Guideline on the Management of Electronic Mail

Table of Contents

		Paragraphs
I.	**INTRODUCTION**	**1-6**
	■ Definitions	1
	■ E-mail as records	2-3
	■ Purpose and application of the Guideline	4-6
II.	**APPROPRIATE USE OF THE GOVERNMENT E-MAIL SYSTEM**	**7-17**
	■ Segregation of personal and official e-mail	10
	■ Privacy of personal e-mail	11-13
	■ Ownership of government e-mail records	14
	■ Regulatory requirements for e-mail records	15-16
	■ Copyrighted materials	17
III.	**SECURITY OF THE GOVERNMENT E-MAIL SYSTEM**	**18-30**
	■ Responsibilities of bureaux and departments	18
	■ Access to Internet	19
	■ Password protection	20-21
	■ Virus detection	22-23
	■ Security after system logon	24
	■ Scanned (bit-mapped) signature	25
	■ Internet mailing list	26-27
	■ Backup	28-29
	■ Related regulations and guidelines	30
IV.	**IDENTIFICATION OF E-MAIL RECORDS**	**31-37**
	■ Rules for identification	31-33
	■ Features of a complete e-mail record	34-36
	■ Contextual and structural details to be captured	37
V.	**CREATION OF E-MAIL RECORDS**	**38-47**
	■ Creation control	38
	■ Composing e-mail records	39-44
	■ Avoiding unnecessary network traffic	45-47

VI. FILING OF E-MAIL RECORDS **48-58**

- The filing responsibility 48
- Filing options 49
- Filing by an electronic recordkeeping system 50-52
- Print-and-file 53-58
  - The role of the subject officer 54-56
  - The role of the registry staff 57-58

VII. DISPOSAL OF E-MAIL RECORDS **59-64**

- Destruction of the record copy 60
- Deletion of the electronic copy after filing 61
- Destruction of non-records 62
- Regular housekeeping 63
- Transfer of archival e-mail records 64

VIII. CARE AND PROTECTION OF ELECTRONIC STORAGE MEDIA **65-73**

- Selection of suitable media 66
- Media labelling 67-68
- Handling and storage of the media 69-71
- Frequent checking of the media 72-73

IX. MANAGEMENT OF CLASSIFIED E-MAIL RECORDS **74-83**

- Confidential Mail System 74-77
- Printing and handling of restricted and confidential e-mail records 78-80
- Destruction or erasure of restricted and confidential e-mail records 81-82
- Related regulations and guidelines 83

Appendix A : Examples of E-mail Records and Non-records
Appendix B : Features of a Complete E-mail Record
Appendix C : Major Capabilities of a Properly Designed Electronic Recordkeeping System

Flowchart 1 : Create and Handle Unclassified E-mail
Flowchart 2 : Create and Handle Restricted and Confidential E-mail
Flowchart 3 : File E-mail Printout

I. INTRODUCTION

Definitions

1. In this Guideline, unless the context otherwise required -

*"**Electronic Mail (e-mail)**"* means electronically transmitted information created on or received by a computer or an electronic device via a telecommunication system. It includes the text in the message itself and the attachment, if any, of external files such as text files, spreadsheet files, database files, image/graphic files, etc. E-mail can be transmitted within an organization, among government agencies and between government agencies and the public.

"Electronic Recordkeeping System (ERKS)" is a computer system with the necessary records management capabilities designed to electronically collect, organize, classify and control the creation, storage, retrieval, distribution, maintenance and use, disposal and preservation of records.

"Record" is any recorded information, regardless of medium or format, created or received by an organization in the course of official transaction and subsequently kept for further reference and as evidence of such business.

"Record copy" is the official copy of a record retained for legal, fiscal, operational, accountability or archival purposes. Only the record copy should be maintained in a recordkeeping system as the corporate information resource.

"Recordkeeping system" is a manual or automated record/information system in which records are collected, organized and classified to facilitate and control their storage, retrieval, distribution, maintenance and use, disposal and preservation.

E-mail as records

2. E-mail created or received for official business and kept as evidence of such business are records. They are subject to the same legislative and regulatory framework that applies to all other records.

3. To ensure that e-mail records are accurately and adequately documented and are readily retrievable and usable as and when required, they should be captured into a reliable recordkeeping system and managed properly.

Purpose and application of the Guideline

4. This Guideline gives guidance and instructions to help bureaux and departments identify, create, file and manage e-mail records so that sufficient and accurate evidence of official business and activities will be retained for legal, operational, accountability and archival purposes.

5. Electronic recordkeeping system (ERKS) has not been a commonly adopted system to capture, organize, control and preserve electronic records including e-mail documents. Bureaux and departments generally use "print-and-file" to retain important e-mail records. This Guideline provides standardized procedures for the "print-and-file" practice to ensure that the required information of an e-mail record will be adequately and effectively captured in a paper recordkeeping system.

6. This Guideline is intended for all e-mail users, registry staff and departmental Local Area Network (LAN) Administrators. The principles and procedures in this Guideline cover all e-mail records unless otherwise specified. For ease of reference, a series of flowcharts that illustrate the recordkeeping procedures for different types of e-mail are also provided in the Guideline.

II. APPROPRIATE USE OF THE GOVERNMENT E-MAIL SYSTEM

7. The government e-mail system is installed primarily for official business communication.

8. Although government policy permits officers to send and receive personal e-mail messages using the government accounts provided via the government e-mail system, extensive use of the system for private communication that may interfere with the normal work activities should be avoided. Comments or materials that are illegal, inappropriate, offensive or disrespectful to others should not be disseminated through the system. Officers may also send or receive e-mail through their private accounts provided that the requirement stipulated in paragraph 19 is fulfilled.

