
 Government of South Australia		South Australian State Emergency Service		INFORMATION TECHNOLOGY MANAGEMENT
				POLICY
				ITMPOL003
POLICY				
SASES EMAIL				

1. What this Policy covers:

- 1.1 This policy is applicable to all employees and members of the SA State Emergency Service (SASES) as defined in the *Fire and Emergency Services Act 2005*.
- 1.2 This Policy upholds the IT Management Directive – ITMDIR001 from the Chief Officer SA State Emergency Service, the SAFECOM Email Policy and the *Public Sector Act 2009*.
- 1.3 Any email user who contravenes or fails to comply with this Policy is liable to disciplinary action.
- 1.4 Any email user may also be personally legally responsible for the misuse or abuse of email pursuant to the *Public Sector Act 2009* and the Public Sector Code of Conduct (paid employees) or the SASES Code of Conduct (volunteers and paid employees).

2. Why we need this Policy:

- 2.1 This policy will:
 - Inform all email users in SASES of their responsibilities and obligations associated with the email environment.
 - Ensure that the principles of IT security are consistently and efficiently applied in the SASES email environment.
 - Minimise the possibility of threat to the security of the email environment which may cause loss or damage to SASES.
 - Ensure that good business practices are promoted in the email environment, thereby improving and protecting delivery of SASES services through education and discipline.

3. Special terms used in this Policy:

AGD	Attorney General's Department of South Australia.
Archive	Electronic folder where documents created in email environment are transferred for storage.
Attachment	Existing electronic document or file which is attached to an email.
Business Procedures	Documented business decisions for email use to be implemented within SASES which must be consistent with this Policy.
Business Use	Anything which could reasonably be described as being, in any way, linked to the functioning of the organisation and its membership.

Chief Officer (COSES)	For the purpose of this policy, CO refers to the Chief Officer, South Australian State Emergency Service.
CS-T	Customer Service-Technology Branch of the Attorney-General's Department of South Australia.
Data	Any record, including visual text or graphics, made or received by SASES in conducting our business. This includes data made or received in both the physical and electronic environments as the case may be.
Data Classification	Prescribed security rating of this data according to the SA Government Security Standards and Guidelines.
Distribution List	List of email addressed either provided by IMS or compiled by users.
DPP	Directives, Policies and Procedures
Email	Electronic mail, calendar, tasks, contact, notes, journal entries and attachment(s).
Email Environment	Infrastructure which enables SASES members to communicate electronically via email with other Government employees and external third parties via the internet.
Employees	Employees or staff referred to under the <i>Fire and Emergency Services Act 2005</i> or the <i>Public Sector Management Act 1995</i> .
External Party	Any person(s) or organisation who is not a user within SASES.
IMS	SAFECOM'S Information Management Services team.
Internet	Un-trusted public networks.
Mailbox	User's personal repository which provides a storage, delivery and receipt function for email.
SAFECOM	SA Fire and Emergency Services Commission
Service Team	SAFECOM's team delivering a service.
SES or SASES	State Emergency Service or South Australia State Emergency Service
Template Word Document	Standard documents created in Microsoft Word (or other applications) tailored for SASES.
User	Employee, volunteer, contractor or visitor who IMS has provided an authorised login and password to any or all of the computer networks.
Member	Registered member of SES (paid or volunteer) who carries out community work within the Emergency Services Sector on a voluntary basis.

4. What the Policy says:

4.1 What We Will Do:

- 4.1.1 SASES will provide users with an email environment for business use only. Email and the email environment are not provided for personal or private use.
- 4.1.2 For the definition of business use, see definitions above.

5. Conforming to this Policy:

5.1 Procedural Obligations:

- 5.1.1 All users who use the SASES email environment must adhere to the following work standards and procedures for email.

5.1.2 Security

Every user's mailbox and all of its contents past, present, deleted, received or sent may:

- Be accessed at any time by IMS during the course of administering the email environment.
- Be audited at any time either by IMS or by any other authorised entity, to assess among other issues, compliance with this Policy.

5.1.3 Network login names and passwords for each user are the access keys to each personal mailbox. Email users must not:

- Provide their logins or passwords to other users or third parties;
- Attempt to gain access to another email user's mailbox or to intercept another user's messages;
- Attempt to send any email under false pretences; or
- Leave workstations unattended without appropriate protection having been enabled, such as the activation of the password protected screensaver.

