DATA PROTECTION POLICY

(Policy for Data Protection, Data Classification, Information Labelling and Handling Procedures)

DOCUMENT SUMMARY:

AUTHOR	INFORMATION SECURITY MANAGER
REVIEWED BY	CIO/CISO
CURRENT VERSION	2.0
DATE OF CURRENT VERSION	04-03-2020
DATE OF ORIGINAL VERSION	05-08-2018
DOCUMENT REFERENCE NO.	SFO-DPP-POL-002
DOCUMENT TYPE	POLICY
DOCUMENT STATUS	FINAL
DOCUMENT CIRCULATION	NEED BASED CIRCULATION ONLY
OWNER	INFORMATION SECURITY MANAGER
APPROVED BY	MANAGING DIRECTOR

DOCUMENT AMENDMENT RECORD

CHANGE NO.	DATE	PREPARED BY	BRIEF EXPLANATION
1	05-08-2018	Policy for Data Protection, Data Classification, Information Labelling and Handling Procedures	Version 1.0
2	04-03-2020	Policy for Data Protection, Data Classification, Information	Version 2.0

		Labelling and Handling Procedures	

1.0 Purpose

1.1 The purpose of this policy is to establish a framework for information protection and classification of 'SFO' data and to set out the procedures for appropriate handling of information according to its criticality to 'SFO''s objectives and relevant compliance requirements. 'SFO' has adopted this policy to safeguard the confidentiality, integrity and availability of its information assets.

With this policy, we ensure that we gather, store and handle data of employees, customers, stakeholders and other interested parties fairly, transparently and with the utmost care and confidentiality and respect towards individual rights.

2.0 Scope

2.1 This policy applies to all work-related data held by and on behalf of 'SFO'. It applies to all employees and staff, visitors, contractors and third-parties handling 'SFO' data.

2.2 'SFO' IT systems designed for specific purposes or inherited to support certain processes and are not covered in this policy must have local information management and data handling policies and procedures that align with this policy.

2.3 This policy does not cover data (information) that is non-work related.

3.0 Principles

3.1 All 'SFO' data will be classified in terms of its value, sensitivity and confidentiality using the Data Classification Table.

3.2 As defined in the Data Classification Table, information will be appropriately labelled. All staff are required to follow the procedure for information labelling.

3.3 The Data Classification, Information Labelling and Handling Procedures will direct how 'SFO''s information should be classified, labelled and handled. Where information falls within more than one classification group, the more stringent information labelling and handling procedure will apply.

3.4 This policy will apply to information handling and management in all processes, projects and services that involve the processing of highly sensitive, confidential and personal data. Project leads/managers will ensure that documentation exists describing: the data involved and named data owners, the assigned classification group or groups and labelling, and handling procedures.

3.5 Third parties responsible for handling information on behalf of 'SFO' are required to have procedures for appropriate and secure handling of 'SFO' information in place to safeguard such information and maintain compliance with regulatory requirements.

4.0 Responsibilities

4.1 Data owners are responsible for ensuring that the appropriate data classification group and information labelling are assigned to the data used within their Business Units, Divisions and Projects and the appropriate handling procedures (in terms of storage, access, dissemination, and disposal of data and storage devices) comply with related 'SFO' Information Security and Data Protection Policies.

4.2 Periodically, data owners should review the classification groups assigned to 'SFO' data under their care to ensure their classifications are still appropriate in the light of new or changes to this policy, legal, academic and administrative requirements. In all cases, data sensitivity and value to 'SFO' should guide any data reclassification and handling.

4.3 Where data is classified as Highly Sensitive or Personal/Confidential, this should be made clear to those who have access to the data. Records Coordinators must ensure they follow the appropriate guidelines provided in this policy.

4.4 All individuals who access, use or manage 'SFO''s information are responsible for applying the appropriate handling rules for each classification group, and to seek advice from their line manager and the Information Security Manager if more clarification is required on how to handle 'SFO' information.

4.5 All individuals who access, use or manage 'SFO''s information are responsible for reporting any breach of this policy to the IT Service Desk.

5.0 Compliance

5.1 'SFO' has an obligation to comply with relevant statutory, legal and contractual requirements. The Data Classification Policy and Information Handling Procedures are part of the Information Security suite of policies, designed to ensure that 'SFO' information (from creation to retention and/or

destruction) is handled in the most secure manner to satisfy business and relevant compliance requirements.

5.2 Failure to adhere to this policy and related procedures will be addressed in accordance with relevant 'SFO' disciplinary procedures and third-party contractual clauses relating to non-conformance with the Information Security Policy and related policies.

