COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 26.10.2009
SEC(2009) 1412 final

COMMUNICATION FROM THE PRESIDENT, IN AGREEMENT WITH VICE-PRESIDENT S. KALLAS

Commission policy on the internal use of email

TABLE OF CONTENTS

Commission policy on the internal use of email

1. CONTEXT

The Commission considers email to be a core communication service that is critical to the continuity of its operations[1] and plays a key role in the conduct of our work. How well staff communicate by email not only reflects on them as individuals, but also impacts on the organisation as a whole.

Like many other organisations, the Commission faces growing difficulties with email overload, the time spent managing mailboxes, the rising costs associated with transmitting documents via email and questions of legal liability relating to the transmission and retention of emails.

This document establishes a comprehensive Commission Policy on the way email should be used:

– It is *not* about introducing new rules but rather about consolidating existing administrative notices, staff policy rules and best practice recommendations.

– It is *not* about setting up new arrangements for documents retrieval, filing and archiving; these issues are covered by the new Ares document management system.

– It is *not* about imposing a straight jacket to all services but rather about setting up a general framework conducive to a better use of email within the Commission.

– It is about responding to the challenges of email overload and the exponential increase in spending for the operation of the Commission email service.

In practical terms, it advises users on how to make more efficient and responsible use of email and makes them aware of the constraints under which the email service operates.

2. PURPOSE

The purpose of this Communication is to establish a reference framework which will be made operational through implementing measures to ensure a smooth transition from current operating practices to a more efficient electronic communications environment.

Its goals are to:

- Establish a basis upon which to improve existing practice and develop new working methods with email.

- Ensure that users of the Commission's email system fully understand the guidelines on its acceptable use and the specific requirements placed upon them.

- Increase awareness of consequences of abuse.

---

[1] Commission Staff Working Document SEC(2006) 899 of 12.7.2006 "Framework for business continuity management in the Commission".

It does not lay down rules to cover every possible situation, but sets out the general principles that staff should apply when using email.

3. SCOPE

This Communication covers the use of email for sending and receiving messages internally and transmitting messages externally, and addresses both business and personal usage. It extends to the administration of the user's mailbox including the means, methods and decision criteria for storing email messages and their corresponding attachments. It applies to all users having access to a Commission email account, i.e. in one of the following forms:

– “mailbox_name@ec.europa.eu”

– "mailbox_name@ext.ec.europa.eu"

– "mailbox_name@publications.europa.eu".

This includes personal, functional and temporarily allocated mailboxes

4. RISKS

The Commission recognises that operating an email service involves the following risks to the Commission’s reputation, business efficiency, operational environment and staff well-being, of which users should be aware and take into account when using email:

(1) Possible adverse effects on the reputation of the Commission when staff communicate inappropriately with citizens, stakeholders, businesses and other organisations.

(2) Legal and financial liability relating to nature of message content, its disclosure and retention (confidentiality, data protection, defamation and evidentiary value).

(3) Disruption of data transmission services potentially affecting the continuity of the Commission’s operations.

(4) Excessive data storage costs.

(5) Inappropriate use of email that can have a negative impact on staff relations.

(6) Reduction of productivity through non-compliance with guidelines on effective and efficient use.

(7) Exposure of the Commission’s computing environment to viruses, spyware and malicious software.

5. BEST PRACTICES

The Commission encourages initiatives[2] that promote more secure, effective and efficient use of the email system. Clearly written messages with focused content and properly structured format make for more effective professional communication.

The following seven best practice principles for the use of email should be respected as new tools and facilities become available, and users should take note of the specific best practices described in Annex 2 that conform to these general principles:

(1) Pull not push

This concept seeks to minimise the number of document attachments transmitted through the email system by promoting the working method whereby users send links to documents in the body of an email message whenever this option is feasible, rather than attach documents to the email message. New document management (ARES/HERMES) and collaborative working tools (My IntraComm corporate portal) will help to reinforce this principle. Annex 2 describes the working method in detail.

(2) Need to be informed

This involves a common understanding of who needs to receive directly an email message and who should receive a copy. The direct addressee(s) or "To:" recipients in the message distribution list are expected to take direct action and/or respond. However, the "Cc:" recipients should be strictly limited to users requiring the information in the message to perform their duties. Furthermore, mailing lists should be limited in size, supervised by their owners and regularly updated. Staff should be prudent when using the Reply to All function and should normally never reply to mailing lists. Annex 2 outlines the protocol guidelines for applying this principle.