9. Disciplinary proceedings may be considered against those officers who have infringed the government's e-mail records policy or guideline, or related regulations issued by relevant bureaux and departments, subject to the gravity and consequence of such infringement.

Segregation of personal and official e-mail

10. To facilitate proper management of e-mail records, officers should avoid mixing official and personal e-mail documents in the same mailbox. Officers should remove and delete personal e-mail messages from the mailbox as soon as possible. If retention of personal e-mail is considered necessary, these should be stored in a labeled folder in the local hard drive of an officer's workstation.

Privacy of personal e-mail

11. The government does not guarantee privacy of personal e-mail sent or received via the government e-mail system, nor will the government be held responsible for such e-mail. It reserves the right to access all e-mail sent or received via the government e-mail system where circumstances warrant or for the purpose of,

for example, system maintenance, guarding against unlawful activities or abusive behaviour.

12. When an officer has inadvertently been given access to another officer's personal e-mail, he should inform the sender as soon as practical and should not disclose the information in the personal e-mail to a third party without the consent of the data subject.

13. The departmental LAN Administrator needs to maintain an e-mail traffic log[1] of the server that covers all e-mail, including personal e-mail transmitted through the government e-mail system, for security, statistics, diagnostic and other system monitoring purposes. Only authorized officers should have access to the log, which should be disposed of according to operational needs with a records disposal schedule agreed by the Government Records Service (GRS).

Ownership of government e-mail records

14. Official e-mail records are government property and the government has the right to access, read, use, manage and dispose of these e-mail records. Some e-mail records may also be selected as archives for permanent preservation.

Regulatory requirements for e-mail records

15. Like all other government records, e-mail records are subject to the requirements of laws and regulations such as the Evidence Ordinance, Copyright Ordinance, Official Secrets Ordinance, Personal Data (Privacy) Ordinance, Electronic Transactions Ordinance, Code on Access to Information, Security Regulations and Public Records (Access) Rules.

16. It should be noted that unknown, incomplete, unmanaged or mismanaged e-mail records that are subsequently unusable, inaccessible, irretrievable or released to unauthorized individuals would expose the government to legal, business and accountability risks.

Copyrighted materials

17. Copyrighted materials, including those downloaded from the Internet[2], should not be stored in the government e-mail system or disseminated to others without the prior permission of the relevant copyright owners.

[1] This log is a record and contains information such as the timestamp and processing time of the event, message ID, sender, recipient and physical size of each e-mail. It may be printed and retained in paper form.

[2] Software from the Internet should not be downloaded to run on a government computer without permission of the copyright owner and the Head of Bureau/Department. For details, please see ITSD Circular No. 5/2000 – "Intellectual Property Rights Protection and Software Asset Management".

III. SECURITY OF THE GOVERNMENT E-MAIL SYSTEM

Responsibilities of bureaux and departments

18. Bureaux and departments are responsible for applying adequate security measures to their business routines and protecting government information and computer resources, including e-mail records and the e-mail system, against internal and external fraud and unauthorized access.

Access to Internet

19. Unless the Internet access is made through the Central Internet Gateway or an approved departmental Internet gateway, connections to the Internet should be restricted to dial-up connection from either standalone workstations or workstations that have been logged off from the Local Area Network (LAN) environment.

Password protection

20. To enhance the security of the government e-mail system, officers should set up passwords for their workstations and e-mail accounts to prevent unauthorized access and use. Officers should also safeguard and change their passwords regularly.

21. Officers should use passwords with a mix of no less than six alphabetic and non-alphabetic characters (digits or punctuation). Passwords should be difficult to guess but easy to remember, so that they do not have to be written down.

Virus detection

22. The departmental LAN Administrator should arrange automatic updating of the virus signature or definition files for officers who use the government e-mail system. Officers should make sure that the auto-protection function of the anti-virus software in their workstation is always enabled whenever they use the system to access any document or information.

23. Officers should not open any e-mail from unknown or suspicious sources. The departmental LAN Administrator should be informed immediately should any virus be found.

Security after system logon

24. After logging on the e-mail system, officers should not leave their workstations unattended unless a password-protected screen saver has been activated. If the e-mail client program is Lotus Notes, officers are advised to press [F5] to clear the logon information when they are temporarily away from their workstations.

Scanned (bit-mapped) signature

25. The attachment of a scanned signature to an e-mail cannot authenticate the identity of the sender as a scanned signature can be easily cut and pasted or manipulated by others to give the appearance that a message was officially signed. Therefore, officers should not put scanned signature in their e-mail messages or attachments.

Internet mailing list

26. Officers should use Internet mailing lists for internal user groups (for example, xxgroup@xxdept.gov.hk) with great care. Exposing these lists to potential public mailing lists, such as newsgroups and web sites, may result in officers on the list receiving unsolicited e-mail from the Internet.

27. Any system irregularities should be reported immediately to the departmental LAN Administrator.

Backup

28. To avoid information loss during unexpected system shutdowns or failures, bureaux and departments should determine the nature and types of potential risks they may encounter and develop appropriate backup strategies for the e-mail system and e-mail documents.

29. Where backup procedures are automated with the use of appropriate software, the job logs of such backup runs should be checked to ensure that the backup operation is successful. Bureaux and departments may consult the Information Technology Services Department (ITSD) for advice on the arrangement of system and data backup.

