الخطة المبدئية لتشغيل عمليات البيانات وتخزينها

ملخص تنفيذي:

تقدم هذه الخطة إطارًا شاملاً لتشغيل عمليات البيانات وتخزينها في الهيئة، حيث تعنى الخطة المبدئية بتحديد آليات وممارسات تشغيل البيانات، بما يشمل عمليات: جمع البيانات وتخزينها وحفظها وحمايتها بما يضمن الكفاءة والأمان والالتزام بالمعايير المعتمدة.

الأهداف الاستراتيجية:

- ضمان تشغيل البيانات بشكل آمن وفعال.
- تحسين كفاءة تخزين البيانات.
- الامتثال للمعايير والسياسات المعتمدة.
- دعم استمرارية الأعمال من خلال خطط تشغيل واضحة.

النطاق:

تشمل هذه الخطة جميع عمليات تشغيل وتخزين البيانات الحساسة وغير الحساسة داخل الهيئة.

الإجراءات:

- تقييم الاحتياجات والقدرات:
  - تحديد متطلبات تخزين البيانات بناءً على طبيعة البيانات ومستوى حساسيتها.
  - تقييم قدرات التخزين والبنية التحتية لضمان كفايتها.

- تخزين البيانات:
  - استخدام حلول تخزين آمنة ومشفرة مع التحكم الكامل في الوصول.
  - تصنيف البيانات وتحديد مستويات الحماية المطلوبة بناءً على حساسيتها وفقًا لمعايير الهيئة.

- حفظ واستبقاء البيانات:
  - تحديد فترات حفظ البيانات والاستبقاء بناءً على المتطلبات القانونية والتنظيمية.
  - تنفيذ آليات آمنة لحذف البيانات بعد انتهاء فترة الاستبقاء.

- ضوابط الأمان:
  - استخدام تقنيات تعتيم البيانات (Data Masking) لحماية البيانات الحساسة عند نقلها إلى بيئات غير بيئة الإنتاج.
  - مراجعة دورية لسياسات تخزين البيانات وممارسات الاستبقاء بما يتوافق مع معايير الهيئة.

- التوثيق والمراجعة:
  - توثيق جميع عمليات تشغيل وتخزين البيانات بشكل تفصيلي.
  - مراجعة دورية للخطة والتحديث بناءً على المستجدات التقنية والتشريعية الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا).

تشغيل البيانات:

- تنفيذ عمليات تشغيل البيانات وفقًا للمعايير الأمنية.
- جدولة مهام تشغيل البيانات بشكل يومي وأسبوعي وشهري.
- ضمان توفر البيانات بشكل مستمر.

استبقاء البيانات:

- ملحق إطار عمل تصنيف البيانات المعتمد (يشمل استبقاء البيانات) / Data Classification Framework

أدوار ومسؤوليات:

- مدير قواعد البيانات :مسؤول عن مراقبة الأداء والصيانة.
- اخصائي قواعد البيانات مسؤول عن تنفيذ الإجراءات الفنية المذكورة.
- مسؤول أمن البيانات :مسؤول عن مراجعة الضوابط الأمنية.
- فريق الدعم الفني :مسؤول عن حل المشكلات الفنية والتقنية.
- فريق الامتثال للبيانات مسؤول عن مراقبة الامتثال بهذه الخطة

أدوات وتقنيات التشغيل والتخزين:

- استخدام أنظمة إدارة قواعد البيانات مثل Oracle و.SQL Server وMySQL
- اعتماد التخزين في مركز البيانات الرئيسي ومركز التعافي من الكوارث
- استخدام نظام التخزين الاحتياطي والاسترجاع والمراقبة - "روبيرك" Rubrik

خطة التنفيذ:

- المرحلة الأولى (شهرين) : تقييم الوضع الحالي.
- المرحلة الثانية (6 شهور): تنفيذ الأدوات والتقنيات المعتمدة.
- المرحلة الثالثة (3 شهور): مراجعة الأداء والتحسين.

المخاطر وخطة التخفيف:

- فقدان البيانات :تطبيق نسخ احتياطي يومي.
- الوصول غير المصرح به :تنفيذ آليات التحكم في الوصول.

مؤشرات الأداء الرئيسية:

- معدل تواجدية البيانات.
- زمن الاستجابة لطلبات البيانات.
- عدد الحوادث الأمنية المسجلة.

التقييم والمراجعة:

- إجراء مراجعات دورية للخطة.
- تحديث مستمر للسياسات والإجراءات بناءً على نتائج المراجعة.
- تقديم تقارير أداء بشكل دوري.

الملاحق:

- ملحق إطار عمل تصنيف البيانات المعتمد / Data Classification Framework

الاعتمادات:

المهمة	الإدارة المسؤولة	التاريخ	التوقيع
إعداد	مدير البنية التحتية وأمن البيانات أ. أنس الحويل		
اطلاع	المدير العام للإدارة العامة للبنية المؤسسية أ. رائد المطيري		
موافقة	المدير العام مكتب إدارة البيانات أ. حصة خالد بن ملافخ		
موافقة	المدير العام للإدارة العامة لذكاء الأعمال والتحليلات أ. خالد القرني		
اعتماد	المدير العام للإدارة العامة للبنية التحتية والتشغيل أ. باسل الدوسري		

الهيئة السعودية للتخصصات الصحية
Saudi Commission for Health Specialties

Unified Data Classification Framework

Document Control

Document Information	
Document Title	Unified Data Classification Framework
Publish Date	
Classification	
Document Version	
Document control Number	

Document Changes			
Date	Version	Name	Notes

Activity	Person	Signature	Date
Drafted by	Innovative Solutions	Innovative Solutions	8 Aug ,2023
Reviewed by	Mohammed Alqahtani		27 Sep 2023
Approved by	Hessah Bin Mulafikh		1 October 2023

Table of Contents

1. Introduction

In today's data-driven world, data is one of the most valuable assets for any organization. However, as data volumes continue to grow, so does the risk of data breaches, which can result in significant financial and reputational damage. Therefore, it is essential for an organization to implement a robust data classification framework as part of their governance, risk management, and compliance (GRC) strategy.
A data classification framework is a fundamental component of any GRC program that helps organizations identify, classify, and protect their most critical data assets. It provides a structured approach to categorizing data based on its sensitivity, value, and risk, which can be used to determine appropriate security controls, access privileges, and retention policies.

Saudi Commission for Health Specialities (SCFHS) is committed to protecting the security and privacy of information residing with SCFHS's assets which is stored, processed, and transmitted, regardless of media type, in accordance with applicable legal & regulatory requirements. Information is a critical and valuable asset to SCFHS. Therefore, the protection of information from a wide range of threats in order to ensure business continuity, minimize business risks and maximize return on investments & business opportunities is imperative by the SCFHS management. To reinforce its commitment to Commission Security, the top management of SCFHS established the Operational

Information Security function whose main purpose is to protect information during storage, processing and transmitting within SCFHS's environment.
The operational security function would identify the risks existing with SCFHS and reduce the same to an acceptable level by deploying management, technical and operational controls without compromising the confidentiality, integrity, and availability of the information. Operational security is seen as an enabler to achieve SCFHS business strategy and objectives. This security framework document is the commitment from SCFHS to provide a secured environment that facilitates business in a more productive manner.

2. Purpose

The primary purpose of a data classification framework document is to establish a consistent and repeatable process for classifying data across the organization. This ensures that all employees, departments, and systems are aligned on how data is classified, which can help minimize the risk of data breaches and ensure compliance with regulatory requirements.
This document is a framework for assessing data sensitivity, measured by the adverse effects a breach of the data would have upon SCFHS. This document has been created to help effectively manage information in daily mission-related activities.
Determining how to protect and handle information depends on a consideration of the data's type, importance, and usage. The document is also intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside the SCFHS without proper authorization. The framework outlines the minimum level of protection necessary when performing certain activities, based on the classification of the information being handled.