(3) Observance of email communication protocols

This involves a set of guidelines on when to use email and when to use alternative means of communication. It also builds on the Optim@il best practice working methods in terms of creating effective message content, smart distribution settings, secure communications and optimal storage techniques. Annex 2 covers this catalogue of best practice techniques.

(4) Proper deployment of email in business processes

This concerns the inappropriate and excessive use of email to drive business processes and act as the information system underpinning the process rather than to support the communications within the process. This is fully explained in Annex 2 and is directed at those users who perform roles as process managers or process owners.

---

[2] In 2001 the Email Service led a best practice workgroup which in 2003 produced an Optim@il best practice guide: http://www.cc.cec/home/dgserv/digit/corporate_ict/infrastruct/corp_systems/email_tech/optimail/index_en.htm.

(5) Reporting spam/abuse/spoofing

This is the principle whereby users take responsibility, as part of the email user community within the Commission, for reporting issues and events that could adversely affect the proper and correct functioning of the email system. Annex 2 provides sample cases and procedures to be followed.

(6) Using the Out of Office Assistant

The email user community must be responsible for informing other users (both the internal and external email community) if they are not available to respond to incoming messages. The Out of Office tool should always be used when users are not in a position to read and/or respond to messages for one working day or more and no delegations or other mechanisms (eg internal auto-forward) are in place to actively manage incoming email[3].

(7) Mailing list management

The inappropriate use of mailing lists carries risks of sudden surges in email traffic. This leads to degraded service, information overload and increased mailbox maintenance for mailing list members. Using mailing lists for a limited number of well-defined purposes, maintaining up-to-date membership lists and suppressing reply options will greatly reduce these risks.

6. LEGAL CONSIDERATIONS

Email messages are increasingly produced as evidence in legal cases and disciplinary actions. Consequently, users should be aware of their obligations under both the Staff Regulations[4] and civil and criminal law when using the Commission's email system.

The use of the email system for illegal or irregular purposes, in any way that might disrupt the functioning of the service itself or in any manner contrary to the interests of the Commission is prohibited.

In particular, the following are contrary to the principles laid down in the Staff Regulations or in other provisions applicable to officials and are consequently prohibited:

- Messages involving remarks of a defamatory, discriminatory (e.g. based on sex, race or disability), harassing, libellous, obscene, offensive or threatening nature[5].

- Messages unlawfully disclosing confidential information, including personal data, to recipients who do not have a need to know.

---

3 As an example "I am not available to read email, contact person name etc"; one not need specify fixed periods or other information that could compromise a user's personal security.

4 See Administrative Notice No 45-2006/15.09.2006 and Articles 11(1),12 and 12a of the Staff Regulations.

5 This is not contrary to the freedom of expression recognised under Article 17a(1) of the Staff Regulations.

- Distribution of messages of a non-official character that are unsolicited and addressed to a large number of recipients and/or featuring requests for recipients to forward such messages widely (for example chain mail, spam or personal advertisements).

- Forged messages.

- Messages which seek to disguise the identity of the author.

- Messages from another user's email account unless authorised.

- Deliberate deletion of messages relating to internal or external enquiries e.g. as part of an administrative investigation.

- Messages containing EU classified[6] information (EU TOP SECRET, SECRET UE, CONFIDENTIEL UE, RESTREINT UE[7]).

Messages transmitted inside the Commission must use the encryption tool provided for secure e-mail (currently SECEM[8]) when these contain sensitive non-classified business or personnel information (e.g. tendering details or medical data). Similarly, transmission of such information to third parties should always be conducted via secure IT systems.

Staff should be aware that any messages or information sent, in particular when transmitted externally using the Commission's email system, are statements that are attributable to the Commission. Depending on the context, an email can carry the same weight in law as a letter written on headed Commission paper.

Staff should take particular care when sending messages externally which constitute information that a third party may rely upon in accordance with the relevant rules or the Code of Good Administrative Behaviour[9].

Furthermore, staff should note that even with a disclaimer, a connection with our institution exists and a statement could be imputed legally to the Commission. Therefore, no one should rely solely upon disclaimers as a way of protecting the Commission from the personal comments and opinions expressed by an individual user. Expressions of opinion should be avoided while using the Commission's email system. Any reservation that the content of the message expresses personal views should be made explicitly in the message body itself instead of relying on this being implicitly understood through an appended standard disclaimer.

