States of Jersey	Acceptable Use Policy
IS-POL-001	

1. Purpose and Scope

This policy explains the acceptable uses of States of Jersey ('States') information systems and data. By communicating a clear set of security objectives, it is intended to help protect States systems and data against unauthorised or unintended disclosure or loss.

This policy applies to all States employees, and covers all information systems (whether paper-based or electronic) that handle States data.

2. General Responsibilities

As a user of States systems or information, you have three primary areas of responsibility:

- The security of any information that you handle
- Reporting suspected security incidents
- The safety of any equipment assigned to you

Security of information can be further divided into three core principles:

- Confidentiality (protection against unauthorised disclosure)
- Integrity (protection against unauthorised alteration or corruption)
- Availability (protection against loss of access)

Your system access is conditional on full compliance with this policy and all other referenced policies, as well as any security-specific guidance that you are asked to follow.

3. Information Handling

All information, whether electronic or paper-based, must be protected according to its sensitivity. The key principles are:

- All information must be assigned a security classification. The lowest and most common levels are UNCLASSIFIED (i.e. public) and OFFICIAL (the default). Classified information must not be released externally.
- Irrespective of the classification, information may only be made available on a need-to-know basis
- Data sharing between departments or external parties requires proper authorisation

Full details can be found in IS-POL-002 Information Classification Policy and the accompanying IS-GUIDE-002 Information Handling Guide.

4. Equipment

The term 'equipment' includes computers, smartphones, tablets, cameras, and so on. Equipment assigned to you should only be used for the States business purposes for which it was intended (see also 12.3 Personal use and privacy). In addition:

- All equipment must be kept in good working order and protected from damage, unauthorised access and theft
- Equipment must not be removed from States premises without appropriate authorisation
- Lost equipment must be reported immediately to the IS Service Desk

5. Passwords

Passwords are the primary barrier to unauthorised access, for this reason they require special protection:

- Passwords, pass phrases and PIN codes must not be stored or transmitted insecurely
- Passwords should be long, complex and not reused. They must be changed regularly.
- Never share credentials with anyone unless authorised to do so

If you suspect that your password has been discovered by someone else, change it and advise the IS Service Desk immediately.

6. Office Security

Regardless of your role, the facilities that you work in contain information and systems that must be protected from unauthorised access:

- Computers must be locked when left unattended for short periods: hold down the Windows key (⊞) and press L (for Lock)
- When you leave your work area for any significant length of time (e.g. meetings or breaks) then make sure that paperwork is cleared away
- When leaving the office, all areas must be cleared and draws, cabinets, windows and doors locked
- Confidential waste must be placed in the appropriate containers or destroyed
- Challenge unidentified individuals in, or trying to gain access to, restricted areas

7. Unacceptable use

Unacceptable use of States systems includes, but is not limited to:

a) Accessing, downloading, storing, processing, publishing, displaying or sending inappropriate material. For example, material that is illegal, pornographic, or likely to cause offense
b) Activity that could damage someone's reputation; which is meant to annoy, harass or intimidate another person in any way; or, or could lead to litigation
c) Attempting to access any information or systems that you are not authorised or intended to have access to
d) The use of internet-based office applications ('cloud services'), internet-based email accounts ('web-mail'), online file storage, social networking, and gaming sites unless specifically authorised to do so as part of your responsibilities
e) Downloading, running or installing unauthorised software or material on any computer system, for example, screensavers, games or music
f) Attempting to disrupt or disable computer systems, security controls or services.
g) Causing systems excessive strain, or unwanted or unnecessary interference with other users. For example, broadcasting (distributing widely) unwanted emails, sending jokes, 'chain' letters or hoaxes of any sort
h) Using States systems to carry out your own business or for profit. This includes placing business-related adverts on the intranet
i) Making unauthorised copies of information, passing information to third parties without authority, or retaining States information after termination of employment

7.1. Control failure does not imply permission

The failure of security tools and controls to block certain actions should not be taken as implied permission to ignore policy requirements.