3. Scope

This document applies to all data or information that is created, collected, stored or processed by SCFHS, in electronic or non-electronic formats. The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes electronic information, printed data, and data shared manually or electronically.
All employees should familiarize themselves with the information labelling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect the SCFHS's confidential information (e.g., confidential information should not be left unattended in conference rooms).
This Document address the following controls and framework:

- ECC:2018 - 2-7- Data and Information Protection
- DCC:2022 – Data Cybersecurity Controls
- NCAR - National Center for Archives & Records

- CSCC:2019 – Critical Systems Cybersecurity Controls
- NDMO - Data Management and Personal Data Protection Standards

4. Roles and Responsibilities

Each role involved in this framework shall have main responsibilities as follows:

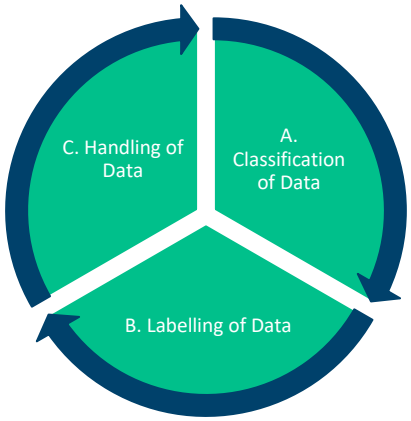
Role	Responsibility
SCFHS Cybersecurity Steering Committee	• Provide leadership and oversight for the execution of the Data Protection and Privacy Policy. • This committee provides oversight for the security and privacy of SCFHS's Information on behalf of SCFHS and its management. • This committee provides oversight for security and protection of SCFHS's Information /technology assets on behalf of SCFHS and Management. • This Committee shall be a decision-making body with respect to any major change in the Data Protection and Privacy Policy. • This Committee is responsible for reviewing and approving this policy.
SCFHS Cybersecurity Executive Committee	• Review, assess and approve the Policy Exceptions (waiver) of the cybersecurity governing policies at SCFHS. • Periodic Review of the CS audit reports, and review of Security Incident Reports if and when required. • Reassess and re-approve the waiver once its allotted time-period is expired.
Governance and Compliance	• Ensure proper development, periodic review, update and communication of the Data Protection and Privacy Policy in coordination with Data Protection and Privacy Department and ensure alignment to leading industry standards, and compliance with laws, regulations, and organizational requirements. • Lead the implementation of the Data Protection and Privacy Policy and relevant procedures within SCFHS.

Role	Responsibility
	• Coordinate with different departments like Digital Technologies, etc. in order to make sure the Data Protection and Privacy Policy is in alignment with all other policy and procedures and controls implemented. • Conduct and track all the compliance checks covering the Data Protection and Privacy Policy related controls. • Coordinate with relevant stakeholders to ensure remediation of identified gaps within defined timeline. • Partner with Human Capital and drive the security awareness program, education and training related to the Data Protection and Privacy Policy and related do's and don'ts. • Provide reasonable assurance that the controls covered by the Data Protection and Privacy Policy are effective. • Develop procedures in compliance with this policy.
Data Protection and Privacy	• Perform Data Protection Impact assessment in support of identifying and minimize the data protection risks in current and new projects • Develop all Data Protection & Privacy requirements based on leading practices, international standards, and local regulatory frameworks, and cooperate with the supervisory authorities NDMO on Data Protection and Privacy requirements development or checks • Coordinate with SCFHS departments to gather and document specific requirements regarding data protection and privacy • Monitor the development, implementation and compliance in data management policies and procedures, such as data classification and labelling • Document the results of periodic data protection and privacy checks and share with relevant stakeholders • Provide consultation on encryption and cryptography mechanisms in order to support the implementation of data protection (in use, at rest and in fly)

Role	Responsibility
	• Document the results of troubleshooting of data protection incident and mitigation actions taken upon escalation, in collaboration with Cybersecurity Intelligence & Defence • Follow up with changes in laws and regulatory frameworks and collaborate with Governance and Compliance to ensure compliance of Privacy frameworks by providing new recommendations in policies and check activities • Maintain comprehensive records of all data processing activities conducted by the organization, including the purposes of all processing activities • Perform compliance monitoring against applicable legal Frameworks and, where appropriate, international best practice (e.g. Generally Accepted Privacy Principles). • Perform Data protection and Privacy Framework maintenance and enhancements. • Perform management, tracking and coordination of SCFHS Data Privacy risks and issues. • Handle personal data requests. • Handle Disclosure requests. • Evaluate and sign-off of significant change requests using of appropriate techniques (including privacy impact assessments and privacy threshold analysis) Data Protection and Privacy incident management. • Ensure appropriate agreements/obligations are in place for personal data flowing between the SCFHS and other parties (other Business Sector Areas and external parties). • Monitor data flows between the SCFHS and other parties (other Business Sector Areas and external parties). • Conduct data Privacy awareness sessions. • Develop procedures in compliance with this policy.
Monitoring and Response	• As part of regular activity, monitor all the data at rest or in fly throughout the SCFHS network and take required action for any suspicious activity.

Role	Responsibility
	• Develop procedures in compliance with this policy.
PMO\Project Owner	• Ensure all third-party contracts, which involve personal data processing are complied with this policy. • Ensure effective implementation of security controls and practices by third party to protect personal data. • Ensure all third parties sign an NDA before information sharing. • Develop procedures in compliance with this policy.
Business Sector Areas – Such as MOI Business Sector.	• Comply with this policy document. • Ensure timely notification delivery to data subject(s). • Develop procedures in compliance with this policy.
Security Architecture	• Support in identifying Security Architecture needs and requirements. • Enforce the implementation of the security requirements as per Reference Security Architecture. • Liaise with Risk Management Team to identify areas of risks and address them with new security requirements when applicable. • Develop procedures in compliance with this policy.
Third Parties	• Comply with this policy document as part of contractual obligation.
SCFHS Departments	• Ensure continuous compliance with this policy document. • Develop record retention procedures. • Ensure participation in the annual Data protection and training and awareness program. • Develop procedures in compliance with this policy.

5. Data Classification Framework



Data classification is a vital component of the data governance program, helping to maintain appropriate control and ensure the highest level of protection for SCFHS's data assets. The framework for data classification serves as a comprehensive model to be followed consistently across SCFHS as it defines the policy rules for the data classification lifecycle and breaks down the classification lifecycle into three distinct phases as outlined in the model:

Key Data-Loss Risks

One of the greatest challenges in managing data loss is that there are so many reasons why data loss can occur, numerous data loss scenarios to account for and many different controls that must be effective in order to manage the problem.
There is no simple solution or tool that can be implemented to address the variety of data loss risks that organizations face. In order to address the pervasive issue that data loss risks pose, a comprehensive solution that includes people, processes and technology needs to be implemented. Data loss can occur due to various reasons and can have severe consequences for businesses and individuals. Here are some key data-loss risks:

Hardware Failure: Hard drives, servers, and other storage devices can fail, leading to the loss of data. This can happen due to physical damage, power surges, or other hardware-related issues.

Software Corruption: Software errors, bugs, viruses, and malware can corrupt or erase data stored on computers or servers.

Accidental Deletion: Human error, such as accidentally deleting files or formatting drives, is a common cause of data loss.

Theft: Physical theft of devices such as laptops or mobile phones can lead to the loss of sensitive data.

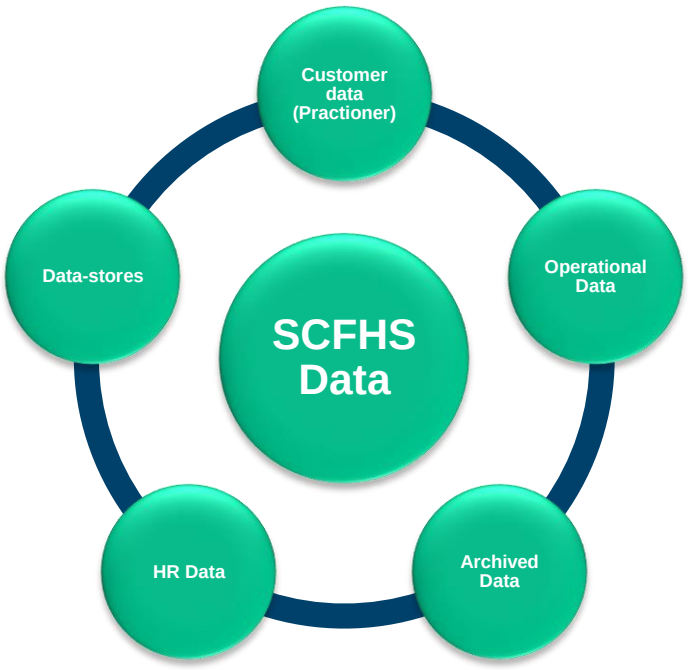
Natural Disasters: Natural disasters such as floods, fires, earthquakes, and hurricanes can damage hardware and destroy data stored on it.

Cyber Attacks: Cyber-attacks such as hacking, phishing, and ransomware can compromise data security and lead to the loss of data.

Insider Threats: Malicious insiders, such as employees or contractors, can intentionally delete or steal data.

