Ministry of Communications & Information Technology

Information Classification and Handling Standard

Table of Contents

Introduction

1.1 Purpose

In our day to day operations, Ministries and the Government of Samoa create, hold and receive a large volume and range of information, including but not limited to citizens or the Government itself. Some of this information will be sensitive or secret and as such must be protected from compromise, modification or other loss or unauthorised disclosure. Protecting information from potential disclosure or modification means that handling requirements (people and technology controls) - where necessary - must be applied.

The requirements outlined within this Standard are here not to cause hinderance but provide benefit. Information classification should not only foster trust between Ministries, ensuring that all Ministries understand and treat information that is shared between each other appropriately, but it should also demonstrate to Samoan citizens that we protect their information as required.

The Government of Samoa (GoS) have designed and developed the following Information Classification and Handling Standard. This will assist Ministries to appropriately and consistently assess the sensitivity of the information they hold, classify that information, and then apply (if any), the relevant handling requirements.

1.2 Scope

This standard applies to all GoS information assets, including those assets which may be handled or stored by external suppliers or service providers, but reside under the control of GoS. Additionally, it includes all supporting electronic and physical systems underpinning the information - whether maintained within GoS systems and premises, or hosted / managed by contracted third parties.

1.3 Non-compliance

Failure to appropriately classify and handle data in accordance with this standard may result in a negative impact to the GoS, its partners and citizens, such as reputational damage, disruption to operations, or loss of privacy.

Compliance with this policy shall be monitored internally. Any employee who becomes aware of any violation or suspected violation of this policy must inform the Cybersecurity division. Failure to comply will result in disciplinary actions. The Cybersecurity division will be informed and where it is deemed necessary, non-compliance may be escalated to the CEO of the Ministry of Communications & Information Technology (MCIT) to be dealt with.

Information Classification Labels

The GoS has identified 6 classification labels into which it's information may be categorised under.

UNOFFICIAL

- This type of information is not related to work that is performed by the GoS or any of it's Ministries, nor does it form part of any official duty. In some instances, this information may already be public.
- This type of information does not require any protections because **public disclosure of this information will not impact the GoS or a Ministry**.

  E.g. information sent about dinner from a work laptop

OFFICIAL

- Official information is information that is generated or collected as part of the GoS or one of it's Ministry's routine operations. This information is designed to be consumed by the public.
- This information is still important, and will require some controls and protections in place to ensure it's integrity and availability are maintained (confidentiality is less of a concern). **Public disclosure of this information will result in no or insignificant damage** to the Ministry or GoS.

  E.g. Government press releases, public health figures, published annual reports

OFFICIAL: SENSITIVE

- Official Sensitive relates to Information and assets collected or used that could **result in limited damage to an individual, one of the Ministries, or the GoS if compromised**. As such, information or assets deemed 'Sensitive' require additional care when handling.

  E.g. Personally identifiable information (PII), political or religious affiliations, health information, biometric information, commercial in confidence information, ISP meeting minutes about market share

PROTECTED

- Protected information and assets are those that are collected and used and **if compromised, would damage national interests, Ministries or individuals.**
- This category also includes Cabinet Submissions made by Ministries, as well as cabinet decisions.

  E.g. Unpublished legislation, Strategic initiatives of GoS ministries

SECRET

- Information and assets collected or used that if compromised **would cause serious damage to national interests, Ministries or individuals or disrupt foreign relations**.
- This category also applies to Cabinet papers/memoranda, the Cabinet business list and Cabinet minutes which is the exclusive property of the Cabinet of Samoa.

  E.g. Intelligence briefings, government research papers relating to national security