8. Communications

8.1. General

The term 'communications' is broad and includes e-mail, letter, fax, instant messaging ('IM'), chat, blogs, forums, social media sites, voicemail, and media appearances.

In most cases communications are inherently insecure, and control of the contents is lost once it has been released. Most content can be copied, altered and redistributed in unintended and often undesirable ways. Once material reaches the internet it can be virtually impossible to remove. For these reasons special care must be taken when communicating externally.

In addition to the general guidance in Section 7 (Unacceptable use), consider the following:

- Most messages sent or received as part of your official duties are official records. You must not claim your personal opinions represent official States opinions unless this is part of your responsibilities
- When responding to an inflammatory remark, remain professional in your tone and don't be hasty; remember it's an official record and legally discoverable.
- Documents that are made available externally should be first converted to PDF to preserve the integrity of their contents and minimise the risk of hidden data being sent out by mistake.

8.2. Email

If you are granted access to a colleague's e-mail (for example to cover holiday or sickness), then under no circumstances should you open messages that are clearly of a personal nature.

Email is not a secure form of external communication. Sensitive communications must be encrypted. Other email good practices to follow are:

- Avoid sending large files; either send as a ZIP file or send a link to the file location.
- When sending to multiple third-party recipients, do not use the 'to:' field, as any address listed will be visible to all other recipients. Instead use the 'bcc:' field.
- Messages such as virus warnings, security threats, offers, scams, chain emails and so on should not be opened or forwarded to colleagues or replied to. Instead they should be reported to the IS Service Desk so that filtering controls can be updated.
- Avoid broadcasting emails to lots of people. Instead limit the recipients to those who actually need to know and have a genuine interest.

Do not forward business messages to a personal email account. A more extensive guide to email best practices is available in IS-GUIDE-003 (Email Management Guide).

8.3. Social media, blogs etc:

These may only be used for business purposes, but should still be used with caution. Key considerations are:

- Never express opinions or give advice (since this could be deemed as attributable to the States)
- Never post technical information or personal details
- Always use generic emails

- Under no circumstances post classified data
- Complex material should be prepared offline, and independently checked prior to posting.

8.4. Phone, fax, post

When using the telephone to discuss sensitive matters, be aware of the risk of being overheard; some meeting rooms do not provide adequate sound-proofing.

When sending a sensitive fax, ensure that the intended recipient is there to receive it.

If mailing or couriering sensitive information, ensure the package is carefully labelled so as not to indicate its contents.

9. Record keeping

Special attention must be given to the organised filing of any official records, which includes:

- Matters relating to a business relationship or contract
- Interactions with the public or businesses
- Instructions and advice given or received
- Minutes of board meetings

Any such material must be carefully stored in a structured, organised filing system, and retained in line with an approved retention schedule.

9.1. Where to store documents

Documents that constitute records must be captured using one of the following methods (in order of preference):

- Captured SharePoint or LiveLink
- Saved on shared L: drive in .msg format at the appropriate place in the organisational filing system
- Printed to paper and placed in the organisational filing system

9.2. Your personal H: drive

This folder is intended as a temporary work area, or for documents that are of a private nature such as appraisals. Although it is assigned to you it can still be accessed by certain ISD staff. The H: drive is not intended for personally-owned material (See also 12.3). All other corporate information must be stored using one of the approved storage locations described above.

10. Backups

If you are responsible for a standalone system, then you are also responsible for ensuring that appropriate backups are made. Backup media must be stored securely and kept separate from the original system.

11. Data Protection

11.1. States Departments

Each States department handles personal data and is therefore required to register individually with the Data Protection Commissioner.

11.2. Users

It is every user's responsibility to ensure that they understand:

- the general requirements of the Data Protection Law
- Who their Data Protection Officer is
- What types of data processing has been approved for their department

Special care should be taken when transferring or hosting data off-island, since this may breach the law if the relevant exemption has not been granted.

11.3. States Members

All States Members who handle personal data must be notified to (i.e. have registered with) the Data Protection Commissioner. You must notify in your own right as an individual regardless of any States Department Data Protection notification you may be part of. It is your responsibility to ensure that you have notified. Failure to comply will lead to your account access being disabled.