Related regulations and guidelines

30. In dealing with security issues relating to information systems and classified information in electronic form, bureaux and departments should follow the provisions set out in paragraphs 350-383 of the Security Regulations and ITSD's circulars and guidelines on information technology security.[3]

[3] Related ITSD's circulars and guidelines include ITSD Circular No. 6/99 – "Security of Government Networks Connected to Internet", ITSD Circular No. 21/99 – "Guidelines on the Acceptable Use of Internet Services", Guidelines on I.T. Security, Baseline IT Security Policy, and Guidelines on Information Security Incident Handling.

IV. IDENTIFICATION OF E-MAIL RECORDS

Rules for identification

31. In deciding the record status of an e-mail, the subject officer may adopt the following: if a document contains the same information that will be kept in a paper file, this e-mail should be treated as a record and be captured in a recordkeeping system.

32. Where there is doubt as to whether an e-mail is a record, the subject officer should consider it a record, and arrange to have it filed in an appropriate manner.

33. Some typical examples of e-mail records and non-records are given in Appendix A.

Features of a complete e-mail record

34. E-mail records must possess sufficient details of content, context and structure to provide reliable, authentic and complete evidence of official business.

35. Content of an e-mail refers to the information or idea that the sender wants to convey in the message. It may be shown in the message or in the attached document transmitted with the message. Context comprises the information about the circumstances in which the message is created, transmitted, maintained and used. Structure means the physical and logical format of the e-mail and the way parts of a message relate to each other.

36. A sample illustrating the content, context and structure of an e-mail record is given in Appendix B.

Contextual and structural details to be captured

37. To ensure the completeness and reliability of an e-mail record, in addition to its content, bureaux and departments should capture the following contextual and structural details as far as possible:

a. Details of the author (including the author's full name, designation, bureau or department, and e-mail address);

b. Details of the recipient (including the recipient's full name, designation, bureau or department, and e-mail address);

c. Transmission and receipt information including date and time of sending and receiving the e-mail;

d. Subject or title of the e-mail;

e. File reference of the e-mail if a copy of it will be filed as a record;

f. Security grading where applicable; and

g. Indication of any attached document and the file name and extension of the document.

V. CREATION OF E-MAIL RECORDS

Creation control

38. To ensure efficient and cost-effective records management, officers should create e-mail on a need basis. Officers should also take note of the circumstances in deciding whether communication by e-mail or paper is more appropriate. In general, using one mode of communiation, and preferably the same mode adopted by the sender, in making a reply would suffice.

Composing e-mail records

39. When making a response, officers may use the built-in reply function to link the reply to the incoming e-mail. The attachments and histories embedded in the imcoming e-mail should be removed from the reply, unless these are absolutely necessary.

40. Officers resorting to electronic communication via the government e-mail system represent the government, as is the case when they communicate by written correspondence. Officers should use appropriate tone and wording, and carefully check their e-mail and attachments for proper content and tone before transmission.

41. Officers should not put the text all in capital letters as it will make the text difficult to read. Moreover, uppercase text is often interpreted as having extra emphasis.

42. Officers should preferably limit an e-mail message to one subject matter and assign a brief but meaningful title in the “Subject” field for easy identification.

43. To facilitate filing and information retrieval, officers should give adequate information about the e-mail in the body of the message as listed in paragraph 37.

44. GRS and ITSD have developed templates to standardize the layout of government e-mail records and ensure that the required details are properly captured. These templates are designed for composing e-mail that will be captured in a recordkeeping system. Further guidance and information about these templates can be obtained from ITSD. Existing cc:Mail and Lotus Notes templates could be used

for personal or informal e-mail.

Avoiding unnecessary network traffic

45. Care should always be taken to ensure that e-mail messages are properly addressed. Officers should select the recipient(s) from the on-line address book provided in the government e-mail system to minimize the possibility of misaddressing.

46. Officers should consider carefully the need for sending e-mail with large attachments or requesting return receipts. Such measures will consume considerable time in transmission, create heavy network traffic and affect system performance.

47. Chain e-mail[4] should not be sent via the government e-mail system. Transmitting mass e-mail without any legitimate business reasons should also be avoided. If it is required to send unsolicited e-mail to a large group of recipients for optional information distribution or sharing, officers should take the following steps to reduce the number of copies routed to individual users:

a. Use a mailing list that allows recipients to join or leave the list freely (for example, instead of sending news extracts to all users in a department, a list of news subscribers should be used); and/or

b. For internal communication, put the attachment(s) in a shared network directory, create hyperlink(s) in the message and request recipients to browse the attachment(s) on-line.

VI. FILING[5] OF E-MAIL RECORDS

The filing responsibility

48. To ensure that the record copy of an e-mail record is captured in the recordkeeping system, bureaux and departments should adopt the following rules:

a. Where the sender and recipient(s) of an e-mail record are using the same file, the sender should designate his copy as the record copy and arrange to have it filed in the recordkeeping system; and

b. Where the sender and recipient(s) of an e-mail record are using different files (for example, communication between a bureaux and a

[4] Chain e-mail refers to those messages that request the recipients to send the copy of same e-mail to a specific number of others so that its circulation increases in geometric progression.

[5] Filing is a process in which registry staff analyze the content of a document, classify it according to established records classification scheme, and put it onto a properly titled and coded file folder. Effective filing contributes to prompt, accurate and complete retrieval of information.

department or with outside organizations or individuals), the action officer should arrange to have his copy officially filed.

Filing options

49. There are two options for filing e-mail records:

a. Electronic filing – transfer e-mail records to an Electronic Recordkeeping System (ERKS) for centralized filing and management; or

b. Print-and-file – print e-mail records immediately after transmission or receipt and file the printout in a paper recordkeeping system.

