

Information Classification & Handling Policy

1.0 Purpose

- 1.1 To define the information classification and handling policy for information assets.

2.0 Scope

- 2.1 For NYP staff who are involved in the handling of information assets.

3.0 Officer-in-charge


- 3.1 CNC is responsible for the maintenance and updating of this policy.

4.0 Information Classification and Handling Policy

4.1 Information Asset Classification and Control

- 4.1.1 Information assets should be appropriately classified and managed to prevent unauthorised access, modification and destruction. The **Singapore Government Security Instruction for the Handling and Custody of Classified Information** should be referred to.
- 4.1.1.1 All information assets should be identified. If assets are not identified and documented, they may not be given adequate protection.
- 4.1.1.2 The security classification of the information asset should be documented. This is to make clear the level of protection required for that information asset. In addition, it should also include the sensitivity categorisation which considers the impact of unauthorised disclosure of entity data, which comprises data on individuals and business.
- 4.1.1.3 Information assets shall be security graded solely on its content and security implications according to the following classifications:
- Official (Open)
 - Official (Closed)
 - Restricted
 - Confidential
 - Secret
 - Top Secret
- 4.1.1.4 Information assets shall be categorised according to the following Sensitivity:
- Sensitive High (causes serious physical, financial, or sustained emotional injury or social stigma to the individual; causes sustained financial loss to business)
 - Sensitive Normal (causes temporary and minor emotional distress or disturbance to the individual; causes a reduction in competitiveness or a compromise of business interests)
 - Non-Sensitive (does not cause physical, financial, or emotional injury to the individual; OR in personal information that is socially expected to be openly available; Does not impact a


business' processes or operations; OR is Business information that is socially accepted as openly available)

4.1.1.5 Please click  [here](#) to refer to the Guide to Right-Classification of Systems

4.1.2 Any information asset bearing a security classification such as Restricted, Confidential, Secret, or Top Secret is a classified information asset.

4.1.3 Information assets in NYP as endorsed by NYP IT and Digitalisation Steering Committee is mainly non-national security information in which case if it is classified, the security classification should either be

- Restricted or
- Confidential

4.1.4 Please click  [here](#) to refer to the Security Classification and Sensitivity Categorisation for NYP Application Systems.

4.1.5 Information assets are classified in NYP as follows:

Info Type	Information Assets	Security, Sensitivity Classification
Student & Course-related	BOG Papers	Restricted, Sensitive Normal
	Course Proposals (* ¹)	Restricted, Sensitive Normal
Agreements	MOUs/Partnership Agreements Approval Papers (* ²)	Restricted, Sensitive Normal
Financial	Payroll Data	Restricted, Sensitive Normal
Personnel & Company-related	Staff Salary	Restricted, Sensitive Normal
For Information Assets not listed in this table, they are "Official(Open) / Official(Closed)" by default.		

(*¹) **Before the course is launched**

(*²) **MOUs/Partnership Agreements Approval Papers are generally Official (Closed).**

However, selected papers may be classified as Restricted, if the partner requests for it

4.2 Information Labelling and Handling

4.2.1 Classified information should be handled with care and should not be left unattended. Classified information in softcopy should be kept on NYP-issued external electronic storage media that must be FIPS 140-2 Level 3 encrypted or equivalent standard with authentication and minimally AES-256 bit encryption enabled, and the storage media must be kept securely in the office.

To minimise the risk of sensitive data being compromised on user devices, staff shall ensure that sensitive data can only be accessed through NYP's or central Whole of Government secure platforms, where practicable.

Where practical, staff shall utilise the approved central document collaboration platforms such as NYP Share Point or Singapore Government Document Collaboration Service (SG-DCS) for accessing, sharing and editing of documents containing data

Where practical, staff shall utilise the approved data platforms of the GDA such as Analytics.Gov and Vault to access, share and analyse data.

4.2.2 When information is printed, it should keep its security classification so that users can identify what document handling procedures need to be followed.

- All classified material should be stamped or labelled accordingly.
Hardcopy output from user applications should show the security classification of the information
- being printed. This will ensure that the printed output will be given appropriate protection according to its security classification.
- Hardcopy classified information should be kept under lock and key and not be left unattended.

- 4.2.3 No person shall be given knowledge or possession of any classified information unless there is a need for him/her to know or possess such information. Hence, discussion on classified information should not be carried out in the presence of staff/vendors who are not supposed to know.
- 4.2.4 Staff are not allowed to host, store or process classified information or materials in non-government facility including but not limited to public cloud, online services and messaging platform such as DROPBOX and Google Drive
- 4.2.5 If public cloud or online services for unclassified information is to be subscribed, staff shall assess the risks of using these online services and storage facilities and ensure that no classified information is stored in these online services.

Document No.: ICTS-03, Version: 17, Effective Date: 1 Aug 2023

Updated By / Date: Nicole Yong / 21 Jul 2023

Approved By / Date: IDSC Policy Work Group (IPWG) / 1 Aug 2023