Any investigation into abuse or infringement of this email policy and, in particular, these legal aspects may lead, where appropriate, to disciplinary or other legal sanctions.

---

6 http://www.cc.cec/security/help_advice/information_en.htm.

7 The RUE system is however available for those needing to send and receive 'RESTREINT UE' documents.

8 http://www.cc.cec/home/dgserv/digit/everybody/e_mail/secem/index_en.htm.

9 Code of good administrative behaviour - http://www.cc.cec/pers_admin/code/conduct/index_en.html.

7. PERSONAL USE

The Commission's email system is provided to staff for performing job-related functions and for general staff welfare matters (e.g. contacts with schools, accommodation agencies, local and central government offices, pension offices). Limited, occasional, or incidental use of email for personal, non-professional purposes is acceptable. For instance, users may also, or alternatively use their personal webmail services, provided that they comply with the Commission's administrative notice[10] on acceptable use of the information and communication technology services, which covers email and internet use, and that they take care to avoid introducing viruses or spyware (malware) when accessing private webmail through the Commission's data network.

For security and spam prevention reasons, users should be prudent in divulging their Commission email address for personal matters.

The fundamental rights to confidentiality of communication and privacy are guaranteed. However, in exceptional cases such rights may – in accordance with the applicable regulations - be limited, for example in cases of investigations concerning fraud and other illegal behaviour (see section 9 below) or in cases where there are grounds for suspecting abuse (ref. section 6 above).

Acceptable personal use does not include private emails for profit-making or commercial purposes and shall not conflict with users' contractual obligations or Staff Regulations.

Personal emails should be clearly indicated as such either by using the message property settings, or by use of a disclaimer or by an indication in the message header.

8. MESSAGE STORAGE

The primary purpose of the Commission's email system is to facilitate communication, not to provide document archiving and data storage. In fact, the email system has no formal repository or archival role whatsoever. In order to manage email storage appropriately users are required to do one of three actions on a message in a timely manner – REGISTER the message where necessary[11], FILE it[12] and/or DELETE it.

While it is recognised that existing working practices depend heavily on email storage facilities, the launch in 2008 and 2009 of two new corporate tools to support document management and collaborative working should have a significant impact in reducing dependency on email message stores as informal information reference repositories to support the Commission's business processes.

Centralised and harmonised electronic document management facilities underpinned by DGs' official filing plans are in the process of being implemented through the ARES system being progressively rolled out across all DGs. This will impact both directly and indirectly on email storage requirements:

---

10 Administrative Notice No 45-2006/08.06.2006 "Acceptable Use of the Commission's ICT services (PC equipment, email and internet acess systems, telephone, fax and mobile phones)".

11 In Ares or Adonis.

12 Either in a personal folder opened in Outlook, or on a drive.

(1) Where an email message qualifies as a document, it will have to be registered and filed in accordance with document management rules and guidelines[13] using the ARES system.

(2) The central e-Domec compliant document repository HERMES will act as a fully accessible and commonly shared platform for electronic document storage, update and retrieval. This document management system will facilitate access to documents through links according to the "pull not push" best practice principle described in section 5 above.

The launch of the new My IntraComm corporate portal, which replaces Intracomm will gradually stimulate changes to collaborative working methods. This new technology will in the future support activities such as on-screen workflow, shared workspaces, drafting and reviewing tools, project management utilities, and other features in an integrated environment. Over time, this development will reduce the need to use email messages to drive standard workgroup operations and at the same time facilitate easily accessible workgroup repositories underpinning collaborative working structures and practices.

The emergence of these new tools will impact upon working practices and gradually reduce reliance on email storage capacity as a reference system for working documents and associated commentaries. The Commission currently invests considerable resources in data storage media for the email system and it is important that this investment is used economically and contained in the future so that resources can be switched to meet the emerging storage needs of the new tools.

It should be noted that the Commission is not in the position of some publicly available free email services which offer considerable amounts of individual storage capacity — their revenue is based on commercial profit, whereas the Commission uses public funding. It is true that over the years the cost of storage has gone down, in particular the price of disks for home use in electronics stores; however secured heavy duty equipment required for professional use in data centres remains extremely expensive.