Electronic filing by ERKS

50. ERKS may offer an effective and long-term solution to e-mail records management. In this regard, the government is studying the feasibility and implications of developing a standard ERKS for service-wide application. Bureaux and departments will be informed of the study findings.

51. Major functions and capabilities of ERKS are summarised in Appendix C.

52. Bureaux and departments using computer systems other than the government e-mail system to manage e-mail records are advised to contact GRS to confirm if their computer systems provide adequate records management functions. Individual bureaux or departments who are planning to develop or install ERKS should consult GRS, ITSD and/or MSA at an early stage.

Print-and-file

53. Unless otherwise agreed with GRS, bureaux and departments should use the print-and-file approach for managing their e-mail records, i.e. they should print the e-mail records and put the hard copy on paper files as other government records.

The role of the subject officer

54. The subject officer should confirm the record status of the e-mail sent or received through his mailbox, arrange to print the e-mail and attachment (as applicable) and pass them to the registry staff for filing.

55. The subject officer or his delegate should check and ensure that sufficient details of the content, context and structure of the e-mail record have been printed or manually marked on the printout (see paragraph 37).

56. The subject officer should arrange to:

a. Print the e-mail as soon as possible upon its transmission or receipt;

b. Print the e-mail directly from the e-mail client program. To preserve record authenticity, the e-mail should not be exported or copied to other programs for printing;

c. If the time of transmission or receipt of the e-mail record is critical to the transaction, check the correct time on the e-mail server;

d. Where operationally required, identify the full name and designation of the recipient and manually mark such details on the printout; and

e. Store multimedia or non-textual attachments that cannot be printed out to a designated directory on the server, change their attribute to read-only and manually record the full path of the network directory on the e-mail printout. To facilitate cross-referencing, there should be an index showing the details of the attachments stored in the designated directory and the file reference of the corresponding e-mail message.

The role of the registry staff

57. Similar to the handling of paper records, registry staff should classify, index and code the printout of e-mail records without delay.

58. Registry staff should ensure that all the necessary information is printed or manually marked on the printout and that all attachments, if any, are filed with the message in processing such records. Where there is doubt about the completeness of the record, advice from the subject officers should be sought.

VII. DISPOSAL[6] OF E-MAIL RECORDS

59. Bureaux and departments should make arrangements for their officers using the government e-mail system to separate e-mail records from personal e-mail messages and non-records in a timely manner. Identified e-mail records should be properly filed and disposed of when further retention is not required.

[6] Disposal is actions taken with regard to records as determined through the appraisal of legal, financial, operational, accountability and historical values of the records. Disposal actions may include physical destruction or permanent erasure of records of no residual value, transfer of records to GRS for inactive storage for a specific period before destruction/erasure, or transfer of records appraised to have archival value to GRS for permanent retention.

Destruction of the record copy

60. As is the case of paper records, bureaux and departments should, base on their legal, fiscal and/or operational needs, compile and agree with GRS their records disposal schedules for e-mail records; and obtain the prior consent of the GRS Director before permanent erasure or destruction of the record copy.

Deletion of the electronic copy after filing

61. In general, after the printout copy of the e-mail record has been captured into a recordkeeping system, the subject officer or his delegate should erase or delete the electronic copy, which is no longer a record, from his mailbox as soon as possible or within 90 days from the date of transmission.

Destruction of non-records

62. Officers should check their workstations regularly to delete non-records. Non-records such as the duplicate electronic version of e-mail records as mentioned in paragraph 61, convenience or reference copies of e-mail records and personal e-mail messages can be disposed of without separate authorization of the GRS Director.

Regular housekeeping

63. The government e-mail system must not be used as a storage area for files and documents. Old and obsolete e-mail should be deleted regularly to keep the mailbox to a manageable size. The departmental LAN Administrator should ensure that old e-mail would be purged periodically and automatically. Even under an electronic recordkeeping system, inactive e-mail records should be moved to off-line storage such as magnetic tapes or CD-ROM to facilitate records disposal.

Transfer of archival e-mail records to GRS

64. Bureaux and departments should transfer those e-mail records appraised by GRS as possessing archival value to GRS for permanent retention. GRS will develop a separate guideline on the requirements and procedures for the electronic transfer particularly of those e-mail records that cannot be captured by the print-and-file approach. Bureaux and departments will be notified when this is available.

VIII. CARE AND PROTECTION OF ELECTRONIC STORAGE MEDIA

65. Users of ERKS should select suitable removable storage media and implement proper protective measures to minimize the impact of media deterioration and possible information loss.

Selection of suitable media

66. The storage media chosen should be stable and fully compatible with the information retrieval system. Floppy disks should not be used to store e-mail records of long-term or permanent value.

Media labelling

67. The removable storage media should be identifiable by external labels with sufficient information about the media and records stored therein. Such identification information may include:

- Unique identifier of each tape/disk/disc
- Name of the organizational unit responsible for the record
- Descriptive title of the content
- Date of creation
- Security grading
- Type of copy, i.e. master or backup
- Operating environment, i.e. hardware and operating software
- Name and version number of the software which creates the attachment
- Manufacture date of the storage medium
- Storage location

68. Label contents of the media should be written before attaching the labels to magnetic and optical media. Soft felt-tip markers should be used to prepare the label contents to avoid debris and scratches.

Handling and storage of the media

69. The storage media should be handled by their edges and kept away from dust, smoke, heat, direct sunlight and strong magnetic field. Magnetic and optical media should be shelved in an upright, vertical position to prevent warping of containers. They should be kept in protective containers when not in use.