Risks

- Loss or theft of laptops and mobile devices
- Unauthorized transfer of data to USB devices
- Improper categorization of sensitive data
- Data theft by employees or external parties
- Printing and copying of sensitive data
- Unintentional transmission of sensitive data



Consequence

- Brand damage and loss of reputation
- Loss of competitive advantage
- Loss of customers Loss of market share
- Erosion of shareholder value
- Regulatory fines
- Significant cost and effort to notify affected parties and recover from the breach

Data Protection Roles

1. **Data Owners**: The data owner in data protection roles is the individual or organization that has the responsibility for determining the purpose and means of processing personal data. In other words, the data owner is the entity that decides why and how personal data is collected, processed, stored, and shared. It's important to note that the data owner is not necessarily the same as the data controller or data processor. The data controller is the entity that determines the purposes and means of processing personal data, while the data processor is the entity that processes personal data on behalf of the data controller. However, in some cases, the data owner and the data controller may be the same entity. It all depends on the specific circumstances of the data processing activities and the applicable data protection laws and regulations. Some of these responsibilities include:

   - ✓ **Determining the purpose and scope of data collection**: As a data owner, they are responsible for determining the purpose and scope of data collection, and ensuring that it is lawful, fair and transparent.
   - ✓ **Ensuring data quality:** Data owners are responsible for ensuring that the data they collect is accurate, complete, and up to date. This means putting in place processes to maintain data quality and taking steps to correct any errors or inaccuracies in the data.
   - ✓ **Protecting data security:** You are responsible for protecting the security of the data you collect, including putting in place appropriate technical and organizational measures to prevent unauthorized access, loss, or damage to the data.
   - ✓ **Complying with data protection laws:** Data Owners are responsible for complying with all applicable data protection laws and regulations.
   - ✓ **Responding to data subject requests:** Data Owners must be prepared to respond to data subject requests for access, rectification, erasure, or restriction of processing, as well as requests to transfer data to another controller.

2. **Data Custodians:** A data custodian is responsible for the care, maintenance, and protection of data within an organization. In the context of data protection, the role of a data custodian is critical in ensuring that sensitive data is handled in compliance with applicable laws, regulations, and industry standards. The specific responsibilities of a data custodian may vary depending on the nature and scope of the organization's data holdings, but typically include the following:
   - ✓ **Data storage**: A data custodian is responsible for ensuring that data is stored in a secure and organized manner that protects it from unauthorized access, theft, loss, or corruption.
   - ✓ **Data access control:** A data custodian must implement appropriate access controls to ensure that only authorized individuals have access to sensitive data. This includes implementing user authentication and authorization mechanisms, as well as monitoring and auditing data access to detect and prevent unauthorized activity.

- ✓ **Data backup and recovery:** A data custodian is responsible for implementing appropriate backup and recovery procedures to ensure that data can be restored in the event of a disaster or other disruptive event.
- ✓ **Data retention and disposal:** A data custodian must ensure that data is retained for the appropriate length of time and disposed of securely when it is no longer needed.
- ✓ **Compliance monitoring**: A data custodian must monitor and report on compliance with applicable data protection laws, regulations, and industry standards, and take appropriate corrective action if necessary.

3. **Data users:** Data users are individuals or groups who have authorized access to data within an organization. In the context of data protection, data users have a critical role in ensuring that sensitive data is handled in compliance with applicable laws, regulations, and industry standards. The specific responsibilities of data users may vary depending on their roles and the nature of the organization's data holdings, but typically include the following:
   - ✓ **Data access:** Data users must access data only as authorized and must not exceed the permissions granted to them. They must also be aware of any restrictions on the use or disclosure of the data, such as data subject consent, contractual or legal obligations, and other privacy or security considerations.
   - ✓ **Data handling:** Data users must handle data carefully and responsibly, using appropriate security measures to protect it from unauthorized access, theft, loss, or corruption. This includes protecting the data while in use, storage, or transit, and ensuring that it is not shared or used improperly.
   - ✓ **Data accuracy:** Data users must ensure that the data they are working with is accurate, up-to-date, and relevant to the task at hand. They must also report any inaccuracies or discrepancies they detect, and take corrective action as needed.
   - ✓ **Data retention and disposal:** Data users must comply with the organization's policies and procedures for data retention and disposal, ensuring that data is retained for the appropriate length of time and disposed of securely when it is no longer needed.
   - ✓ **Compliance monitoring:** Data users must be aware of and comply with applicable data protection laws, regulations, and industry standards. They must report any suspected violations or breaches of data protection and cooperate with investigations and audits as needed.

Data Classification Schemes

This section determines the tiers of data and associated levels of protection and describes each level in terms that are meaningful to the organization.

	Extremely Confidential (EC)/ Very Confidential (VC)	Confidential (C)	Internal Use (I)	General/Public (G/P)
Description	Applies to information that is considered very sensitive and critical to SCFHS's ongoing operations	Applies to sensitive information that defines the way in which SCFHS operates. "Confidential - Third Party" is a subset of confidential information entrusted to/by another corporation under non-disclosure agreements and contracts.	Applies to information that is not approved for general circulation outside the organization.	Applies to information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone.
Legal & Regulatory Requirements	Protection of data is required by law and regulators.	Protection of data is required by business.	Protection of data is at the discretion of the Data Owner.	Protection of data is at the discretion of the Data Owner.
Reputation Risk	**Critical**	**High**	**Moderate**	**Low**
Business requirements	Data disclosure would seriously damage the organization if lost or made public. It would cause severe impact on organizational objectives.	Data disclosure would moderately impede or disrupt organization if shared internally or made public. Short term delay in achieving organization objectives.	Data disclosure would inconvenience the organization or management, but is unlikely to result in financial loss or serious damage to SCFHS's credibility / reputation	No possible damage to SCFHS.
Integrity Requirements	Prevent unauthorized changes. Software Integrity controls such hashing, checksum etc. should be put in place	Prevent unauthorized changes. Software Integrity controls such hashing, checksum etc. should be put in place	Apply IT-inherent completeness and accuracy assurance mechanisms. Prevent unauthorized changes.	No requirement.

	Authorization / Intervention of 2 or more people is required for any change / deletion (write access). Mandatory audits should be carried out on a regular basis to verify the write access of individuals / groups Establish traceability of authorized data modifications. Provide traceability with tamper-proof evidence.	Establish traceability of authorized data modifications.		
Availability Requirements	As per Business Impact Assessment (BIA) for Information Systems.	As per BIA for Information Systems.	As per BIA for Information Systems.	No requirement.
Data Access and Control	Access to named /designated individuals only on a need to know basis Enhanced security to computing environments (cryptography) Protected with data leakage prevention Techniques.	Access to named /designated individuals only on a need to know basis Enhanced security to computing environments (cryptography) Protected with data leakage prevention Techniques.	Role based Access control	Minimum Access restrictions and apply security best practices to computing environments
Audit Requirements	Periodic Application / System testing to maintain confidentiality. Periodic review of systems and procedures for potential misuse and/or	Periodic review of systems and procedures for potential misuse and/or unauthorized access.	Optional review of systems and procedures.	No audit controls required.

	unauthorized access. Data Owner/Customer would submit an annual report to Information Security outlining departmental security practices and training participation.			

Data Labelling Guidelines

This section gives instructions for labelling information (most commonly files and folders) in a way that makes it easy for users to visually determine the classification level of a document and enables automated tools, such as data loss prevention (DLP) systems, to programmatically identify sensitive documents and protect them accordingly.

Description	Applies to information that is considered very sensitive and critical to SCFHS's ongoing operations	Applies to sensitive information that defines the way in which SCFHS operates.	Applies to information that is not approved for general circulation outside the organization.	Applies to information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone.
Printed Documents	All printed documents should be labeled Labeling should be on the top of each document			Labelling not required.
Electronic Documents (Word, Excel, PowerPoint etc.)	All electronic documents should be labeled Labeling should be on the top of each document. All system generated reports should be labelled automatically based on data elements.			
Removable Media	All removable media should be labeled by pasting a tag.		Labelling not required.	Labelling not required.
Electronic Mail	E-mails should be labeled and label shall be on top of the body of the message. Highest classification rating between the message and attachment would be applicable to the electronic mail Label shall not be present in the subject field.			Labelling not required.
Electronic Data (Software, Databases etc.)	Label the classification rating as an attribute in database. Metadata tags should be utilized wherever applicable.			Labelling not required.
Scanned Documents	All scanned documents should be labelled automatically while scanning through authorized software.			
File Cover /Envelops / Media Cases	All file covers/ envelops / media cases should be labelled.		Labelling not required.	Labelling not required.

Data Handling Guidelines

This section provides specific requirements for protecting data according to its classification level. For each classification level, data handling guidelines define how data must be stored, transmitted and processed.