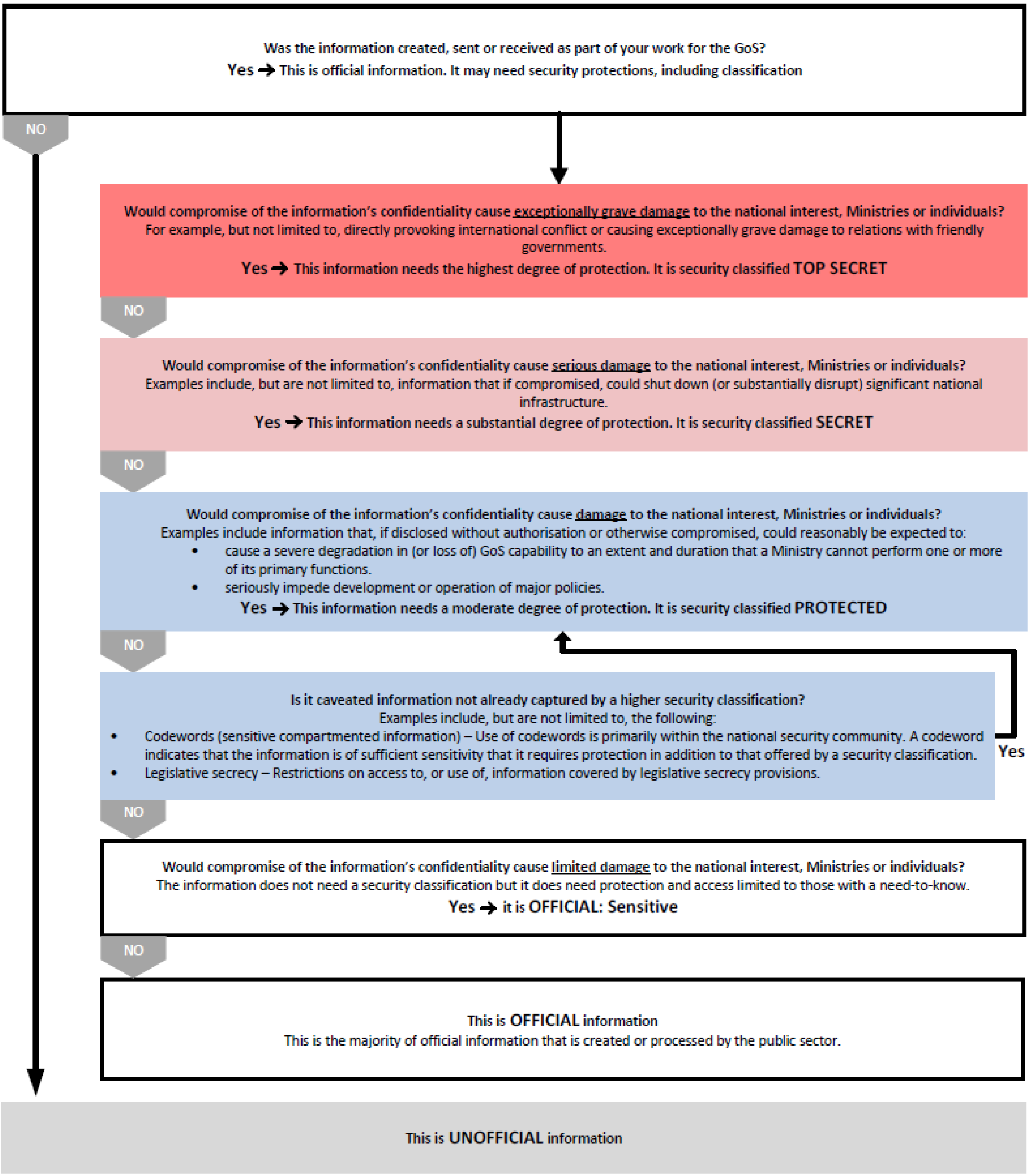
TOP SECRET

- Information and assets collected and used that **if compromised would cause exceptionally grave damage to national interests, Ministries or individuals.**

  E.g. Military defence plans and operations, nation state trade deals prior to announcement

How to classify information

Any piece of information, once created or collected, must be classified. To classify information, you are required to assess it and the impact that its disclosure would result in (as per the classification labels above). The following diagram demonstrates the process that all staff should familiarise themselves with to consistently and appropriately classify information.



Was the information created, sent or received as part of your work for the GoS?
Yes → This is official information. It may need security protections, including classification

NO

Would compromise of the information's confidentiality cause exceptionally grave damage to the national interest, Ministries or individuals?
For example, but not limited to, directly provoking international conflict or causing exceptionally grave damage to relations with friendly governments.
Yes → This information needs the highest degree of protection. It is security classified **TOP SECRET**

NO

Would compromise of the information's confidentiality cause serious damage to the national interest, Ministries or individuals?
Examples include, but are not limited to, information that if compromised, could shut down (or substantially disrupt) significant national infrastructure.
Yes → This information needs a substantial degree of protection. It is security classified **SECRET**

NO

Would compromise of the information's confidentiality cause damage to the national interest, Ministries or individuals?
Examples include information that, if disclosed without authorisation or otherwise compromised, could reasonably be expected to:

- cause a severe degradation in (or loss of) GoS capability to an extent and duration that a Ministry cannot perform one or more of its primary functions.
- seriously impede development or operation of major policies.

Yes → This information needs a moderate degree of protection. It is security classified **PROTECTED**

NO

Is it caveated information not already captured by a higher security classification?
Examples include, but are not limited to, the following:

- Codewords (sensitive compartmented information) – Use of codewords is primarily within the national security community. A codeword indicates that the information is of sufficient sensitivity that it requires protection in addition to that offered by a security classification.
- Legislative secrecy – Restrictions on access to, or use of, information covered by legislative secrecy provisions.

