone used and do not make assumptions about the tone others are using. What may sound funny in speech may be viewed as aggressive, abrupt, rude or sarcastic when sent as e-mail.

3. Never send an e-mail in anger. Even if one regrets sending a particular message one is almost never in a position to delete it.

4. Always remember that an e-mail is simply an electronic letter. It can be forwarded to others, it can be printed, and it can stay around for a long time.

5. Do not forward e-mail without the sender's permission.

6. Keep messages concise and to the point.

7. Remember to select the most appropriate medium at your disposal when communicating. In certain instances speech, telephone, post, fax or other media may be more appropriate than e-mail.

8. Include a return address on any ‘bulk-mail’ to allow any recipient in any such message to request to be excluded from any future related messaging.

9. Not use the service in connection with surveys, contests, pyramid schemes, chain letters, junk e-mail, spamming, promotional materials or any other form of duplicative, unsolicited or unauthorised advertising messages (commercial or otherwise).
Appendix B - Restrictions on use of e-mail and Internet Services

B.1. E-mail

1. Impersonate or forge the signature of any other person when using e-mail.
2. Amend messages received in a fraudulent manner.
3. Gain access to, examine, copy or delete another person's e-mail without the necessary authorisation from the person concerned.
4. Disclose their password or other means of access.
5. Use someone else's password or other means of access in a computer.
6. Use e-mail to harass or defame any person or group of persons.
7. Use e-mail to conduct any personal business or for commercial or promotional purposes.
8. Send as messages or attachments items that may be considered offensive, pornography, illegal material, chain letters, or junk mail.
9. Send e-mail in bulk unless it is formally solicited.
10. Place Government-assigned e-mail address on non-official business cards.
11. Send trivial messages or copy messages to people who do not need to see them.
12. Send unsolicited mass e-mailing to more than twenty-five (25) e-mail users, if such unsolicited e-mailing provoke complaints from the recipients.
13. Use the service of another provider, but channelling activities through a MAGNET account as a re-mailer, or use a MAGNET account as a mail drop for responses.

B.2. Internet

1. Download files from the Internet without adhering to existing policies on virus control.
2. Download material (including software) that is not work-related.
3. Enter into any contract over the Internet without approval from the appropriate Head of Department or his/her delegate.
4. Use the Internet to conduct any personal business or for personal commercial purposes.
5. Post a single article or advertisement to more than ten (10) Usenet or other newsgroups, forums, e-mail mailing lists or other similar groups or lists.
6. Post to any Usenet or other newsgroup, forum, e-mail mailing list or other similar group or list articles, which are off-topic according to the charter or other owner-published FAQ or description of the group list.
B.3. Restrictions on Internet Access

Government is duty bound to prevent access to illegal material and also has a moral obligation to prevent access to material which although not illegal may be harmful to society. For this reason, adequate filtering technology will be used and further matters on this subject are covered in the Policy titled - Web Filtering, and related documents as per References section.

B.4. Restriction to e-mail specific to combat Spam

E-mail message in which the number of recipients exceeds 25 recipients will be blocked.
In addition to the above rule, if the size of message is greater than 1.5Mb than that e-mail message will be blocked too.
Appendix C - Management Information and Audits

C.1. Management Information

Tracking and auditing the use of e-mail and Internet are necessary to ensure that:

1. The best use of these facilities is made in providing a service to the public and communicating within the Public Service.
2. Personal use of these services is for exceptional purposes, according to policy.
3. The security of confidential and/or official information is maintained.
4. Unauthorised activity, such as hacking; spamming, Denial of Service Attacks, Malicious Relay Attempts and any security breaches are detected.

The Agent shall produce management reports that will highlight overall patterns of usage of e-mail and Internet for each department on a monthly basis. This information shall be made available to the CIMU and to the Head of Department or his/her designated delegate.

C.2. Audits

The Agent shall, under the guidance of the CIMU, periodically carry out audits on the use of the e-mail and Internet Services.

E-mail usage audits shall explore the following data:
1. Name of the sender.
2. Destination address or addresses.
3. Date and time sent of e-mail.

Internet usage audits shall explore the following data:
1. Date, time and duration of access.
2. IP Address of the computer accessing the Internet.
3. URLs/IPs accessed.
4. Name of any file accessed or downloaded.