One major area of concern for the on-line storage of emails has been linked with the introduction of the EAS (Email Advanced Storage) system, which automatically compresses and removes messages from the mailbox, transfers them to another storage facility and uses a reference link to maintain their presence in the mailbox. This measure was brought in to alleviate pressure on fixed storage capacities in on-line mailboxes. However, the storage capacity requirements for EAS have grown exponentially since its introduction, in the absence of any control on its size. The spiralling costs need to be contained, so the physical capacity of EAS will have to be limited in the longer term. This means that older messages stored in EAS will have to be erased to make way for newer arrivals.

Another area that will require change concerns the Public Folders facility within the email system, as it has been utilised as a shared information space. Actions are already under way to reduce dependency on this facility and alternative facilities will be required as this functional aspect of the email system will become obsolete in the future for technical reasons.

[13] SEC(2006) 353 "Guidelines for the registration of e-mails in the framework of the Electronic Archiving and Document Management Policy of the European Commission (e-Domec)".

It is expected that the best practice of email usage and the emergence of new working tools will go a long way towards containing the mass of unnecessary email storage and free-up IT resources for more productive uses. But it may prove necessary to accompany the change with technical constraints, which will further encourage good use of email, so that messages and attachments with no storage value are quickly and definitively removed from the system.

The following rules will be phased in (some only as a last resort, if the other measures prove insufficient to stem the rapid growth of email cost to the Commission) — see Annex 1 for proposed future target parameters:

(1) All messages that are retained using the Email Advanced Storage system (EAS) will be permanently deleted after a fixed period of time (x years).

(2) Document attachments for internally generated emails should be limited to file formats necessary for work-related purposes. Moreover, large files (especially those with multi-media format with embedded video, music and images) should only be attached to e-mails for fully justified professional reasons.

(3) The current service of automatically storing messages in EAS will be gradually phased out and users are encouraged to manually select messages destined for EAS storage in order to take advantage of this facility.

(4) Mailbox messages in the Inbox folder that have been read but not filed as well as those remaining in the Sent items folder will be automatically deleted from the online email system after a fixed period of time (x months). An alternative storage system will be used as a failsafe mechanism to ensure this information can be retrieved if necessary. [This measure is intended only as a last resort; its introduction would require a pilot testing phase and availability of new tools for document management and collaborative working that offer alternative operational means of document and information sharing.]

For memory, the following existing rules are recalled:

(5) Individual mailboxes continue to be of a fixed and limited size[14].

(6) Documents that are freely available and directly accessible on the Commission's information systems should not be attached to emails nor stored within the email system — whenever possible, messages should feature only hyperlinks to these documents.

(7) Documents which fulfil the formal criteria for registration and filing must be registered and filed as such in the official document management system(s) in use in a

[14] Whereas the mailbox size will continue to be of fixed limit, an individual mailbox capacity can be increased in the case of an exceptional business reason (critical function, emergency etc.) by application from the DG IRM to DIGIT's Email Service. Such increases are granted by DIGIT within certain limits and under specific conditions, amongst which, where there is evidence that despite thorough mailbox administration (e.g. cleaning messages from the mailbox) being actively applied, the email traffic density is too high to allow effective use of the mailbox within the standard limits.

DG, where they will be retained in accordance with the Common (or, where appropriate, a DG-specific) Retention List[15].

This Email policy encourages more efficient communication and active mailbox management in order to improve the use of central email storage facilities and help users with classifying and filtering their message stores.

9. EMAIL PRIVACY

DG DIGIT routinely monitors statistics of the global volume of email traffic for the following operational and service improvement purposes:

- Service planning
- Service operations
- Cost analysis and resource allocation
- Configuration management of information resources
- Detection of abnormal activity levels that could lead to delays or blockage of the email system, thereby affecting the continuity of the Commission's operations.

The Commission has the right to review any electronic files and messages in cases of suspected breaches of legal or security obligations, and may check the contents of email messages under the conditions set out in the Commission's investigation procedures. Subject to appropriate authorisation this may include access to email message content and attachments without prior notification.

However, all monitoring and investigation activities have to fully comply with data protection rules.

It should be stressed that the Commission may be held liable for damages caused by its staff in the performance of their duties. As a result a member of staff may be held personally liable pursuant to Article 22[16] of the Staff Regulations.

10. ENCRYPTION

It must be assumed that internal or external electronic communications are by their nature not totally secure. Accordingly, particularly sensitive information should be transmitted by other means and where necessary encryption should be used.