Data Classification Guide

Classification Type	Highly Sensitive (HS)	Confidential / Personal (CP)	Open /Non-sensitive(Open)
	Highest and Strictest controls on Data Labelling and Data Handling to ensure Confidentiality and Integrity.	Appropriate levels of controls to ensure Confidentiality and Integrity.	Unrestricted access and free for sharing.
Examples	Highly sensitive business and commercial information relating to the organisation or other organisations e.g. a trade secret; commercially sensitive design, solution, engineering drawing etc	Personal information about individuals who can be identified from it. Some examples include their salary information, copies of CVs, contact details.	Information which is in the public domain.
	Sensitive financial information e.g. contractual information at the time of tender, eg quotes, proposals, pricing data	Commercially sensitive information e.g. contractual information, or supplier information provided in confidence.	Information which should be routinely disclosed e.g. some minutes of meetings.
	Unprotected intellectual property.		
	Sensitive personal information e.g. race, ethnic origin, politics, religion, trade union, membership, genetics, biometrics (where used for ID purposes), health, sex		

	life, or sexual orientation.		
	Sensitive IT information e.g. authentication details eg passwords, tokens etc		
Level of Protection Required	Such information requires a high level of security controls that will ensure its confidentiality and integrity is maintained at all times. It should only be shared under a very strict environment such as: - provide only hardcopies to authorised individuals in face to face meetings and retrieve these copies at the completion of any meeting. Where this is not possible, use email, post or hand delivery with the appropriate marking in place (refer to the data handling procedures below). - those receiving highly sensitive data must only make additional copies or edits with the originator's authority. - and only on a "need -to–know" basis within 'SFO', or external to 'SFO', to fulfil statutory and legal requirements. • It should be kept up-to-date and stored in highly restricted areas within centrally managed server locations, shared areas or cloud storage, or restricted physical storage	Such information requires the most suitable security controls that will ensure its confidentiality and integrity is maintained at all times with limited access only on a "need -to –know" basis within the 'SFO', or external to 'SFO', to fulfil statutory and legal requirements. • It should be kept up-to-date and stored in highly restricted areas within centrally managed server locations, shared areas or cloud storage, or restricted physical storage areas. Access should be limited to named data owners and authorised individuals, and appropriate monitoring controls and backup arrangements put in place. 'SFO' approved storage facilities should be used where third parties are responsible for data management. • Data should be securely wiped off electronic devices where device has been decommissioned or disposal of paper records should follow confidential waste disposal procedures.	Such information requires the most suitable security controls that will ensure its confidentiality and integrity is maintained at all times with limited access only on a "need -to –know" basis within the 'SFO', or external to 'SFO', to fulfil statutory and legal requirements. • It should be kept up-to-date and stored in highly restricted areas within centrally managed server locations, shared areas or cloud storage, or restricted physical storage areas. Access should be limited to named data owners and authorised individuals, and appropriate monitoring controls and backup arrangements put in place. 'SFO' approved storage facilities should be used where third parties are responsible for data management. • Data should be securely wiped off electronic devices where device has

	areas. Access should be limited to named data owners and authorised individuals, and appropriate monitoring controls and backup arrangements put in place. 'SFO' approved storage facilities should be used where third parties are responsible for data management. • Data should be securely wiped off electronic devices where device has been decommissioned, or disposal of paper records should follow confidential waste disposal procedures.		been decommissioned or disposal of paper records should follow confidential waste disposal procedures.
Type of Information/information asset			
Paper records	'SFO' Office areas with restricted access: - Keep files in lockable cabinets/drawers which are locked when not in active use. - No papers left out when away from the desk. 'SFO' Office areas with unrestricted access: x Not permitted Off-site working - At home: Should be kept away from public view and stored securely when not in use e.g. kept in lockable cabinets/drawers. - Elsewhere or in transit: Not to be left	'SFO' Office areas with restricted access: - Keep files in lockable cabinets/drawers which are locked when not in active use. - No papers left out when away from the desk. 'SFO' Office areas with unrestricted access: x Not permitted Off-site working - At home: Should be kept away from public view and stored securely when not in use e.g. kept in lockable cabinets/drawers. - Elsewhere or in transit: Not to be left	Permitted. Follow good records management procedures.

	unattended at any time or visible in the car. Post - Must be addressed properly to a named individual, sealed and stamped with 'Private and Confidential' with a return address if not delivered. o Use recorded delivery. Hand or courier delivery should also be considered where possible. o It is recommended that the addressed envelope be enclosed in another sealed and properly addressed envelope. Fax x Not permitted	unattended at any time or visible in the car. Post - Must be addressed properly to a named individual, sealed and stamped with 'Private and Confidential' with a return address if not delivered. o Use recorded delivery. Hand or courier delivery should also be considered where possible. o It is recommended that the addressed envelope be enclosed in another sealed and properly addressed envelope. Fax x Not permitted	
Email			
Internal to 'SFO'	REQUIRED - Only share on a "need-to-know" basis. - Password-protect email attachments. - Mark email with private or confidential. - Verify the recipient's address before you click send. - Redact sensitive information from email messages and attachments if not relevant to all recipients particularly from email chains. - Avoid putting Data Subject name(s) in the Subject field, where possible. x Not permitted: Auto forwarding to personal email.	REQUIRED - Only share on a "need-to-know" basis. - Mark email with private or confidential. - Verify the recipient's address before you click send. - Redact confidential or private information from email messages and attachments if not relevant to all recipients particularly from email chains. - Avoid putting Data Subject name(s) in the Subject field, where possible. x Not permitted: Auto forwarding to personal email. Good practice: Password-protect email attachments.	Permitted