If you believe there are legitimate reasons for States sensitive information to be released externally, then you are referred to the best practices set out in the Information Handling Guide (IS-GUIDE-002). A key requirement is that the Information Owner pre-approves the release. Any unapproved or uncontrolled release will may be in breach of data protection laws, and in any event will treated as a security breach and sanctions imposed accordingly.

12. Monitoring and Privacy

To maintain and improve security, ensure policy compliance, and support the investigation of security incidents, all systems are continuously monitored and periodically audited.

12.1. E-mail archival

All e-mails sent and received, internally and externally, are automatically archived in a secure forensic archival system. Users should therefore be aware that all messages, even if deleted or altered in Outlook, may be retrievable for a designated period of time.

12.2. Disclosure of user activity

ISD are authorised to inspect all user activity that takes place across States systems, in order to investigate or detect inappropriate activity. Details may also be passed to law enforcement or regulatory agencies.

12.3. Personal use and privacy

Where permission is given, limited personal use of IS systems is allowed providing it does not incur significant extra cost or risk, does not adversely affect your work and you follow the acceptable use principles outlined in this document. In respect of privacy, this applies whether the equipment belongs to you or the States.

Users are discouraged from storing or transmitting their own personal data on States systems. Where this is unavoidable, then information should be segregated by placing it in a clearly designated folder. This is done entirely at the user's own risk, and the States of Jersey cannot be held liable for any claims arising from the unauthorised disclosure or loss of users' personal data held in this way.

Users are also reminded that personal devices used for States business under the terms of the BYOD Policy (IS-POL-014) may be wiped remotely,

13. Incident Reporting

You are responsible for reporting any security breaches, suspicious activity or other policy violations that you become aware of. Concerns should be reported in the first instance to the IS

Service Desk so that they can log and track the issue and correlate with any similar events that occur. As a second choice you may refer to your line manager or approach the Data Security Officer directly.

Under no circumstances should you attempt to prove a suspected issue exists, as this may constitute unauthorised activity and may damage valuable evidence. Similarly, do not attempt to respond to a breach yourself unless you have been suitably trained and authorised to do so.

You are encouraged to make handwritten notes of any actions you have already taken, or any other observations that you have made, since these may prove useful later on in an investigation.

14. Legal

In most cases users are personally accountable for complying with legal obligations. Therefore it is your responsibility to familiarise yourself with, and adhere to the legal, regulatory and contractual requirements of your position. Common areas to consider include:

- Anyone who handles information about individuals is bound by the Data Protection (Jersey) Law 2005 or other relevant law if the data is held off-island.
- The Computer misuse (Jersey) Law 1995 makes it an offence access or alter computer material without authorisation.
- Credit card payments are subject to the rules of the Payment Card Industry Data Security Standard (PCI DSS).
- Creative works produced during the normal course of your employment or duties become the Intellectual Property of the States of Jersey.
- Articles, images and recorded media published by others (e.g. on the internet or in the news) are normally subject to copyright law. Therefore permission must be obtained before re-using or circulating such material.
- Official Secrets (Jersey) Law 1952 – wrongful communication of secret information.
- The Freedom of Information (Jersey) Law 2011 gives citizens the right to ask for any information that is held by the States.

15. Exemptions

In rare circumstances 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.

16. Sanctions

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

- suspension or withdrawal of system access
- disciplinary action up to and including dismissal
- legal action

17. References

This policy refers to the following documents:

Policy and Guidance

IS-POL-002	Information Classification Policy
IS-POL-014	BYOD Policy

IS-POL-017	Email Records Management Policy
IS-GUIDE-002	Information Handling Guide
IS-GUIDE-003	Email Management Guide

Mystates:

Writing Emails
Social Media Strategy
Internet and Email Rules

18. Agreement

By signing this document I confirm I have read and understood this policy on acceptable use of information systems and technology and will adhere to the rules outlined.

Signature (User)	Name in full	Date

(Please ensure that the signed copy of this document is placed on the user's personal file.)