Yes

NO

Would compromise of the information's confidentiality cause limited damage to the national interest, Ministries or individuals?
The information does not need a security classification but it does need protection and access limited to those with a need-to-know.
Yes → it is **OFFICIAL: Sensitive**

NO

This is **OFFICIAL** information
This is the majority of official information that is created or processed by the public sector.

This is **UNOFFICIAL** information

Information Handling Requirements

	OFFICIAL	OFFICIAL: SENSITIVE	PROTECTED	SECRET	TOP SECRET
Encryption and Storage	Encryption isn't required on internal networks. Approval as to whether encryption is required by the CEO. Storage is allowed if unauthorized access is prevented.	Information at rest and in transit must have encryption applied. Storage is allowed if controls preventing unauthorised access is in place.	A minimum best practice level of encryption (e.g. AES 128) must be applied when in transfer over public networks, and when at rest (both on internal and public networks)	Internationally recognised best practice encryption (e.g. AES 256) is required when in transit must be applied at rest. Storage only to occur if absolutely necessary.	Internationally recognised best practice encryption (e.g. AES 256 / TLS 1.3) is required for transfer when in transit. Encryption must be applied at rest. Information is not to be stored.
Sharing and Transportation	Authorised personnel can share and carry this information. Receipt of acknowledgement by the intended audience should be considered. Reputable carriers and tracked postage are required when sharing.	Anyone authorized by the CEO or with access based on their role can share and / or carry this information. Transmission must be done using pre-approved carriers and secure carry methods only.	Only those who are authorized to know about / of the information or asset may carry and share protected information. Any information shared must have its receipt acknowledged. It cannot be emailed or left unattended).	Information / assets cannot be carried or shared outside of those who are aware based on the 'need-to-know' principles. This information is not to leave the room it is shared in.	Information / assets cannot be carried or shared outside of those who are aware based on the 'need-to-know' principles. This information is not to leave the room it is shared in.
Retention	In the absence of a regulatory retention obligation, a common timeframe must be established for the retention of Official information by the MCIT.	Retain this information according to any regulatory requirements (e.g. medical, business, privacy or cabinet obligations). A timeframe for the retention of all other information that is classified as Official Sensitive should be applied, after which it is disposed of.	Protected information may only be retained for the minimum period necessary.	This material should not be retained longer than necessary. Retention is only allowed in exceptional circumstances. Approval to retain this material can only be granted by the most relevant senior staff member with Top Secret clearance.	Information classified as 'Top Secret' must not be retained any longer than necessary, and must follow the relevant disposal procedures below as soon as it is no longer required.
Disposal	Disposed of as per best practices and available means. Media/assets may be reused.	Disposal procedures determined as sufficient by CEO. Media/assets may be reused, and must be sanitized through procedures determined as sufficient by the CEO with advice from MCIT ICT & SamCERT.	Disposal procedures determined as sufficient by CEO. Media/assets may be reused ONLY if necessary and must be sanitized through procedures determined as sufficient by the CEO with advice from MCIT ICT & SamCERT	Destroyed ASAP by authorised persons only, under supervision and through specific burning, shredding or disintegration practices with evidence of disposal. Media/assets are not reused.	Destroyed ASAP by authorised persons only, under supervision and through specific burning, shredding or disintegration practices with evidence of disposal. Media/assets are not reused.
Access	Access to information of this classification is provided as per job function and restrictions are not required.	Access is only provisioned to specified personnel and access is only to be granted by the CEO.	Access is only provisioned to authorised personnel and access is only to be granted by the MCIT CEO after being discussed with relevant stakeholders.	Access is on a need-to-know basis and only to be granted by the Minister.	Access is on a need-to-know basis and only to be granted by the Ministry of Prime Minister and Cabinet (MPMC)

Information classification across the lifecycle

2.1 Information Re-Classification

Staff must give consideration to information throughout its lifecycle, and keep in mind that information classification labels will need to be monitored, reviewed and sometimes, reclassified.

The classification label applied to a piece of information or asset may change and fluctuate over time and throughout its lifecycle, depending on the context it resides in and with any changes that may impact its confidentiality. For example, what once may have been labelled OFFICIAL SENSITIVE may now be public (e.g., a press release) and as such, no longer requires the same protections that were previously in place.

Data aggregation may also result in changes to information classification labels.
This occurs when information that may relate to an individual system, person or document, is compiled with other similar sets of information, which creates a profile or group of information that require additional protections because compromise could result in greater harm.
For example, one piece of information may have no sensitivity in isolation, but when compiled reveals patterns or details that would be considered OFFICIAL SENSITIVE.

As such, it is a requirement that staff and information owners are reviewing their data sets at regular intervals to identify whether over time classification has changed and either requires a lower, or higher designation.

Version Management

Version	Date	Comments and Remarks
1.0		