---

[15] The common retention list for Commission files was circulated as a document from the Secretary-General: SEC(2007) 970 of 4.7.2007.

[16] Article 22(1) states "An official may be required to make good, in whole or in part, any damage suffered by the Communities as a result of serious misconduct on his part in the course of or in connection with the performance of his duties."

Only encryption software approved by ADMIN/DS and supplied by a DG's IT support team may be used for purposes of safeguarding sensitive or confidential information. This must provide the possibility for third parties to recover encrypted information when necessary.

11. CONTRACTORS AND EXTERNAL STAFF

Contracts between the Commission and companies or agencies supplying workers as contractors and external staff should contain a provision according to which their personnel is required to fully respect the conditions laid down in this Communication and that the company will take full responsibility for any breach. Furthermore, for email accounts assigned to non-Commission staff it should be mandatory that all messages (new, forwarded or replies) feature a footer identifying the author as external staff, and the company to which they.

12. ROLES AND RESPONSIBILITIES

The SG will be responsible for the organisational aspects of the use of the email system (i.e. this email usage policy) as part of its role and responsibility for electronic document management and archiving in the Commission.

ADMIN will be responsible for policies relating to use of the Commission's intranet and other central communication tools as an alternative to email, as part of its responsibility for internal communications; and for IT security matters.

DIGIT in collaboration and consultation with local IRM services within DGs will be responsible for the service support and delivery, including evolution of the service, which encompasses the technical enforcement of this policy.

The Communication establishing a business continuity management framework[17] identifies the roles and responsibilities of the key actors in the case of risks of disruption of the Commission's activities, including for maintaining the continuity of critical communication services such as the Commission's email system.

13. REVIEW

This email policy and its implementation will be reviewed initially three years after it comes into force and periodically thereafter to take account, inter alia, of emerging technological developments and organisational requirements[18].

[17] SEC(2008) 898 and 899 of 12.7.2006.

[18] Especially for crisis management and business continuity.

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 26.10.2009
SEC(2009) 1412 final

This document is available in English only

**COMMUNICATION FROM THE PRESIDENT,
IN AGREEMENT WITH VICE-PRESIDENT S. KALLAS**

Commission policy on the internal use of email

Annexes

TABLE OF CONTENTS

Annex 1: List of target operating parameters for future use of email

(1) Mailbox automatic deletion time limit (Inbox — Read & Sent Items): to be defined after operational impact analysis of the pilot exercise(s). Initial notional target – 6 months.

(2) EAS object lifetime limit: 7 years.

(3) In cases where attachments are required, recommended maximum size of internally bound message attachment: 2 Mb.

(4) Recommended maximum number of mailing list members: 150 (if exceptionally a larger mailing list appears to be necessary, its establishment and use should be carefully considered and justified and will require prior agreement by senior DG management).

(5) Recommended document formats for attachments for professional purposes: doc, rtf, xls, pdf, txt, ppt, zip, tiff, jpg, odt, ods, xps

Annex 2: Email best practice guidelines

Introduction

Email has evolved to the point where it has become the standard form of internal and external communication for all Commission staff. A consequence of this is that a number of initiatives have been taken in terms of awareness[1] and training[2] to ensure that maximum effectiveness is derived from the email communication tool. This annex aims to consolidate recommended best practice approaches in terms of effectiveness, efficiency, security, and staff morale.

The guidelines are grouped into the following three categories:

- ***Working methods*** — ways of creating and transmitting messages
- ***Communication protocols*** — a common user understanding of message distribution
- ***Data retention considerations*** — communicating information.

1. Working methods

Users themselves can be more consistent and efficient in the way they use email, thereby significantly alleviating pressure on the email system, on themselves and on their colleagues, including senior managers, who receive a growing number of messages that do not directly concern them. There is also considerable scope for staff to improve their communication style by being more selective in their use of email and by actively engaging other means of relaying and exchanging information such as phone or personal contact.

The following measures improve the way users interact with the email system and in so doing raise efficiency and effectiveness:

- **Alternative modes of communication**

Users should be encouraged to make full use of alternative forms of communication (e.g. phone, voice mail, personal contact, intranet), which in many situations can be preferable, more efficient, more secure and more productive than email.

- **Observance of email's seven functions**

Email is designed for:

– Transmission of official documents (e.g. final communication) using document links.