70. E-mail records of long-term or permanent value are best preserved in an appropriate storage environment with 24-hour air conditioning and controlled temperature and humidity at 18°C ± 2°C and RH 40% ± 5% respectively. For assistance in storing long-term or permanent e-mail records, bureaux and departments may contact ITSD and GRS.

71. Bureaux and departments should provide proper access control and fire fighting equipment and facilities in the storage area to protect the physical security of the media.

Frequent checking of the media

72. Bureaux and departments should check samples of the tapes/disks/discs at regular intervals to ensure the integrity of the media and see that the information is retrievable. Should any signs of deterioration be found, the records should be copied to tested tapes/disks/discs as soon as possible.

73. At present, the physical life span of electronic media is still debatable and technology obsolescence also complicates the preservation of electronic records. Bureaux and departments should thus develop strategies for system migration and implement a proper copying cycle to transfer their e-mail records, especially those requiring long-term or permanent retention, from old media to new media (e.g. from old CD-ROM to new CD-ROM). Normally the interval for media copying should be set for less than 10 years.

IX. MANAGEMENT OF CLASSIFIED E-MAIL RECORDS

The Confidential Mail System (CMS)

74. CMS is installed for government internal communication of classified information. The CMS implementation program is expected to complete by April 2002.

75. CMS is designed for bureaux and departments to transmit electronically classified documents up to "confidential" level via the Government Communication Network (GCN) in compliance with the Security Regulations. Other systems that conform to the requirements stipulated in paragraph 365 of the Security Regulations may also be used to transmit restricted and confidential information. For example, restricted e-mail records can be sent using Lotus Notes via GCN with the encryption function enabled.

76. Before using CMS to transmit classified records, officers must be equipped with the necessary facilities. In addition, officers should make sure that the recipient(s) are registered CMS users and the "Subject" and "File Reference" fields of the message to be transmitted do not contain classified information.

77. At the moment, CMS is the only means by which officers can transmit "confidential" e-mail via GCN. Transmission of "secret" and "top secret" e-mail should follow the requirements specified in the Security Regulations.

Printing and handling of restricted and confidential e-mail records

78. In addition to the procedures given in paragraphs 53 – 58 of this Guideline, the subject officer or his delegate should only use a local printer or remote printer in a trusted network to print restricted and confidential e-mail and attachments.

Requirements in the Security Regulations should also be observed.

79. For e-mail records transmitted via CMS, if the trust validation information is required for the transaction of business or record purpose, the subject officer should sign the corresponding printout to confirm that the identity of the sender is checked and verified correct, and arrange to also print and file the screen dumps used to verify the digital signature.

80. Registry staff should classify and put the printout of security graded e-mail records on paper files that have the same security classification of the records, and strictly follow the Security Regulations in handling different security graded documents.

Destruction or erasure of restricted and confidential e-mail records

81. Bureaux and departments should follow the requirements stipulated in paragraphs 377-378 of the Security Regulations in disposing of or erasing restricted and confidential e-mail records. All classified information should be cleared from the electronic media before disposal. If the classified information cannot be cleared completely, the media unit should be physically destroyed in a manner that prevents recovery of the information. ITSD could be contacted for technical assistance.

82. Prior consent of the GRS Director should be sought before any classified e-mail records are destroyed or permanently erased. Paragraphs 59 – 64 of this Guideline also apply to the disposal of classified e-mail.

Related regulations and guidelines

83. In addition to the Security Regulations, bureaux and departments should also refer to the most up-to-date guidelines and manuals issued by ITSD on matters relating to system operation, administration and security.[7]

[7] Related ITSD's guidelines include Application User Manual Part I – User Guidelines, Application User Manual Part II – System Administration Guidelines, and Application User Manual Part III –Security Rules for Confidential Mail.

Appendix A

Examples of E-mail Records and Non-records

Typical examples of e-mail record:

- Correspondence relating to formulation and execution of policies and operating procedures
- Commitments, decisions, or approvals for a course of action
- Documents that initiate, deliberate, authorize or complete business transactions
- Work schedule and assignments
- Agenda and minutes of meetings
- Drafts of major policies or decisions circulated for comments or approval
- Final reports or recommendations
- Documents of legal or financial implications
- Acknowledgements of receipt of e-mail records that document essential transactions