Incoming and outgoing from/to 'SFO' email domian.	Only where the recipient does not have an 'SFO' email account and it is absolutely necessary to use this method for a business purpose: REQUIRED - Be sure the recipient understands the risk involved, accepts this method, and will treat the data correctly. - Only share on a "need-to-know" basis. - Password-protect attachments. - Mark email with private or confidential. - Verify the recipient's address before you click send. - Redact sensitive information from email messages and attachments if not relevant to all recipients particularly from email chains.	Only where the recipient does not have an 'SFO' email account and it is absolutely necessary to use this method for a business purpose: REQUIRED - Be sure the recipient understands the risk involved, accepts this method, and will treat the data correctly. - Only share on a "need-to-know" basis. - Password-protect attachments. - Mark email with private or confidential. - Verify the recipient's address before you click send. - Redact sensitive information from email messages and attachments if not relevant to all recipients particularly from email chains.	Permitted
Between two non-'SFO' email accounts for work purposes	x Not permitted	x Not permitted	x Not permitted
Drives / 'SFO' Cloud			
MS Office One Drive and SharePoint	- Permitted You are required to use Microsoft One Drive as part of your O365 licence and owned/shared SharePoint Online sites for work collaboration with 'SFO' team members. - - Only store working documents, that you are working on individually, temporarily in this area. - Ensure appropriate permissions are	- Permitted You are required to use Microsoft One Drive as part of your O365 licence and owned/shared SharePoint Online sites for work collaboration with 'SFO' team members. - Only store working documents, that you are working on individually, temporarily in this area. - Ensure appropriate permissions are assigned to	- Permitted

	assigned to individuals only on a need to know basis. Contact the IT Service Centre for support.	individuals only on a need to know basis. Contact the IT Service Centre for support.	
File Server - Shared Drive	- Store only in restricted folders on your shared drive U: (restricted folders can be requested by contacting the IT Service Centre). - Ensure server security and access controls align with 'SFO' standards. - Store only in restricted folders on the shared drive or an approved server. - You should consider additionally to password-protected files that fall in an extremely restricted category. - Ensure appropriate permissions are assigned to individuals only on a need to know basis. Contact the IT Service Centre for support.	- Store only in restricted folders on your shared drive U: (restricted folders can be requested by contacting the IT Service Centre). - Ensure server security and access controls align with 'SFO' standards. - Store only in restricted folders on the shared drive or an approved server. - You should consider additionally to password-protected files that fall in an extremely restricted category. - Ensure appropriate permissions are assigned to individuals only on a need to know basis. Contact the IT Service Centre for support.	- Permitted
Local Drives on Devices	x Not permitted	x Not permitted	- Permitted
Non-'SFO' Administered Cloud Storage such as iCloud, Google drive, Dropbox and any other cloud storage solutions	x Not permitted	x Not permitted	- Permitted
Laptops, mobile and small storage devices			

'SFO' Owned Laptops	- As of the date of the policy, all new 'SFO'-owned laptops much be encrypted in accordance with the centrally agreed process and end point protection enabled. - Individual users are not allowed to have a local administrator or superuser account. . - Information must be password-protected and only saved temporarily on the C: drive/ local drive where access to the shared drive is not possible and must be transferred immediately to the shared drive when access becomes available and deleted from the C: drive / local drive. - Keep files away from public view when working offsite. - Always use only issued laptops for work purposes only.	- As of the date of the policy, all new 'SFO'-owned laptops much be encrypted in accordance with the centrally agreed process and end point protection enabled. - Individual users are not allowed to have a local administrator or superuser account. . - Information must be password-protected and only saved temporarily on the C: drive/ local drive where access to the shared drive is not possible and must be transferred immediately to the shared drive when access becomes available and deleted from the C: drive / local drive. - Keep files away from public view when working offsite. - Always use only issued laptops for work purposes only.	- Permitted
'SFO'-owned mobile and portable storage devices e.g. smartphones, iPads, tablets, USB, CDs	x Not permitted	x Not permitted	- Permitted
Personal laptops, mobile devices and all types of portable storage devices / storage capable devices	x Not permitted	x Not permitted	- Permitted

- Departments that are Classified as Highly Sensitive and who handle HS data on a regular basis:
  - R & D
  - Finance
  - Engineering
  - Software
  - BDG

All HS category data should be identified, labelled and classified.

- All Highly sensitive areas are also maintained under strict access control and video surveillance at all critical areas.

1. **Definitions**

- Information – A meaningful collection and organisation of data
- Information Asset - A collection of information or information systems
- Data Owner – Unit Heads and Department Heads have overall responsibility for the data (records) within their areas of responsibility, with specific responsibility falling to the Records Coordinator(s) in their departments.
- Records Coordinators – Members of staff within 'SFO' Units/Departments with delegated responsibility for facilitating the management of records within their regulations.
- Data Classification: To identify the sensitive nature of information and categorise (classify) it accordingly.
- Information Labelling: To apply the appropriate classification label to information.
- Information Handling: Creating, editing, copying, transmitting/transporting, printing, storing, deleting and archiving information.