States of Jersey	Information Classification Policy
IS-POL-002	

1. Purpose and Scope

This policy sets out the requirements for information classification within the States. All information handled within the States, whether paper or electronic must be protected according to its value and sensitivity.

This policy applies to all physical and electronic information held or processed by or on behalf of the States, and to employees, temporary staff, contractors and other third-parties with access to States information.

2. Classification Levels

Information must be classified into one of the following categories to ensure the correct level of protection is applied:

UNCLASSIFIED: non-sensitive information that can be accessed or shared freely with all employees, or members of the public.

OFFICIAL: information that is only accessible to employees (or professional advisors, regulators etc.) who have a business interest in the information. This is the default classification.

OFFICIAL – SENSITIVE: information that is only accessible to specific named persons. Examples include employment records, medical records, and assurance reports.

SECRET and **TOP SECRET**: information that if compromised could lead to severe financial loss, risk to life, or adversely impact national security. These increased levels are rarely used and require special handling arrangements; refer to the Data Security Officer for guidance.

3. Data Owners

3.1. General obligations

A Data Owner is an individual who has overall responsibility for collecting, updating, and controlling an information asset. All information must be assigned a data owner; this may be a named individual or specific role. The Data Owner must classify information that they are responsible for.

3.2. Day to day responsibilities

In addition to setting the classification level, Data Owners' responsibilities also include:

- Approving access requests
- Periodic audits of access levels
- Business continuity arrangements for the information asset

- Applying data retention and disposal policies
- Communicating additional risk-based requirements for protecting data

Only the Data Owner can reclassify information.

4. Protective Markings

All information must be clearly labelled with the classification level. As a minimum this should be on the first page of the document, or in the header/footer. The classification level is always printed in uppercase.

5. Security Controls

The security controls that must be applied depend on the classification level:

OFFICIAL

- Access is restricted on a need-to-know basis. Use of shared folders that many users can access is not permitted
- If removable devices (e.g. USB Keys, laptop hard drives, smartphones) are being used they must be encrypted to an approved standard. Encryption keys and passwords must not be stored with the device
- Information must not be left freely available in areas where it may be read by members of the public or other unauthorised individuals
- Data must be securely destroyed when no longer needed e.g. cross-cut shredder. Hard-drives and removable media should be referred to ISD for secure wiping or destruction
- Staff must undergo basic vetting procedures before access is granted

OFFICIAL – SENSITIVE

In addition to the basic controls above, OFFICIAL - SENSITIVE data must have the following additional protection:

- Access is allowed from home, but not where other family members can see it. (See also Acceptable Use Policy)
- Working in public places and while travelling is not permitted
- Individual documents must be encrypted where they are mixed with lower classification documents in the same folder
- Standard corporate email must not be used, instead use an approved secure email or document transfer service
- Minimise photocopying, printing and scanning
- Hand deliveries must be in person, in a sealed container, and receipted
- Data can be transported by car, but must be kept out of sight and never left unattended
- Staff must undergo enhanced vetting procedures according to the individual's role and the type of access required. Checks will normally include criminal records, employment/education history and credit rating. Refer to HR or departmental-specific vetting procedures.

6. Sanctions

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

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

7. Related Documents

IS-POL-001 Acceptable Use Policy

IS-GUIDE-002 Information Handling Guideline

Media Disposal Procedures (ISD Standard Operating Procedure)