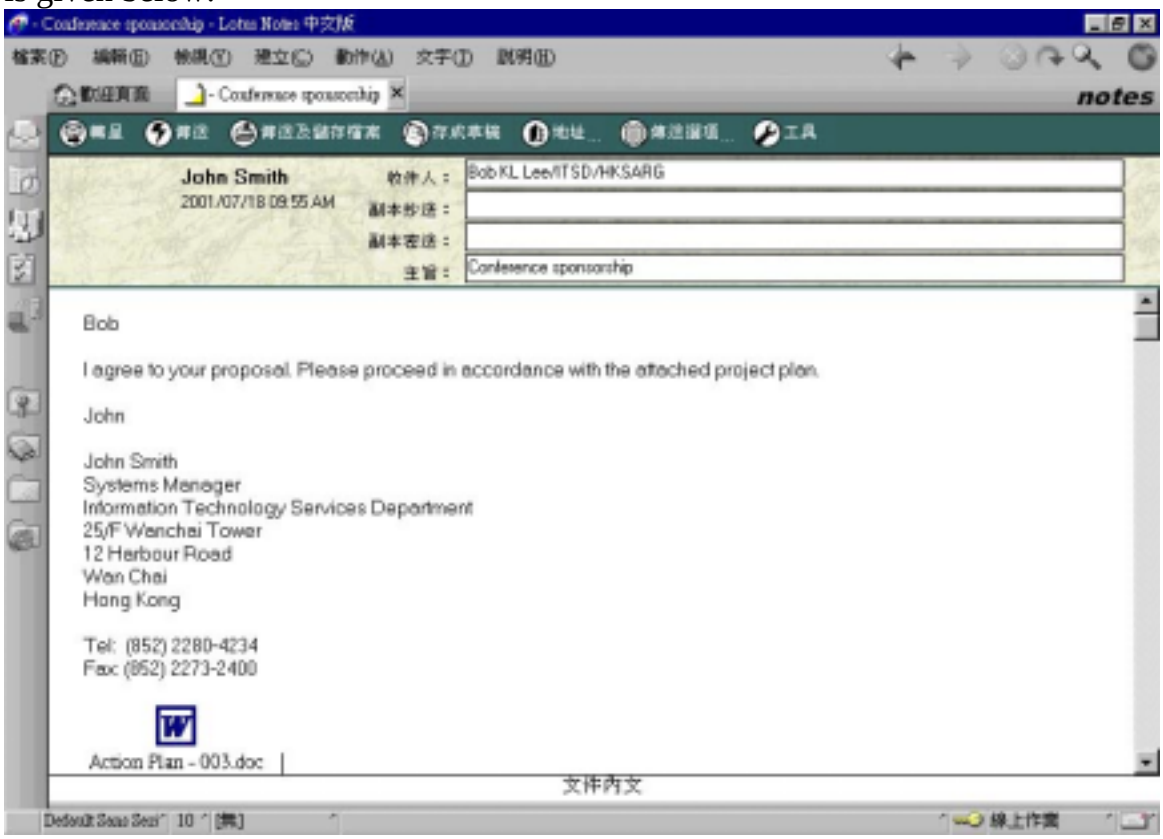
Typical examples of non- records:

- Messages of personal nature
- Copies or extracts of documents that are published or downloaded and distributed for information or reference purposes
- Phone message slips
- Electronic copy of a record of which the paper copy has been filed

Appendix B

Features of a Complete E-mail Record

A sample illustrating the content, context and structure of an e-mail record is given below:



Content:
Content refers to the information or idea that the sender wants to convey in the message. It may be shown in the message or in the attached document transmitted with the message.

In the above example, content refers to the message, “I agree to your proposal. Please proceed in accordance with the attached project plan”. The content also refers to the content of the attachment “Action Plan – 003.doc”.

Context:
Context comprises the information about the circumstances in which the message is created, transmitted, maintained, and used.

Context can be addressed at many different levels. In the example above, the context is the e-mail address information in the “To” field, the subject, “Conference sponsorship”, and the information in the body indicating that the message is being sent to “Bob” from “John” (for which there is some identifying information such as position, address, etc.). The context is also the information at the bottom of the message that there is an attachment, “Action Plan – 003.doc”. Other contextual

information also exists which may be hidden from view or that may not emerge until after the message has been sent (e.g. date).

Structure
Structure means the physical and logical format of the records, and the way parts of a message relate to each other (for instance, a message header and the body of a message; a message and its attachments) and the way separate messages relate to each other (for example, a message and its reply).

In the example above, the structure would comprise all of the elements that make up the documentary form of the e-mail message. These would include the header fields (not the information in the fields, only the headers themselves such as “to”, “from”, “subject”, etc.), the length of the fields, their position on the message, etc. Also included would be the format of the message body and the identifying link to attachments (but not the contents of the attachment itself). Anything that would comprise the layout and format of the message would be considered to form its structure.

Appendix C

Major Capabilities of a Properly Designed ERKS

Major capabilities of a properly designed ERKS should include:

a. Manage records created and received in different formats (e.g. electronic, paper, microfilm, tapes);

b. Provide version control of documents;

c. Capture the record copy of an e-mail and its attached documents (if any) together with the necessary details of content, context and structure at the time of transmission or receipt;

d. Code and classify e-mail records and group related records in different formats together in accordance with pre-defined records classification scheme;

e. Provide accurate and timely information retrieval;

f. Support shared use of information through users' desktops in accordance with established information access rules;