C.2.1 Audits requested by the CIMU

The emphasis of audits requested by the CIMU shall be on the overall usage and performance of the e-mail and Internet systems, and not on the usage patterns of individual Account Holders. On the basis of the audits carried out, the CIMU shall advise individual Heads of Department/Entity or their designated delegates on any action it may deem appropriate.

C.2.2 Audits requested by Heads of Department/Entity

The emphasis of audits requested by Heads of Department/Entity or their designated delegates is expected to be on the usage of the e-mail and Internet Services made by individual Account Holders as well as general performance within their respective departments. On the basis of the audits carried out, the individual Heads of Department/Entity may take any action regarding individual Account Holders that they may deem appropriate.
Audits shall not routinely involve the content of e-mail messages or attachments. Heads of Department/Entity may, however, request the Agent to conduct audits into the content of work-related e-mail at any time without prior notice or Account Holder consent.

In cases where breaches of policy or improper use of the e-mail service is suspected, the Head of Department shall request the employee's consent prior to auditing the content of e-mails classified as 'personal'.

Account Holders shall however be aware that:

1. The contents of all messages created, sent or received using the Government's e-mail system, and

2. Information on websites visited, and software/data downloaded using the Government's Internet Service

may be accessed in accordance with the provisions of the Electronic Commerce Act, the Criminal Code and the Secret Services Act.
Appendix D - Sanctions on use of e-mail

Communication by e-mail that is carried out within the provisions of this Directive is approved. Account Holders are encouraged to communicate with other Account Holders by e-mail on all business internal and external matters.

The use of the Internet is approved for the conduct of research and other activities directly related to the working duties of the Account Holder and for the transmission of e-mail.

D.1. Personal Use

Personal use of e-mail and Internet is allowed only in exceptional cases and provided that this does not interfere with the performance of the Account Holder’s duties or those of other Account Holders.

Personal use shall not include use:

1. That requires substantial expenditure of time.
2. For private business, personal gain or profit.
3. That impedes the efficiency of e-mail or Internet Services.
4. That clogs mailboxes with large numbers of messages or bulky attachments.
5. That would violate or breach any legislation and regulation.
6. That would violate or breach the Code of Ethics.

On no account shall exceptional personal use disrupt the system and/or harm Government’s reputation.

E-mails shall be deemed personal only if the Account Holder classifies them as ‘Personal’ from that appropriate functionality within the software.

D.2. Official Use

An official e-mail is such when it is created in the official conduct of business and is evidence of Government’s policies, decisions, procedures or business or contains information or data of value to Government.

The e-mail equivalents of signed letters, letter-minutes, internal memoranda and circulars fall within the definition of official e-mail.

D.2.1. Use of Official e-mail

Account Holders are encouraged to transmit and respond to official correspondence via e-mail whenever:

1. All intended recipients are known to have access to the e-mail service; and
2. Any documentation to be attached is available in soft copy. In this instance the Account Holder must use document software formats for which all recipients have compatible software.
In particular Account Holders shall:

1. Copy e-mails only to those people who have a need to know of the subject in hand.
2. Use e-mail to respond to e-mails received from the public.
3. Respond to e-mail in the language in which it was received (Maltese/English).
4. Include full name, designation and work location at the bottom of each official e-mail sent.
5. Send and action e-mails which are official communications according to departmental policy and according to the guidelines below for transmission of classified information via e-mail.
6. Correctly classify each e-mail to be sent using the functionality of the software according to the level of security to be applied to the information, based on the Classification of e-mail as indicated in Appendix F.
7. Delete classified information from the e-mail inbox immediately upon retrieval of the information.
8. Store and administer classified information in accordance with departmental policy on classified information.
9. Make use of automatic signature file to include full name and designation with outgoing e-mail messages. The signature file should also include a disclaimer.

D.2.2. Filing of Official e-mail

Account Holders shall, within one working week:

1. Print out and file hard copies of all official e-mails, including attachments, according to the filing system adopted by their department.
2. Ensure that they print both the message text and the message properties.
3. File only official e-mail messages.

The electronic copy of the printed and filed hard copy is than to be deleted, unless it is required by the Account Holder to exercise his duties. An example of such need would be to reply copying to the message in the immediate future (one-two days). No specific official time frames are being set and it is being left up to the good judgement of the Account Holder not to amass messages in the mailbox.

Account Holders may also wish to refer to Section 7.7 of the Manual on Registry Services – November 1990, which deals with Communications Received Direct.
Appendix E - Typical e-mail Address and Alias Names

The standard e-mail address and alias naming conventions are determined and maintained by the Central Information Management Unit (CIMU).