Description	Applies to information that is considered very sensitive and critical to SCFHS's ongoing operations	Applies to sensitive information that defines the way in which SCFHS operates.	Applies to information that is not approved for general circulation outside the organization.	Applies to information that has been declared public knowledge by someone with the authority to do so and can freely be given to anyone.
Marking	Labeling is must	Labeling is must	No Requirement	No Requirement
Filing and Media labels	Labeling is must	Labeling is must. The label on a file cover to be at least equal to the label on the most sensitive item in the file	No Requirement	No Requirement
Document Register (For Paper documents)	Maintain Document register Record should be kept of incoming and outgoing material All incoming documents must be placed without delay in an appropriate file cover	Maintain Document register (Optional)	No Requirement	No Requirement
Removal	Must be in personal custody of individual and kept in a locked container Removal must be authorized by the manager (or equivalent) responsible for the business unit that is custodian of the information A written record of removal must be maintained	Must be in personal custody of individual and when not in use kept in a locked container Removal must be authorized by the manager (or equivalent) responsible for the business unit that is custodian of the information	No need for authorization for removal Ensure adequate custodial arrangements, including overnight storage.	No Requirement

Auditing	Where a register is maintained, audits must be conducted at irregular intervals (spot checks) Personnel nominated to conduct spot checks are required to sight documents and acknowledge this in writing. This process should be carried out in conjunction with the custodian of the information / resource.	Spot checks (Optional)	No Requirement	No Requirement
Copying	May be prohibited by originator Authorization required for copying Same level of access control is required for copy To be kept to a minimum in keeping with operational requirements, each copy numbered.	May be prohibited by originator	To be kept to minimum in keeping with operational requirements	No Requirement
Physical Storage	Follow Clear desk' policy Hard copy and any form of unencrypted removable electronic media must be held in a locked container. Servers and associated devices processing or storing "Extremely	Follow Clear desk' policy Hard copy and any form of unencrypted removable electronic media must be held in a locked container. Servers and associated devices processing or storing "CONFIDENTIAL"	Follow Clear desk' policy Hard copy and any form of unencrypted removable electronic media must be held in a locked container. Servers and associated devices processing or storing "Internal Use" data must be sited in secure facilities (lock and key).	No Requirement

	Confidential / Very Confidential" data must be sited in secure facilities (lock and key).	data must be sited in secure facilities (lock and key).		
Mobile	Encryption is required. Remote wipe must be Enabled.	Encryption is required. Remote wipe (Optional)	No Requirement	No Requirement
Data at Rest	Must be encrypted by using an encryption method approved by Operational Information Security Department.	Must be encrypted.	No encryption Required.	No Requirement
Disposal	Paper Items: Shred using 2 axis shredder. Electronic data should follow sanitization process Authorization required before disposal For highly sensitive information implement dual control authorization	Paper Items: destroy by shedding Electronic data should follow sanitization process. (Life Cycle of Disposal and Reuse of Asset Policy) Authorization required before disposal	No requirement.	No Requirement
Printing	Should be printed only in designated printers and verify printer before printing. Person who sent the print should collect the document immediately.	Should be printed only in designated printers Person who sent the print should collect the document immediately.	May be printed on any printer.	No Requirement
Physical Mail	Single sealed opaque envelope that indicates the classification, receipt at	Single sealed opaque envelope that indicates the classification, receipt at	Single sealed opaque envelope that indicates the sensitivity label of the Information, delivered by SCFHS's internal	No Requirement

	discretion of originator AND: Either passed by hand between people who have the need to know Or placed in a locked container and delivered direct, by hand, by an authorized messenger May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between members of staff with the need to know and there is no opportunity for any unauthorized person to view the information. Double enveloping required AND receipt required AND: Either placed in a locked container or delivered direct by an authorized messenger. Or delivered by an approved overnight courier Electronic media (example: backup tapes) should be placed in locked contained and delivered.	discretion of originator AND: Either passed by hand between people who have the need to know Or placed in a locked container and delivered direct, by hand, by an authorized messenger May be passed, uncovered, by hand within a discrete office environment provided it is transferred directly between members of staff with the need to know and there is no opportunity for any unauthorized person to view the information. Either single opaque envelope that does not give any indication of the classification AND placed in a locked container and delivered direct, by hand, by an authorized messenger AND receipt required; Or double enveloping AND receipt required AND delivered by an approved overnight courier.	mail system (or provider) May be passed, uncovered, by hand within a secure area provided it is transferred directly between people with the need to know and there is no opportunity for any unauthorized person to view the Information.	
Electronic Transmission	Must apply encryption for emails and un-trusted networks	Must apply Standard encryption for	Infrequent transmissions may be made without special controls	No Requirement

	using encryption methods approved by Operational Information Security Department. Verify each recipient before sending emails. Unsecure Protocols Prohibited. 1. RSA 2048 bits (or equivalent) 2. AES 256-bits (or equivalent)	emails or un-trusted networks. Unsecure Protocol should not be used. 1. RSA 2048 bits (or equivalent) 2. AES 256-bits (or equivalent)	Regular or frequent traffic must be encrypted (Optional).	
Websites	Posting to intranet sites is Prohibited unless it is preapproved. Posting to internet sites is prohibited.	Posting to publicly accessible Internet sites is Prohibited.	Posting to publicly accessible Internet sites is Prohibited.	No Requirement.
Usage of Cloud Drives	Strictly prohibited.	Strictly Prohibited.	Temporary storage allowed.	No Requirement.

Data Classification Mapping

This section explains what types of data are considered sensitive and are useful in both providing guidance to the support teams that manage data protection technical controls and providing guidance to the users that work with the relevant information.

Data Class	Classified Data Elements	EC/ VC	C	I	G/P
Personnel Data	Compensation and Benefits				
	Position Management				
	Staff Promotion Data				
Customer Data	Students Data, Job seekers, Practioners				
	Filled Forms (Professional Registration, Trainings etc)				
Strategic or Operational Financial Data	Financial Reports				
	Financial Regulatory Reporting				
	Audit Reports				
	Bank Account Information				
	Fixed Assets Inventory				
Legal Data	Compliance Related Report / Data / Dashboards				
IT Data	Username & Password Pairs				
	Public Key Infrastructure (PKI) Cryptographic Keys (public & private)				
	Hardware or Software Tokens (multifactor authentication)				
	Internal IP Addresses				
	Privileged Account Usernames				
	Inventory lists				
	Configuration files				
	DB Dumps				
	Source Code				
	Binary Code				
Archived Data	Scanned documents				
Sales and Marketing Data	Business Plans				
	Branch Floor plans (Designs)				
	Marketing Designs				
	News Releases				
Operational and Risk related data	Risk Reports				
	Risk Analytics				
	Risk Dashboards				
	Policies , Procedures & Awareness Material				

6. Data Management and Personal Data Protection Standards-NDMO

The National Data Management Office (NDMO) in Saudi Arabia is a government entity responsible for managing and governing the country's data resources. It was established in 2019 to lead the implementation of the Saudi Data and AI Authority (SDAIA) strategy, which aims to promote the use of data and artificial intelligence (AI) in the country.

The NDMO's mandate includes developing policies and regulations for data management and protection, promoting data sharing across government entities, and ensuring that data is used effectively and efficiently to support decision-making and innovation. It also oversees the implementation of data management practices and provides guidance and support to government entities to help them improve their data management capabilities.

The NDMO works closely with other government entities and private sector organizations to promote the development of a strong and sustainable data ecosystem in Saudi Arabia. Its vision is to establish Saudi Arabia as a global leader in data and AI, and to leverage these technologies to drive economic growth, social development, and national transformation.
Below are some elements of the data privacy framework provided by the National Data Management Office.

1. **Data Protection Principles:** The framework outlines data protection principles that provide the foundation for data privacy practices. These principles include ensuring transparency, obtaining consent, limiting data collection, ensuring accuracy, and providing security measures. Below are some of the principles set forth:
    - **Transparency**: The principle of transparency requires that data subjects be informed of the purpose and scope of data processing activities. SCFHS must provide clear and concise information to data subjects about the collection, use, and disclosure of their personal data.
    - **Consent**: The principle of consent requires that data subjects provide their explicit and informed consent for the processing of their personal data. SCFHS must obtain consent from data subjects before collecting, using, or disclosing their personal data, except in limited circumstances where consent is not required by law.
    - **Data Minimization**: The principle of data minimization requires that SCFHS collect only the personal data that is necessary for the purposes for which it is processed. Data should be limited to what is necessary, relevant, and proportionate to achieve the purposes for which it is collected.
    - **Accuracy**: The principle of accuracy requires that SCFHS take reasonable steps to ensure that personal data is accurate, complete, and up to date. Data subjects have the right to request corrections to their personal data if it is inaccurate or incomplete.
    - **Security:** The principle of security requires that SCFHS implement appropriate technical and organizational measures to protect personal data from unauthorized access, use, or disclosure. Measures should be implemented to ensure confidentiality, integrity, and availability of personal data.
    - **Retention**: The principle of retention requires that SCFHS retain personal data only for as long as it is necessary to fulfil the purposes for which it was collected. Once the retention period has expired, data should be securely deleted or destroyed.
    - **Accountability**: The principle of accountability requires that SCFHS be responsible and accountable for their data protection practices. This includes having policies and procedures in place to ensure compliance with data protection

laws and regulations, as well as conducting regular audits and assessments to identify and address risks to data protection.