5.1.4 Email users must report any known apparent or perceived breach of this Policy to their respective Manager and IMS.

5.1.5 Email creates the potential for inadvertent transmission or reception of confidential and restricted information, therefore, email users must ensure that:

- The following SAFECOM / AGD standard disclaimer is visible on the initial page of every email message:

“The information in this email may be confidential and / or legally privileged. It is intended solely for the addressee. Access to this email by anyone else is unauthorised.

If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful.”
- All email messages are correctly addressed. The user must check all address details prior to sending the email message. Failure to correctly address an email may result in the following:
- Any incorrectly addressed email to an external party may, by default, be delivered to the external email system administrator(s) who may therefore have cause to consider and review the contents of this email sent by a SASES user.
- Incorrectly addressed incoming email to SASES users will be delivered to, and may be read by IMS to ascertain the intended user. Where possible, IMS will forward the email to the intended user with a message explaining the address error. Where the correct user cannot be identified, IMS will return the email to the sender with an explanatory message.
- Every email (including all attachments) is classified according to the Data Classification and Confidentiality Section of this Policy.

5.1.6 Email users must not introduce viruses or any other harmful software to the SASES email environment.

5.2 Copyright Infringement and Contractual Commitments

- 5.2.1 Users must not breach any copyright provisions which may attach to data used in the SASES environment.
- 5.2.2 Users must not enter into or commit SASES to a contract via the use of email outside of their delegation or authority.

5.3 Email Ethics

In all communications, email users must:

- 5.3.1 Act with respect and courtesy.
- 5.3.2 Only provide advice via the email environment if authorised to do so.
- 5.3.3 Not store or distribute information that is offensive, sexually explicit or inappropriate (including the use of swear words and blasphemy).
- 5.3.4 Not distribute material that may cause or constitute sexual / racial harassment or bullying.
- 5.3.5 Maintain business writing etiquette when composing email messages by:
 - Incorporating a meaningful and specific subject line;
 - Composing messages with brief, succinct and relevant content;
 - Responding to messages in a prompt manner;
 - Avoiding the use of topical, colloquial or slang expressions;
 - Seeking permission from the sender of an email before forwarding to another recipient.
- 5.3.6 Every email user must have regard to the following:
 - Section 6 of the Public Sector Management Act 1995 which sets out employee conduct standards;
 - Provisions of the Equal Opportunity Act 1984 (SA);
 - The Racial Discrimination Act 1974 (Cth) which has wider provisions and applies to State employees and contractors alike;
 - The Commissioner for Public Employment Circular No. 64 Guidelines for Ethical Conduct which confirms public employees' ethical responsibilities; and
 - The possible consequences of misuse or abuse of email in relation to issues such as defamation and harassment.

5.4 Email Management

- 5.4.1 According to the SA Whole of Government Email Standards, every email user is provided with a maximum mailbox capacity. Consequently, each email user must adopt a disciplined management approach to their mailbox. Each email user is responsible for the contents of their mailbox and must:
 - Regularly review and update personal distribution lists on a regular basis;
 - Regular audit mailboxes to delete or archive out of date or irrelevant email communications.

5.5 Records Management

- 5.5.1 The implementation of email does not represent the advent of the paperless office within SASES. An email should only be considered as an electronic vehicle by which your communication is passed to the recipient. Email does not and will not affect the way in which you currently produce written communications as part of your business function. Consequently, every email user must have regard to the following:
- Email will not affect the use of your standard Template Word Documents.
 - Data files (such as Microsoft Word documents, Microsoft Excel spreadsheets, graphics files etc) will be communicated to the recipient as an attachment to your covering email message.
 - If a signature is required on a document to authorise the content, the document must be printed and signed then distributed as a hard copy.
- 5.5.2 Where it is important to know that an email has been received by the intended recipient, an acknowledgement response from the recipient should be requested.
- 5.5.3 Management of email messages sent and received by each user must be treated no differently from any other written communication sent to a client or other recipient, particularly:
- Each attachment must be detached into the appropriate network directory in compliance with the SASES Records Management Policy;
 - Each email message must make clear and identifiable reference to the attachment which is appended;
 - Each user must make hardcopies of email and attachments, both sent and received for relevant non-electronic records and files; and
 - Hard copies of email and attachments (sent and received) should be filed according to normal good record management practice for your future reference and for the benefit of other members of your team.
- 5.5.4 Every email user must have respect for the State Records Act 1997 (SA) in their dealings with email, particularly:
- An official record for the purpose of the State Records Act 1997 (SA) includes documents created in the electronic medium; and
 - Damage, alteration or disposal of an official record constitutes an offence for which a maximum penalty of \$10,000 or imprisonment for 2 years may apply (Section 17 of the State Records Act 1997).