The domain name `gov.mt` is in operation for Government and is currently running in parallel with the domain name `magnet.mt`, which shall eventually be phased out.

E-mail addresses for public officers all end with the domain name `gov.mt`, e.g. `mary.borg@gov.mt`. In the case of public sector entities, the CIMU may consider approving the use of the entity name at the third domain level, e.g. `joseph.borg@appogg.gov.mt`.

The use of the entity name at the third domain level for schools and general administration purposes, i.e. `xxxx@educ.gov.mt`, for teachers and school environment, is also acceptable. The domain name is however not applicable for the administrative side of the education sector e.g. general administration of the Education Ministry.

E.1. E-mail Address

The general syntax of an e-mail address is the following:

`<First name>.<Last name>@gov.mt`, e.g. `mary.borg@gov.mt`

In the event that such an address is already in use by another legitimate Account Holder, then the second up to fifth name initial will be inserted between the first and last name. In case where no known initials exist, then an initial will be assigned according to the alphabetic sequence. The default stance is to use as minimum number of initials as possible.

E.2. System Specific e-mail Alias

The general syntax of the System’s Specific alias for an e-mail address is the following:

`<Last name> <First name> at <Entity name>`, e.g. `Borg Mary at OPM`

In the advent that such an address is already in use by another legitimate Account Holder, than the second up to fifth name initial will be inserted after the first but before the “at”. In case where no second up to fifth name initials exist, than an initial will be assigned according to the alphabetic sequence. The default stance is to use as minimum number of initials as possible.

`<Entity name>` refers to a particular Government organisation. The name is determined by the CIMU in consultation with the head of the organisation in question. The CIMU maintains naming conventions for Entity Names in order to achieve semantic consistency and keeps a database of Entity Names in order to prevent duplication. Entity Names were originally limited to Ministry acronyms, e.g. OPM. The CIMU is gradually introducing aliases referring to specific Government departments and entities, e.g. DOI, in consultation with the respective heads. When organisations are already referred to by their acronym, for example, DOI, NAO, this acronym will be used. When they are commonly referred to by a short title (e.g. Customs, Treasury), this may be used.

E.3. Generic e-mail

The naming of generic e-mail accounts is regulated by the Generic e-Mail Account Policy and Directive available from the CIMU Website.
Appendix F - Classification of e-mail messages

Account Holders are to ensure that, where appropriate, e-mails are security classified, using the categories specified below.

F.1. Encrypted communications

Information, the unauthorised disclosure of which could endanger national security, cause serious injury to the interests or prestige of the nation, or any governmental activity thereof, or would be of great advantage to a foreign power.

In this case such information shall only to be transmitted via e-mail over the MAGNET in encrypted format (Secure Mail).

F.2. Non encrypted communications

F.2.1. Confidential

Information, the unauthorised disclosure of which, while not endangering the national security, would be prejudicial to the interests or prestige of the nation, any governmental activity, or would cause administrative embarrassment, or difficulty, or be of advantage to a foreign power.

Information relating to individuals be they members of the public or Public Officers shall also classified be as Confidential.

Such information shall not be transmitted over the open Internet.

F.2.2. Private

Information the unauthorised disclosure of which would be inappropriate or premature, and is intended for the recipient’s eyes only. Such information may not be transmitted to the public, but may be transmitted over the Government e-mail system. Such information may not be forwarded further than Account Holder's mailbox.

Such information is only to be transmitted electronically over the open Internet to persons external to the Public Service if they are using an Internet Service Provider licensed in Malta or they constitute part of Established Organisations being: other Governments or Supra-national organisations such as the European Commission, United Nations, OECD, etc. and their sub organisations such as InfoDev, WHO, FAO, UNESCO, UNOPS, PUMA, SIGMA, etc.

These are most easily identified by Internet domains that fall within an official naming convention (e.g. “gov.uk” for the UK Government, “cec.eu.int” for the European Commission).

F.2.3. Personal

Information that is personal and not connected with business use.

Personal e-mails sent shall be classified as such. Personal e-mail received should be removed from the e-mail system.

Personal data fall under the protection of the Data Protection Act.

F.2.4. No Classification

Information which is not in the public domain but which may be reproduced as required for internal use. Such information shall not be considered as classified information.