2. **Data Privacy Laws and Regulations:** The framework provides an overview of the data privacy laws and regulations such as the Personal Data Protection Law and the Electronic Transactions Law. It also outlines the penalties for non-compliance with these laws and regulations.

3. **Privacy Impact Assessments (PIA):** The framework includes guidelines for conducting Privacy Impact Assessments (PIAs) to evaluate the privacy risks associated with the collection, use, and disclosure of personal data. PIAs are required for new projects or initiatives that involve the processing of personal data. The key elements of the PIA process as per the NDMO guidelines include:
   - **Identify the Purpose and Scope**: The PIA process begins by identifying the purpose and scope of the data processing activity. This includes defining the types of personal data that will be collected, the methods of collection, and the intended use of the data.
   - **Identify Privacy Risks**: The next step is to identify the privacy risks associated with the data processing activity. This includes assessing the potential impact on data subjects, such as the risk of unauthorized access, use, or disclosure of personal data.
   - **Evaluate Privacy Impact**: The privacy impact evaluation involves analyzing the identified privacy risks and assessing their potential impact on data subjects. This includes considering the nature and sensitivity of the personal data, the potential consequences of a privacy breach, and the likelihood of a privacy breach occurring.
   - **Identify Mitigation Measures**: The next step is to identify mitigation measures to address the privacy risks identified in the previous step. This includes considering technical and organizational measures to reduce the likelihood of a privacy breach, such as access controls, encryption, and data anonymization.
   - **Assess Effectiveness of Mitigation Measures**: The effectiveness of the identified mitigation measures is evaluated to determine if they are sufficient to mitigate the identified privacy risks.
   - **Document and Review**: The final step in the PIA process is to document the assessment and review it periodically to ensure that it remains accurate and up to date.
4. **Data Subject Rights:** The framework outlines the data subject rights in Saudi Arabia, such as the right to access, rectify, and delete personal data. It also includes guidelines for handling data subject requests and complaints.

5. **Data Privacy Training and Awareness:** The framework emphasizes the importance of data privacy training and awareness for government employees and stakeholders. It includes guidelines for providing training and awareness programs to promote a culture of privacy across government entities. The following are some key recommendations by NDMO for data privacy training and awareness:

- **Establish a Privacy Awareness Program**: SCFHS should establish a privacy awareness program to provide employees with training and guidance on data privacy policies, procedures, and best practices. The program should be regularly reviewed and updated to ensure that it remains relevant and effective.
- **Identify Training Needs**: SCFHS should identify the training needs of their employees based on their job functions and the sensitivity of the data they handle. For example, employees who handle sensitive personal information may require additional training on data protection and privacy regulations.
- **Develop Training Materials**: SCFHS should develop training materials that are relevant, engaging, and easy to understand. These materials can include videos, e-learning modules, quizzes, and practical exercises.
- **Conduct Regular Training Sessions**: Organizations should conduct regular training sessions to ensure that employees are aware of the latest privacy policies and best practices. The training sessions can be conducted in-person or online, and should be mandatory for all employees.
- **Monitor and Evaluate Training Effectiveness**: SCFHS should monitor and evaluate the effectiveness of their privacy awareness program regularly. This can be done through employee feedback, assessments, and audits.
- **Reinforce Privacy Culture**: SCFHS should reinforce a culture of privacy within the workplace by promoting best practices, encouraging employee feedback and reporting of privacy incidents, and recognizing and rewarding good privacy behaviour

6. **Data Privacy Governance and Accountability:** The framework emphasizes the importance of governance and accountability for data privacy practices. It includes guidelines for establishing data privacy governance structures and ensuring accountability for data privacy practices across government entities. The following are some key recommendations by NDMO for data privacy governance and accountability:
   - **Establish a Data Privacy Governance Framework**: SCFHS should establish a governance framework to manage data privacy risks and ensure compliance with data protection regulations. The framework should define roles and responsibilities, establish policies and procedures, and set up accountability mechanisms.
   - **Appoint a Data Protection Officer**: SCFHS should appoint a Data Protection Officer (DPO) to oversee the implementation of the privacy governance framework and ensure compliance with data protection regulations. The DPO should be a senior member of the SCFHS with expertise in data privacy and security.
   - **Conduct Privacy Impact Assessments (PIAs):** SCFHS should conduct Privacy Impact Assessments (PIAs) to identify and assess the privacy risks associated with their data processing activities. The results of the PIAs should be used to inform the development of privacy policies and procedures.
   - **Develop Privacy Policies and Procedures**: SCFHS should develop privacy policies and procedures that are consistent with data protection regulations and best practices. The policies and procedures should be regularly reviewed and

updated to reflect changes in the regulatory environment and the organization's data processing activities.

- **Implement Privacy by Design**: SCFHS should implement Privacy by Design (PbD) principles into their data processing activities. PbD involves integrating privacy considerations into the design and development of products and services, rather than adding them as an afterthought.
- **Monitor and Report Privacy Incidents**: SCFHS should establish mechanisms for monitoring and reporting privacy incidents. Privacy incidents should be reported to the DPO, who should take appropriate action to mitigate the impact of the incident and prevent future occurrences.
- **Conduct Privacy Audits**: SCFHS should conduct regular privacy audits to ensure that their privacy policies and procedures are being followed, and that privacy risks are being effectively managed.

7. **Data Security Measures**: The framework provides guidelines for implementing appropriate data security measures to protect personal and sensitive data from unauthorized access, use, and disclosure. It includes guidelines for securing data at rest and in transit, implementing access controls and authentication measures, and conducting regular security assessments.
   - **Implement Access Controls**: SCFHS should implement access controls to restrict access to sensitive data to authorized personnel only. Access controls can include passwords, two-factor authentication, and biometric authentication.
   - **Encrypt Data**: SCFHS should encrypt sensitive data to protect it from unauthorized access. Encryption can be used for data at rest and in transit.
   - **Implement Network Security**: SCFHS should implement network security measures such as firewalls, intrusion detection and prevention systems, and network segmentation to prevent unauthorized access to their networks.
   - **Implement Endpoint Security**: SCFHS should implement endpoint security measures such as anti-virus and anti-malware software, and host-based intrusion detection and prevention systems to protect their endpoints from cyber-attacks.
   - **Conduct Regular Vulnerability Assessments**: SCFHS should conduct regular vulnerability assessments to identify and address vulnerabilities in their IT systems and networks.
   - **Implement Data Backup and Recovery Procedures**: SCFHS should implement data backup and recovery procedures to ensure that critical data can be recovered in the event of a data breach or cyber-attack.
   - **Train Employees on Cybersecurity**: SCFHS should provide regular cybersecurity training to their employees to raise awareness of cyber threats and best practices for data security.
   - **Implement Incident Response Procedures**: SCFHS should implement incident response procedures to ensure that they can respond effectively to cyber incidents and minimize the impact of data breaches.

8. **Data Breach Notification**: The framework outlines the requirements for data breach notification in Saudi Arabia. It includes guidelines for reporting data breaches to the relevant authorities and affected data subjects, as well as measures for mitigating the

impact of the breach. The following are some key recommendations by NDMO for data breach notification:

- **Develop a Data Breach Response Plan**: SCFHS should develop a data breach response plan that outlines the steps to be taken in the event of a data breach. The plan should include procedures for identifying, containing, and mitigating the effects of the breach.
- **Determine the Scope of the Breach:** SCFHS should determine the scope of the breach, including the type of data that was compromised, the number of individuals affected, and the potential harm to individuals.
- **Notify Affected Individuals**: SCFHS should notify affected individuals as soon as possible after a data breach. The notification should include a description of the breach, the type of data that was compromised, and the steps the organization is taking to mitigate the effects of the breach.
- **Notify Regulatory Authorities**: SCFHS should notify regulatory authorities as required by law. SCFHS is required to notify the Communications and Information Technology Commission (CITC) of any data breaches that involve personal data.
- **Notify Third Parties**: SCFHS should notify any third parties that may be affected by the data breach, such as vendors, partners, or service providers.
- **Conduct a Post-Incident Review**: SCFHS should conduct a post-incident review to identify the cause of the breach, assess the effectiveness of the organization's response, and identify areas for improvement.