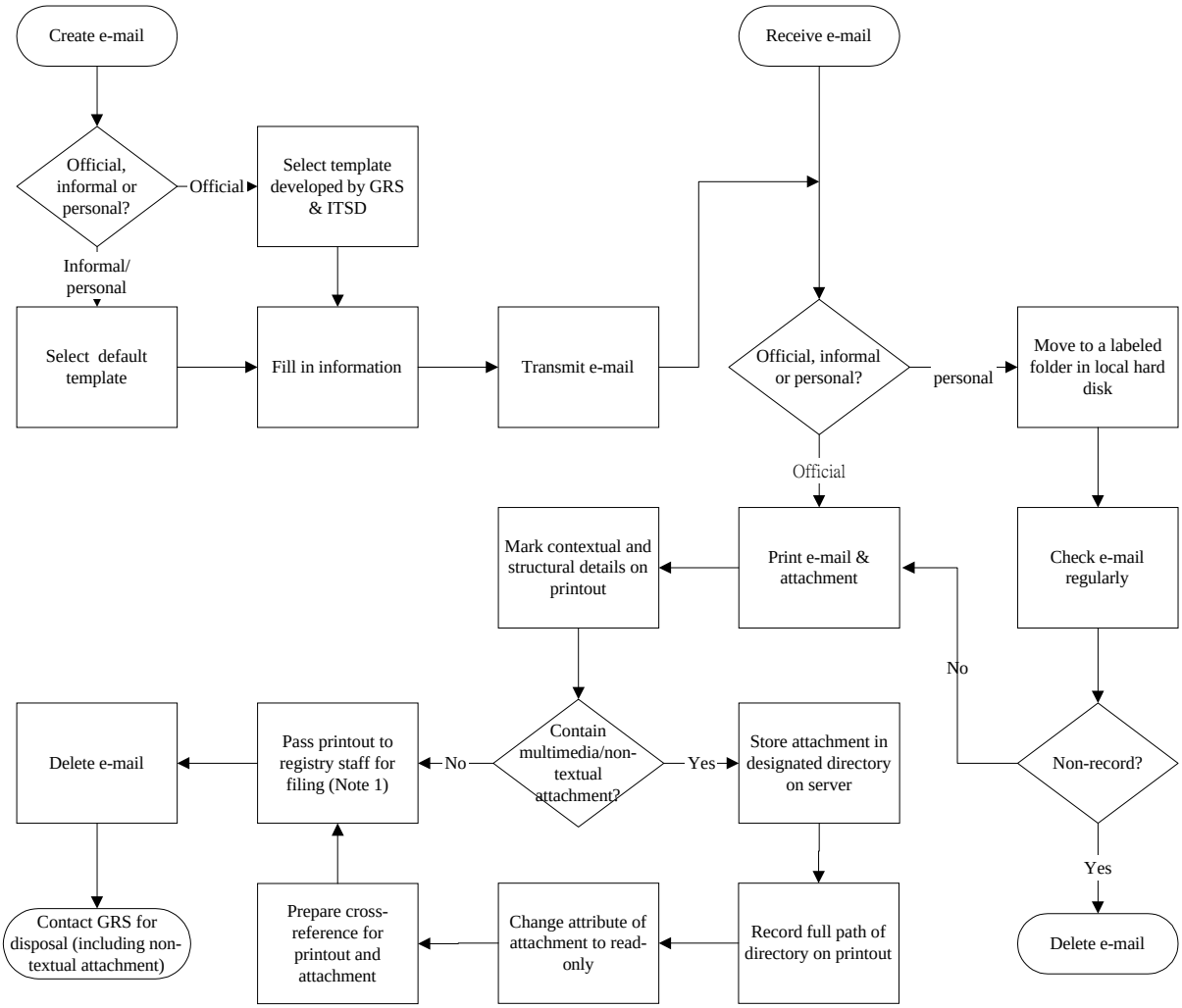
g. Reproduce and reuse the e-mail records electronically with a record copy protected properly;

h. Assign appropriate retention requirements to the records; and

i. Dispose of e-mail records, including destruction of unneeded records and transfer those of archival value to Government Records Service (GRS) for permanent retention in accordance with records disposal schedules.

Flowchart 1

Create and Handle Unclassified E-mail



Note:

Note 1: See Flowchart 3 - "File E-mail Printout"

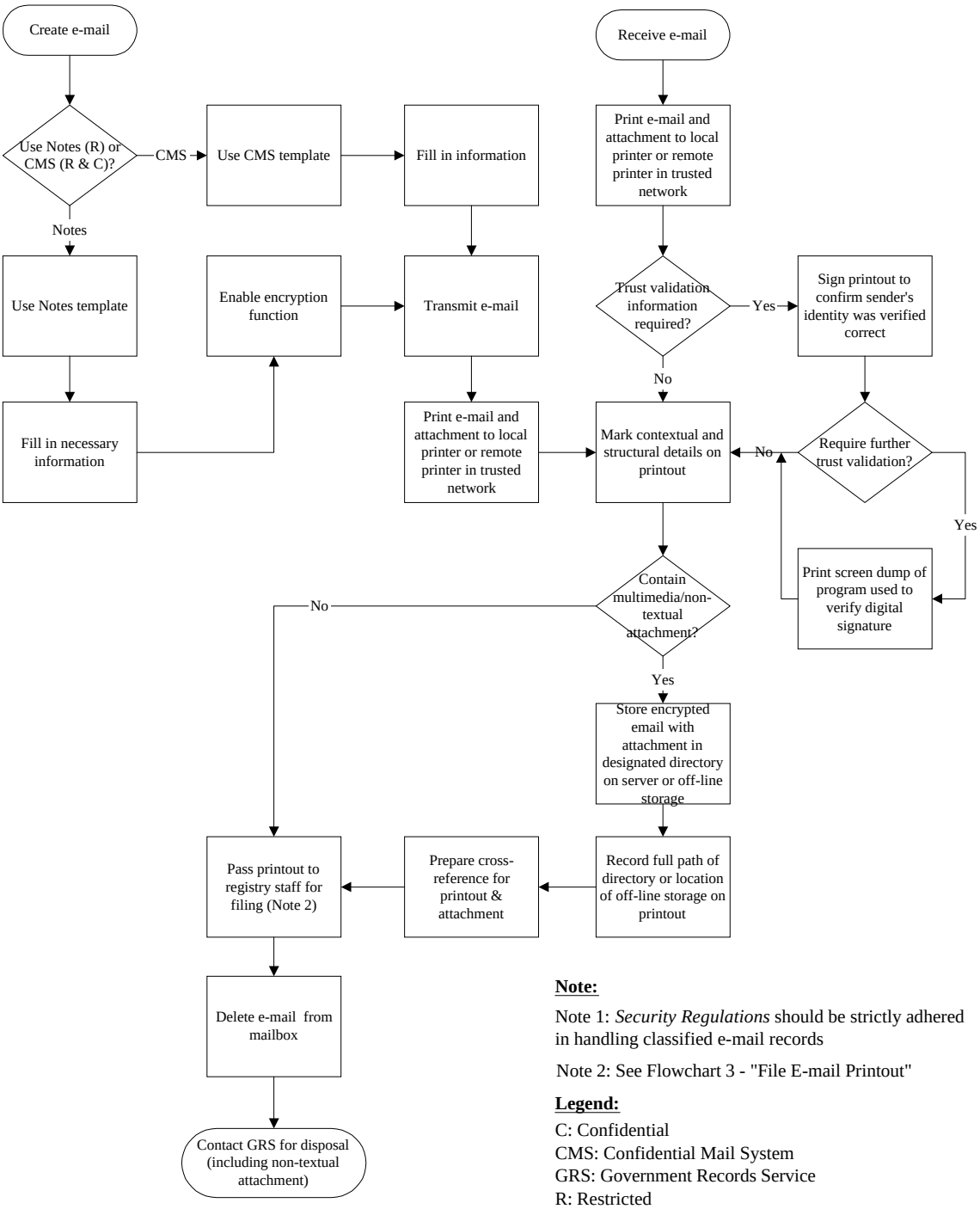
Legend:

GRS: Government Records Service

ITSD: Information Technology Services Department

Flowchart 2

Create and Handle Restricted & Confidential E-mail (Note 1)



Note:

Note 1: *Security Regulations* should be strictly adhered in handling classified e-mail records

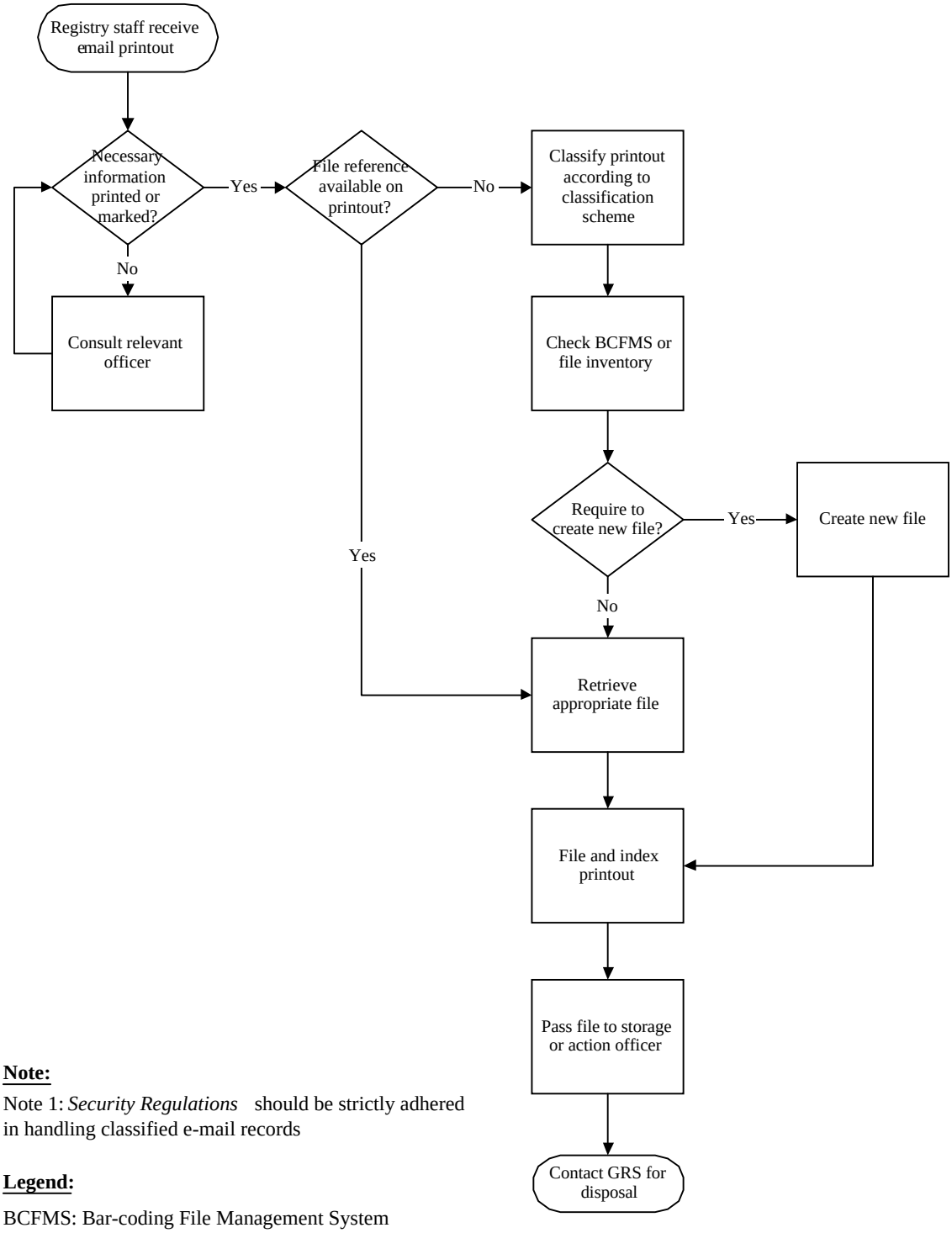
Note 2: See Flowchart 3 - "File E-mail Printout"

Legend:

C: Confidential
CMS: Confidential Mail System
GRS: Government Records Service
R: Restricted

Flowchart 3

File E-mail Printout (Note 1)



Note:

Note 1: *Security Regulations* should be strictly adhered in handling classified e-mail records

Legend:

BCFMS: Bar-coding File Management System

GRS: Government Records Service