States of Jersey	Email Records Management Policy
IS-POL-017	

1. Purpose and Scope

This policy sets out the requirements for managing email records. An effective policy helps ensure that:

- Legislative requirements are met
- Evidence in legal proceedings or criminal investigations is available
- Corporate records are managed and available
- Historic records of the Island are managed and transferred to Jersey Archive

This policy applies to all personnel who create, manage or receive electronic mail using systems owned or managed by Information Services Department.

2. Definitions

2.1. Records

In the Public Records (Jersey) Law 2002, a record is defined as information that –

is created or received in the conduct of a corporate, institutional or individual activity; and has such content, context and structure as to provide evidence of the activity.

Any communications that fall under this definition must be considered as records and captured accordingly.

3. Managing Records

For all messages received, sent or created a process will be defined that ensure that:

- Messages that are business records are identified as such
- Responsibility for capturing message records is assigned
- Messages are captured following an approved method
- Retention policies are applied and adhered to

Detailed guidance and examples are provided in the accompanying guidance document (IS-GUIDE-003).

3.1. Approved Records Management Systems

Email software and other communications tools must not be used for the long term storage of messages. Similarly personal storage folders (referred to as PST files) must never be used. Instead messages must be filed in one of the following systems, in line with other business records:

- An approved electronic records management system (e.g. LiveLink, SharePoint)
- A CRM or case management system (e.g. Nessie, Prescient)
- Saved to disk (e.g. L: drive)
- Printed and manually filed

It is not acceptable for users to maintain their own records management system. For the avoidance of doubt the email system itself must not be used for the long-term storage of email messages.

3.2. Requests to access another mailbox

Temporary view-only access may be given to another person's mailbox under exceptional circumstances, providing there is a documented business case and proper approval. These requirements also apply to messages stored in email archives. Access must be:

- for a stated specific purpose
- view-only
- granted to specified individuals
- authorised by either the mailbox owner or their Head of Department
- revoked within a specified period of time

Actual access must be supervised by the individual's line manager.

3.3. Electronic Discovery of Email

The central email system is supported by a forensic email archiving system which stores all messages (except spam) for a maximum of 2 years. This system is solely to support dispute resolution and legal discovery and must not be relied on for day to day record-keeping purposes.

3.4. Managing Shared Resources

Any shared mailboxes must be assigned an owner. The owner is responsible for applying the requirements of this policy.

4. Legal

This policy supports compliance with the following legislation, which all users are bound by:

- Data Protection (Jersey) Law 2005
- Freedom of Information (Jersey) Law 2011
- Public Records (Jersey) Law 2002

5. Compliance and Enforcement

Periodic checks will be performed by ISD to confirm compliance with this policy, and to identify and report exceptions. Automatic archival functions will also be run on behalf of users:

Compliance Task	**Limit**	**Frequency**
Check mailboxes are under size limit. Archive any exceptions, oldest first.	500MB	Monthly
Check mailbox contains only messages that meet retention requirements. Archive any exceptions.	12 months	Monthly
Scan for .PST files on shared drives. Exceptions will be archived.	0	Monthly
Email archive (Cryoserver) history cut off	2 years	Daily

6. Exemptions

In rare circumstances a policy exemption may be requested. This is done through a formal approval process via the IS Service Desk. Requestors will be expected to make a business case for the exemption, and demonstrate that appropriate compensating controls have been established.

7. Sanctions

Policy breaches may be addressed by one or more of the following:

- suspension or withdrawal of system access
- disciplinary action
- legal action

8. See Also

IS-GUIDE-003 Email Good Practice Guide

END