9. **International Data Transfers:** The framework provides guidelines for transferring personal data outside of Saudi Arabia, including the use of standard contractual clauses, binding corporate rules, and other measures to ensure adequate data protection. The following are some key recommendations by NDMO for international data transfers:
   - **Identify the Purpose of the Data Transfer**: SCFHS should identify the purpose of the data transfer and ensure that it is necessary for the performance of a contract or the provision of a service.
   - **Obtain Consent from Data Subjects**: SCFHS should obtain the explicit consent of data subjects before transferring their personal data outside of Saudi Arabia. The consent should be informed and specific, and data subjects should be informed of the risks associated with the transfer.
   - **Implement Appropriate Safeguards:** SCFHS should implement appropriate safeguards to protect personal data when it is transferred outside of Saudi Arabia. Safeguards can include encryption, anonymization, and contractual clauses that require the recipient to provide a level of data protection that is equivalent to that provided in Saudi Arabia.
   - **Conduct a Risk Assessment:** SCFHS should conduct a risk assessment to identify and assess the risks associated with the transfer of personal data outside of Saudi Arabia. The assessment should consider the nature of the data, the destination country, and the measures in place to protect the data.
   - **Maintain Records:** SCFHS should maintain records of all international data transfers, including the purpose of the transfer, the type of data transferred, and the measures in place to protect the data.

- **Notify Regulatory Authorities:** SCFHS should notify regulatory authorities if required by law. SCFHS is required to notify the Communications and Information Technology Commission (CITC) of any international data transfers that involve personal data.

10. **Data Privacy Compliance Monitoring and Enforcement**: The framework emphasizes the importance of monitoring and enforcing data privacy compliance across government entities. It includes guidelines for conducting audits, inspections, and investigations to ensure compliance with data privacy laws and regulations. It also outlines the penalties for non-compliance and measures for remediation and enforcement. The following are some key recommendations by NDMO for data privacy compliance monitoring and enforcement:
    - **Designate a Data Protection Officer**: SCFHS should designate a Data Protection Officer (DPO) to oversee data privacy compliance. The DPO should have expertise in data protection laws and regulations, and be responsible for ensuring that the organization is compliant with data privacy laws and regulations.
    - **Develop Compliance Policies and Procedures**: SCFHS should develop and implement compliance policies and procedures that are consistent with data privacy laws and regulations in Saudi Arabia. Policies and procedures should cover data collection, storage, use, and disclosure, and include processes for monitoring compliance and reporting breaches.
    - **Conduct Regular Risk Assessments**: SCFHS should conduct regular risk assessments to identify and assess risks to the security and privacy of personal data. Risk assessments should be conducted on a regular basis, and should consider the nature and sensitivity of the data, as well as the potential harm to individuals in the event of a breach.
    - **Implement Controls to Mitigate Risks:** SCFHS should implement controls to mitigate risks identified during risk assessments. Controls can include technical controls, such as encryption and access controls, as well as administrative controls, such as training and awareness programs.
    - **Conduct Regular Audits and Assessments:** SCFHS should conduct regular audits and assessments to ensure that their data privacy compliance policies and procedures are being followed. Audits and assessments can be conducted internally or by a third-party auditor.
    - **Enforce Compliance:** SCFHS should enforce compliance with data privacy policies and procedures through disciplinary actions, such as termination or suspension of employment, as well as legal actions, such as civil or criminal penalties.

11. **Data Protection Officer (DPO):** The framework provides guidelines for appointing a Data Protection Officer (DPO) in government entities to oversee data privacy practices and ensure compliance with data protection laws and regulations.

12. **Data Sharing and Processing Agreements:** The framework includes guidelines for entering into data sharing and processing agreements with third-party service

providers or other government entities. It outlines the requirements for ensuring adequate data protection and privacy in these agreements.

13. **Data Retention and Disposal:** The framework includes guidelines for retaining and disposing of personal data in accordance with national and international data privacy standards. It includes measures for securely disposing of data when it is no longer needed for its intended purpose. The following are some key recommendations by NDMO for data retention and disposal:
    - **Identify the Purpose of Data Retention**: SCFHS should identify the purpose of retaining personal data and ensure that it is necessary for the performance of a contract or the provision of a service. Personal data that is no longer required should be disposed of securely.
    - **Define Retention Periods**: SCFHS should define retention periods for different types of personal data. Retention periods should be based on legal requirements, business needs, and the purpose of the data retention.
    - **Secure Data During Retention Period:** SCFHS should implement appropriate security measures to protect personal data during the retention period. This can include physical security measures, such as locked cabinets and access controls, as well as technical security measures, such as encryption and access controls.
    - **Disposal of Data:** SCFHS should dispose of personal data securely once the retention period has expired. Disposal methods can include shredding, deletion, or other secure methods that ensure the data cannot be recovered.
    - **Develop a Data Retention and Disposal Policy:** SCFHS should develop and implement a data retention and disposal policy that outlines the SCFHS's approach to data retention and disposal. The policy should include retention periods, disposal methods, and security measures, as well as procedures for monitoring and enforcing compliance with the policy.
    - **Maintain Records:** SCFHS should maintain records of all data retention and disposal activities, including the type of data retained, the retention period, and the method of disposal.

14. **Cross-Border Data Requests**: The framework provides guidelines for responding to cross-border data requests from foreign governments or law enforcement agencies. It includes measures for ensuring compliance with national and international data privacy laws and regulations in these requests. The following are some key recommendations by NDMO for cross-border data requests:
    - **Understand Legal Requirements**: SCFHS should understand the legal requirements for cross-border data transfers under both Saudi Arabian and foreign laws. This includes understanding the legal basis for data transfers, the data protection laws and regulations of the foreign country, and any additional contractual or other requirements that may apply.
    - **Evaluate Risks:** SCFHS should evaluate the risks associated with cross-border data transfers, including the risk of unauthorized access, use, or disclosure of personal data, and the risk of non-compliance with data privacy regulations. Risks should be evaluated on a case-by-case basis, taking into account the nature of the

data, the purpose of the transfer, and the country to which the data is being transferred.

- **Obtain Consent:** SCFHS should obtain the consent of individuals before transferring their personal data across borders, unless the transfer is necessary for the performance of a contract or the provision of a service. Consent should be obtained in accordance with data privacy regulations, and individuals should be informed of the purpose of the transfer and the countries to which the data will be transferred.
- **Implement Adequate Safeguards**: SCFHS should implement adequate safeguards to protect personal data during cross-border transfers. This can include technical measures, such as encryption and access controls, as well as contractual measures, such as data transfer agreements and binding corporate rules.
- **Maintain Records:** SCFHS should maintain records of all cross-border data transfers, including the type of data transferred, the purpose of the transfer, and the countries to which the data was transferred.

15. **Continuous Improvement:** The framework emphasizes the importance of continuous improvement in data privacy practices across government entities. It includes guidelines for conducting regular assessments and reviews to identify areas for improvement and implementing measures to enhance data privacy practices.

Data Classification Framework Components

1. **Data Classification Policy:** This component outlines the principles and guidelines that organizations should follow when classifying their data. It provides a set of criteria that can be used to determine the sensitivity and value of different types of data, and it defines the different levels of classification that can be used to categorize data.

2. **Data Classification Process:** This component outlines the steps that organizations should follow when classifying their data. It provides a set of procedures and guidelines that can be used to ensure that data is classified consistently and accurately across the organization.

3. **Data Classification Tools:** This component provides a set of tools and resources that organizations can use to support their data classification efforts. These tools include classification templates, training materials, and other resources that can help organizations implement the framework effectively

Data Classification Policy

The National Data Management Office (NDMO) has developed a Data Classification Policy to help organizations classify their data based on sensitivity and value. The policy provides guidelines and criteria that organizations should follow when classifying their data, and it defines different levels of classification that can be used to categorize data. The following are the key components of the NDMO's Data Classification Policy:

1. **Definition of Data Classification**: The policy provides a definition of data classification, which is the process of categorizing data based on its sensitivity and value. The policy states that data classification is essential for ensuring that data is managed and protected appropriately.