5.6 Data Classification and Confidentiality

The nature of SASES data ranges from public, implying no requirement for confidentiality, to secure, which warrants the highest level of protection. As a consequence, this Policy sets out Data Classifications which must be applied to every email sent by every user.

5.6.1 Data Classifications

There must be adequate controls to ensure that data and the information derived from it are only disclosed to authorised people, commensurate with the value of that data to SASES, according to its Data Classification, namely:

Level	Meaning
C1	Public: Implying no requirement for confidentiality, such as might be the case for certain free of charge public information and / or services.
C2	Restricted: The data being opened available to SASES personnel only and perhaps free for services public information.
C3	Confidential: The data being available on an authorised need to know basis only.
C4	Secure: Warranting the highest level of protection, including: political and commercially sensitive data; legal professional and parliamentary privileged (including Cabinet in Confidence) data; and personal information. Data Classified at the C4 level is prohibited from transmission in the email environment.

5.6.2 Data Classification Procedures

The entire contents of each email must be assessed according to the Confidentiality Classifications in this table. If several Confidentiality Classifications apply, then the highest classification must be assigned and clearly marked on the email.

Every email must be classified before it is transmitted by clicking the appropriate Data Classification button on the toolbar in Microsoft Outlook. Data Classification text, including a brief narrative, will then be inserted on the initial page of the email.

5.6.3 Resolving Inconsistencies

If there are inconsistencies between this Policy and any IMS Procedures, this Policy will prevail to the extent of that inconsistency.

6. Who this Policy affects and what they have to do:

Who	What they have to do
Chief Officer	<ul style="list-style-type: none">Responsible for disseminating and implementing this policySign off on this policy
Deputy Chief Officer	<ul style="list-style-type: none">Responsible for reviewing policiesResponsible for disseminating and implementing this policy
Regional Commanders	<ul style="list-style-type: none">Responsible for disseminating and implementing this policy
Unit Managers	<ul style="list-style-type: none">Responsible for disseminating and implementing this policy
All members	<ul style="list-style-type: none">Responsible for adherence to this policy

7. Who develops and reviews this Policy:

Monitoring and Evaluation	• Chief Officer, Deputy Chief Officer, Regional Commanders and Unit Managers
Development / Review	• Deputy Chief Officer
Interpretation and Advice	• Advice will be sought as and when required
Consultation	• Chief Officer and Deputy Chief Officer, as required

8. How this Policy will be developed:

This policy is a living document and is subject to continuous monitoring, evaluation and improvement in accordance with the SASES Policy & Procedure Framework.

9. References and related documents:

Fire and Emergency Services Act 2005

(State Government) Information Security Management Framework

State Records Act 1997

SES Information Technology Directive - ITMDIR001

SASES Email Policy – ITMPOL003

Premier and Cabinet Circular No. 12, *Information Privacy Instruction*

Commonwealth and State Legislation (as amended)

Public Sector Act 2009

The Commonwealth Consolidated Acts, Freedom of Information Act 1982 governing collection of personal and agency information.

(State Government) Information Privacy Principles 1989.

The Whistleblowers Protection Act, Circular No. 69, September 1993

SASES Code of Conduct

Public Sector Code of Conduct

AGD Virus Protection Policy, November 1996.

10. Attachments:

Nil.

11. Document History:

Published Date:	28/10/2011
Effective Date:	28/11/2011
Review Date	28/11/2012

12. Approval for Publication:

Signature of SES Chief Officer:



Date of Approval for Publication: 10/10/2011