– Procedural collaboration (e.g. message exchange in pursuance of a complaint).

– Workgroup collaboration (e.g. evolution of a draft policy document) using shared file stores.

---

[1] Optim@il: http://www.cc.cec/home/dgserv/digit/everybody/e_mail/use_email/brochure/doc/top15_low_en.pdf.

[2] Syslog entry (2007) SY_OUTL2003_MAIL — Outlook 2003 — Manage your email more efficiently.

– Informal exchange of opinion on a focused issue (e.g. individual viewpoints on a particular issue).

– Personal exchanges without focus (e.g. general information exchange on a subject area).

– Automated notifications of an event (e.g. a workflow action for a procedure).

– Non-controversial private communications (e.g. personal appointments, information exchange).

- **Protection of identity**

Users should only disclose their Commission email address to outside persons if there is a professional need.

- **Segregation of personal and professional use**

Users should be encouraged to take advantage of the many free web email services available for their private email needs. This will reduce overload on the Commission's system and personal mailboxes. In cases where the Commission's email system is used for personal messages, they should be clearly indicated as such.

- **Common message structures**

– Subject headers

The subject header should never be left blank and should indicate purpose (action, info, log, etc). In case where an action is expected the subject header should be even more explicit, indicating theme / expected action / deadline.

– Priority (Importance)

The high priority flag should only be used for messages requiring action on the same day. The low priority flag should be used for personal exchanges.

– Sensitivity

This should be used whenever information is sensitive and in such cases users should seek the permission of the author of the message before forwarding it.

– Netiquette

Abbreviations, symbols and other short cuts often used in forums, blogs, and SMS messaging should be avoided as they can be a source of confusion and annoyance for the recipient.

– Format

In the case where a service has defined guidelines for message format standards including signatures, users are required to observe these guidelines for all email communications of a professional nature.

- **Attachments and links**

Wherever possible document attachments should be replaced by links to common drives or document repositories on web servers (see examples[3]). The development of collaborative tools across the Commission will further facilitate systematic use of this approach.

- **Common document format**

Whenever attachments are used, they should preferably be in one of the document formats recommended for professional purposes (doc, rtf, xls, pdf, txt, ppt, zip, tiff, odt, ods, xps).

- **Formal messages**

All messages of a formal nature should be logged in a document registration system — ARES (or Adonis, for DGs that have not yet migrated).

- **Disclaimers**

Disclaimers do not guarantee legal protection. Any protection they can provide will only be effective if disclaimers are correctly drafted in relation to the material concerned and if they reflect the actual practice of the Commission. The wording and format of an email disclaimer should be approved in each DG[4].

- **Out of Office**

"Out of Office" messages should be mandatory during absences of one working day or more and where no delegations or other mechanisms (eg internal auto-forward) are in place to actively manage incoming email. This form of message should conform to the DG's convention on format and information content (including alternative contact information). From the time the technology will allow for it, different Out of Office messages should be used for internal and for external recipients.

- **Politeness and professionalism**

Message tone must remain polite and avoid expressions that might be perceived as offensive or insulting by recipients. Email should not be used in situations of potential conflict. If an email requires a reply this should be executed in a timely manner (days, not weeks).

- **Malware, spam and phishing**

DG DIGIT's email service filters out a considerable amount of harmful and unsolicited emails entering the Commission. Nevertheless, users should be vigilant and avoid acting upon or forwarding or replying to suspicious email messages since these could contain viruses and spyware (malware) or be masquerading as a trustworthy entity, while attempting to acquire sensitive information such as passwords or private information (phishing). Such messages should be reported immediately[5] to the local IT Support Service as well as the Local Information Security Officer (LISO)

---

3 ABM/SPP Network: http://www.cc.cec/home/dgserv/sg/i/spp/index.cfm?lang=en&page=mm_network.

4 SG will make available a standard general corporate disclaimer approved by SJ.

5 Article 7 of Decision C(2006) 3602 on the security of information systems.

2. Communication protocols

The speed and ease of communication by email has not only encouraged the introduction of more recipients into the information distribution chain but also invited an increased number of replies and responses to replies. In the past, paper-based communications have been self-regulating by the nature of their lengthy production and transmission processes.

The net effect is that email traffic is getting denser and the average user's inbox becomes over-populated with messages. This reduces system performance and creates the added work to filter out the most relevant and urgent information.