2. **Data Classification Levels**: The policy defines different levels of data classification that organizations can use to categorize their data. These levels include:

    - Level 1: Public Data - This level includes data that is not sensitive and can be made available to the public without any restrictions.
    - Level 2: Confidential Data - This level includes data that is not sensitive but should be restricted to internal use within the organization.
    - Level 3: Secret Data - This level includes data that is sensitive and should be protected from unauthorized access.
    - Level 4: Top Secret Data - This level includes data that is highly sensitive and requires strict access controls and protections.
3. **Data Sensitivity Criteria**: The policy provides a set of criteria that organizations can use to determine the sensitivity of their data. These criteria include the potential harm that could result from unauthorized access or disclosure of the data, the confidentiality of the data, and the legal or regulatory requirements that apply to the data.

4. **Data Handling Procedures**: The policy outlines the procedures that organizations should follow when handling data at different levels of classification. These procedures include access controls, data retention and disposal, and data sharing and transfer.

5. **Responsibilities and Accountability**: The policy defines the roles and responsibilities of different stakeholders in the data classification process. It also outlines the accountability framework that organizations should follow to ensure that data is classified and handled appropriately.

Data Classification Process

The National Data Management Office (NDMO) has developed a Data Classification Process to help organizations classify their data based on sensitivity and value. The process provides a set of procedures and guidelines that organizations should follow to ensure that data is classified consistently and accurately across the organization.
The following are the key components of the NDMO's Data Classification Process:

1. **Identify Data**: The first step in the data classification process is to identify the data that needs to be classified. This includes all data that is processed, stored, or transmitted by the organization.

2. **Determine Data Sensitivity**: The next step is to determine the sensitivity of the data based on the criteria outlined in the Data Classification Policy. This involves assessing the potential harm that could result from unauthorized access or disclosure of the data, the confidentiality of the data, and the legal or regulatory requirements that apply to the data.

3. **Assign Classification Level**: Once the sensitivity of the data has been determined, the organization should assign a classification level to the data. This involves using the levels defined in the Data Classification Policy to categorize the data based on its sensitivity and value.

4. **Apply Handling Procedures**: Once the data has been classified, the organization should apply the appropriate handling procedures based on the classification level. This includes access controls, data retention and disposal, and data sharing and transfer.

5. **Review and Update**: The data classification process is an ongoing process, and organizations should review and update their data classification regularly to ensure that it remains accurate and up-to-date. This includes assessing changes in the sensitivity of the data, as well as changes in legal or regulatory requirements.

Overall, the NDMO's Data Classification Process provides a clear and structured approach for organizations to classify their data based on sensitivity and value. By following the process's procedures and guidelines, organizations can ensure that their data is classified consistently and accurately, and that it is managed and protected appropriately.

Data Classification Tools

The National Data Management Office (NDMO) does not specify any particular data classification tools that organizations should use to classify their data. However, the NDMO's Data Classification Policy and Process provide a framework and guidelines for organizations to follow when classifying their data based on sensitivity and value.

Organizations can use a variety of tools and techniques to classify their data, depending on their needs and resources. Some of the commonly used data classification tools include:

1. **Data Discovery and Classification Tools:** These tools can automatically scan an organization's data repositories and classify data based on predefined rules and policies. Some examples of data discovery and classification tools are Microsoft Information Protection, Symantec Data Loss Prevention, and IBM Guardium.

2. **Data Labelling Tools:** These tools allow organizations to apply labels or tags to their data to indicate its classification level. These labels can be used to enforce

access controls and apply handling procedures. Examples of data labelling tools are Azure Information Protection, Google Cloud Data Loss Prevention, and McAfee Data Protection.

3. **Data Classification Workshops**: These workshops involve bringing together key stakeholders in the organization to classify data based on its sensitivity and value. This can be a collaborative and effective way to classify data that may not be easily classified using automated tools.

4. **Manual Classification**: Organizations can also classify their data manually by reviewing each data item and determining its sensitivity based on the criteria outlined in the Data Classification Policy.

Overall, the choice of data classification tools and techniques will depend on the SCFHS needs and resources. However, by following the guidelines and criteria outlined in the NDMO's Data Classification Policy and Process, organizations can ensure that their data is classified consistently and accurately, and that it is managed and protected appropriately.

7. National Center for archives and records NCAR guidelines

The National Center for Archives and Records (NCAR) in Saudi Arabia has developed a comprehensive framework for managing archives and records in the country. The framework is known as the Saudi National Archives and Records Management (NARM) Framework, and it consists some of the key policies:

1. **Records Management Policy**: This policy provides guidelines for the management of records throughout their lifecycle, from creation to disposal. It covers topics such as records creation, retention, access, preservation, and disposal, as well as standards for metadata, formats, and storage.
2. **Electronic Records Management Policy**: This policy specifically addresses the management of electronic records, including guidelines for their creation, retention, and preservation. It also includes standards for electronic records formats, metadata, and storage.
3. **Access to Records Policy:** This policy outlines the procedures for accessing records held by government agencies and other organizations in Saudi Arabia. It covers topics such as access requests, fees, and exemptions.
4. **Privacy Policy:** This policy addresses the protection of personal information contained in records held by government agencies and other organizations in Saudi Arabia. It includes guidelines for the collection, use, and disclosure of personal information.

5. **Digital Preservation Policy**: This policy outlines the procedures for preserving digital records held by government agencies and other organizations in Saudi Arabia. It covers topics such as data migration, file formats, and metadata standards.
6. **Disaster Recovery and Business Continuity Policy:** This policy provides guidelines for the management of records in the event of a disaster, such as a fire or flood. It covers topics such as backup procedures, emergency response plans, and recovery strategies.

These policies are designed to ensure that records are managed effectively and in accordance with established standards and best practices. They are an important component of the NARM Framework and provide guidance for government agencies and other organizations in Saudi Arabia that are responsible for managing archives and records.

Records Management Policy

The Records Management Policy developed by the National Center for Archives and Records (NCAR) in Saudi Arabia is a key component of the National Archives and Records Management (NARM) Framework. The policy provides guidelines for the management of records throughout their lifecycle, from creation to disposal, and is designed to ensure that records are managed effectively and in accordance with established standards and best practices. Here are some of the key details of the policy:

Record Classification: SCFHS must classify their records based on their importance, sensitivity, and value and as per guidelines set forth by NDMO.

Records Retention: SCFHS must establish retention schedules for their records based on legal, regulatory, and business requirements. The retention schedules must define the timeframes for retaining records and their eventual disposition, whether through destruction, transfer to NCAR or transfer to an archival institution.

Access and Security: SCFHS must ensure that records are accessed only by authorized personnel and that security measures are in place to protect records from unauthorized access, loss, or damage. Access to records should be granted based on a need-to-know basis and appropriate security controls should be implemented to safeguard against unauthorized access or disclosure.

Records Storage: SCFHS must ensure that records are stored in a secure and organized manner.

Records Disposition: SCFHS must establish policies and procedures for the disposal of records. Disposition must be carried out in accordance with retention schedules and legal and regulatory requirements.

Records Management Training: Organizations must provide training and awareness programs to personnel who handle records, including training on record classification, retention, access, and security, and records disposition.

Electronic Records Management Policy

An organization needs to follow several policies for Electronic Records Management (ERM) as per National Center for Archives and Records (NCAR) in Saudi Arabia. These policies include:

Electronic Record Classification: SCFHS must classify their electronic records based on their importance, sensitivity, and value. The NCAR provides guidelines for electronic record classification based on Saudi Arabia's laws, regulations, and cultural values.

Electronic Record Retention: SCFHS must establish retention schedules for their electronic records based on legal, regulatory, and business requirements. The retention schedules must define the timeframes for retaining electronic records and their eventual disposition, whether through destruction, transfer to NCAR or transfer to an archival institution.

Access and Security: Organizations must ensure that electronic records are accessed only by authorized personnel and that security measures are in place to protect electronic records from unauthorized access, loss, or damage. Access to electronic records should be granted based on a need-to-know basis and appropriate security controls should be implemented to safeguard against unauthorized access or disclosure.

Electronic Record Storage: SCFHS must ensure that electronic records are stored in a secure and organized manner.

Electronic Record Disposition: SCFHS must establish policies and procedures for the disposal of electronic records. Disposition must be carried out in accordance with retention schedules and legal and regulatory requirements. The NCAR provides guidelines on electronic records disposition, including secure deletion, transfer to NCAR, or transfer to an archival institution.

ERM Training: Organizations must provide training and awareness programs to personnel who handle electronic records, including training on electronic record classification, retention, access, and security, and electronic record disposition.

Access to records policy

Authorized Access: Access to records should be restricted to authorized personnel only. The organization should define roles and responsibilities for personnel who are authorized to access records and establish procedures for granting and revoking access privileges.