One of the remedies to tackle this growth in information flows is to apply the "need to be informed" principle to the email distribution functions (To, Copy, Blind copy, Forward, Reply and Reply to All) by establishing the following protocols for using them responsibly:

- **Email distribution functions**

– Direct addressee function

The addressee function ("To:") should be used either for an action or for information directly affecting the recipient's job function.

– Copy function

The copy function ("Cc:") should be used for information purposes strictly on a need-to-know basis.

– Blind copy function

Blind copy ("Bcc:") should be used in cases where the identity of some or all members of the distribution list needs to be kept confidential or alternatively when sending messages to a very large list of users. It should not be used whenever it compromises the principle of transparency in the workplace. Blind copies should not be sent to external recipients as a general rule, and should never be sent to external recipients where internal recipients are identified in the message header of the email.

– Forward function

The Forward function ("Fw:") for internal email communication should not be used to send messages on to external recipients without the author's knowledge. The recipient who needs to forward a message should inform the sender of the forwarding action, the new recipient(s) and the reason why they want to forward the message. Auto-forwarding to external recipients is not permitted, although an exception can be granted by ADMIN/DS on a case-by-case basis[6].

– Reply function

The Reply function should be used as the standard function for response (instead of Reply to All).

---

[6] See: http://www.cc.cec/security/security_management/infosec/infosec_liso_faq_en.htm#autoforward

– Reply to All function

The Reply to All function should not be used with mailing lists, or with lists of recipients exceeding 10 users except in a situation where there are extraordinary compelling reasons for doing so.

– Functional mailboxes

The use of functional mailboxes should be encouraged for programme-, project- or task-related issues. The designated owner, or the designated manager acting on their behalf, is responsible for the management and transmission of messages using the mailbox. Any user with access to this mailbox transmits messages under the owner's responsibility, in accordance with the responsibility rules established by the owner (the principle of non-repudiation, i.e. the indisputable attribution of responsibility to a staff member needs to apply). However, attention must be paid when sending sensitive information since the sender may not know who has access to that functional mailbox.

– Mailing lists

Mailing lists should be used sparingly, and only following careful consideration of alternative non-email based forms of communication (IntraComm, local intranet, existing newsletters and networks, etc). All large mailing lists should require management approval prior to use, should be locked to prevent replies to them, and a procedure should be in place for mailing list members to unsubscribe themselves if they so wish and if it is demonstrated that they have no direct professional need for the information. Mailing lists should be limited in size and their membership should be reviewed periodically by the owner. As a practical guide for users DIGIT has developed a procedure for using mailing lists[7].

– Delegations

Email users can delegate mailbox rights to colleagues but should be aware that the responsibility for any information transmitted by a delegate lies with the owner of the mailbox. Delegations should only stay in place for as long as they are needed for operational reasons. Delegated users should not wilfully misrepresent the mailbox owner or use the owner's mailbox identity for any purposes other than those operational requirements for which they have been given the delegation. Users must not give colleagues any of their passwords that would allow direct access to their mailbox.

– Spam

Staff should avoid generating internal spam by, for example, inappropriate use of mailing lists for routine communications, responding to mailing lists, using the Reply to All function when the recipient list is large or by sending messages asking others not to send messages.

3. Data retention considerations

The ease with which email can be used to disseminate documents leads to duplicated storage in the Commission. Email messaging should be used to provide links to information sources

[7] See: http://www.cc.cec/home/dgserv/digit/corporate_ict/infrastruct/corp_systems/email_tech/doc/EC%20EVERYBODY%20E-MAIL%20Procedure%20(v3.33).pdf.

and documents and not to multiply copies of the same document. This shift from “push” to “pull” would free up staff time and infrastructure resources while ensuring easy, unified access to the original sources of information. Also, large document attachments consume considerable proportions of a user’s mailbox storage quota, requiring frequent mailbox administration interventions so that other messages can be received and posted. Action in the following areas can improve system performance and resource availability while reducing mailbox administration tasks:

- Document repositories for formal activities — committees and workgroups
- News and information services — protocols and links
- Selective use of EAS services
- Document linking protocol
- Personal folder structures (filing plan map)
- Weekly administration scheduling
- Documentation retention principles.

These will be elaborated upon during the policy implementation phase.

In Annex 1, a fixed retention period is established for messages contained in the Email Advanced Storage (EAS) system; DG DIGIT is studying other means of storing older email items off-line.