Security Controls: Access to records should be protected through appropriate security controls, such as access controls, authentication, and encryption. The organization should also establish procedures for monitoring and auditing access to records to ensure that unauthorized access attempts are detected and reported.

Retention and Disposition: Access to records should be governed by retention and disposition policies that specify how long records should be retained and when they should be disposed of. Access to records should be provided only for authorized purposes and for the duration of the authorized use.

Privacy and Confidentiality: Access to records should be governed by policies that protect the privacy and confidentiality of personal and sensitive information. This includes ensuring that access to records containing personal or sensitive information is restricted to authorized personnel only, and that appropriate measures are in place to protect the confidentiality and integrity of the information.

Record Requests: Access to records should be provided in response to authorized requests in a timely and efficient manner. The organization should establish procedures for handling record requests, including the documentation and tracking of requests, the verification of requestor identity, and the provision of records in the appropriate format.

Privacy Policy

Collection of Personal Information: The organization should only collect personal information that is necessary for its operations and services. The organization should also obtain consent from individuals before collecting, using, or disclosing their personal information.

Use and Disclosure of Personal Information: The organization should only use and disclose personal information for the purposes for which it was collected, unless the individual has provided consent or the use or disclosure is otherwise authorized by law.

Security of Personal Information: The organization should take appropriate measures to protect personal information from unauthorized access, use, or disclosure. This includes implementing physical, technical, and administrative security measures to safeguard personal information.

Retention and Disposal of Personal Information: The organization should establish policies and procedures for the retention and disposal of personal information. Personal

information should be retained only as long as necessary for the purposes for which it was collected, and disposed of securely when it is no longer needed.

Access and Correction of Personal Information: The organization should provide individuals with access to their personal information and the ability to correct or update their personal information if it is inaccurate or incomplete.

Accountability: The organization should be accountable for its management of personal information and should have policies and procedures in place to ensure compliance with privacy laws and regulations.

Digital Preservation Policy

Selection: SCFHS must identify and select digital records that are of long-term value and should be preserved.

Acquisition: SCFHS must ensure that digital records are acquired in a manner that maintains their authenticity, reliability, and integrity.

Access and Use: SCFHS must ensure that digital records are accessible and usable over time by managing their technical dependencies, providing adequate metadata, and using open standards.

Preservation Planning: SCFHS must develop a preservation plan that identifies the technical, resource, and organizational requirements for preserving digital records.

Storage and Backup: SCFHS must ensure that digital records are stored in a secure and reliable manner and that backups are taken regularly to prevent loss.

Monitoring and Maintenance: SCFHS must monitor the condition of digital records to ensure their ongoing accessibility, accuracy, and authenticity.

Migration: SCFHS must plan for the eventual migration of digital records to new formats or systems as technology evolves.

Disposal: SCFHS must dispose of digital records in a secure and responsible manner that takes into account legal and regulatory requirements.

Guidelines for record classification as per NCAR

The National Center for Archives and Records (NCAR) provides guidelines for record classification that organizations should follow:

1. **Identify the purpose of the record**: SCFHS should identify the purpose of the record to determine its classification level.

2. **Determine the sensitivity of the record**: Records that contain sensitive information should be classified at a higher level.
3. **Classify the record**: Once the purpose and sensitivity of the record have been determined, it should be classified according to the NCAR's classification system or the applicable regulatory framework.
4. **Label the record**: Each record should be labelled with its classification level to ensure that it is properly managed and protected.
5. **Apply appropriate security measures**: SCFHS should apply appropriate security measures to protect records classified at higher levels.
6. **Regularly review and update record classifications**: Record classifications should be reviewed and updated regularly to ensure that they are still appropriate and accurate.

Guidelines for electronic record classification as per NCAR

The National Center for Archives and Records (NCAR) in Saudi Arabia provides guidelines for electronic record classification that organizations can follow. Some of the key guidelines are:

1. **Classify records based on their content**: SCFHS should classify electronic records based on their content, using a classification scheme that is aligned with the organization's business functions and activities.
2. **Assign metadata to records**: Metadata should be assigned to electronic records to provide context and aid in their classification, retrieval, and management. Metadata should include information such as the record's title, creator, creation date, and retention period.
3. **Use a consistent naming convention**: Electronic records should be named in a consistent and meaningful way, to make it easy to identify and retrieve them.
4. **Implement access controls**: Access controls should be implemented to ensure that electronic records are only accessible to authorized individuals who have a legitimate need to access them.
5. **Ensure security of electronic records**: Electronic records should be stored in a secure manner, with appropriate safeguards in place to protect against unauthorized access, loss, or corruption.
6. **Regularly review and update record classifications**: Electronic record classifications should be regularly reviewed and updated to ensure that they remain accurate and reflect changes in the organization's business functions and activities.

Guidelines for electronic record storage as per NCAR

The National Center for Archives and Records (NCAR) in Saudi Arabia provides guidelines for electronic records storage to ensure the long-term preservation of these records. These guidelines include:

1. **Storage Media**: SCFHS should use storage media that are reliable and durable, such as hard disks, magnetic tapes, optical disks, and solid-state drives.

2. **Storage Environment**: The storage environment should be controlled to prevent damage to the electronic records. This includes temperature control, humidity control, and protection against dust, water, and fire.
3. **Backup and Recovery**: SCFHS should regularly back up their electronic records and store the backup copies in a secure location. This ensures that records can be recovered in case of data loss or corruption.
4. **Encryption**: Electronic records should be encrypted to prevent unauthorized access and ensure confidentiality.
5. **Access Controls**: SCFHS should implement access controls to prevent unauthorized access to electronic records. This includes password protection, user authentication, and role-based access control.
6. **Monitoring and Auditing**: SCFHS should regularly monitor and audit their electronic records storage systems to ensure compliance with policies and regulations, and to detect and prevent security breaches.
7. **Migration and Conversion**: SCFHS should regularly migrate electronic records to new storage media and convert them to new formats to ensure their long-term accessibility and readability

The retention period for archives and documents as defined by the National Center for Archives and Records (NCAR) can vary depending on the type of document and its value or significance.

For example, the retention period for administrative documents and financial records can be 10 years after the end of the fiscal year. However, the retention period for archival documents and historical records can be permanent, as these documents are deemed to have long-term or permanent value.

Guidelines for electronic record disposal as per NCAR

The National Center for Archives and Records (NCAR) provides guidelines for the disposition of electronic records, including secure deletion, in its Electronic Records Management Policy. Here are some key guidelines:

1. Electronic records should be disposed of in accordance with approved records retention schedules and legal requirements.
2. The disposition of electronic records should be documented and authorized by appropriate personnel.
3. The method of disposition, including secure deletion, should be appropriate to the sensitivity and confidentiality of the records.
4. Secure deletion should be performed using an approved method that renders the data irrecoverable.
5. The effectiveness of secure deletion should be verified through testing or other means.
6. If electronic records are to be transferred or sold to a third party, the records should be securely deleted, or the transfer should be authorized by appropriate personnel and documented.

Retention period guidelines by NCAR

SCFHS adapt the guidelines that was issued by The National Centre for Archives and Records (NCAR) for records retention periods for various types of records, including archives and documents. Here is a summary of the retention periods defined by NCAR and used by SCFHS:

1. **Administrative records**: These records include correspondence, memoranda, and reports that relate to the administration of an organization. The retention period for administrative records is five years. Registration or scorecard (visualized on electronic media should have a retention period of 3 years from the beginning of the year following the end date of registration in the associated department and 17 years in documentation Center.
2. **Financial records**: These records include invoices, receipts, and other financial documents. The retention period for financial records is ten years.
3. **Personnel records**: These records include employee files, payroll records, and benefits records. The retention period for personnel records is five years after the employee leaves the organization.
4. **Legal records**: These records include contracts, licenses, and other legal documents. The retention period for legal records is ten years after the expiration of the contract or license.
5. **Medical records**: These records include patient records, test results, and medical billing records. The retention period for medical records is 25 years.
6. **Archives and historical documents**: These records include important historical documents and artifacts. The retention period for archives and historical documents is permanent.

8. Data Cybersecurity Controls (DCC)

Cybersecurity related to human resources:

The cybersecurity requirements in human resources prior to employment, during employment and after termination/separation must include at least the following:

- The entity's employees undertake not to use messaging or social networking applications or personal cloud storage services to create, store, or share the entity's data, except for secure messaging applications approved by the relevant authorities.

Cybersecurity Awareness and Training Program:

The cybersecurity awareness program should cover data protection themes, including:

- Risks of leakage and unauthorized access to data during its lifecycle.
- Secure handling of classified data while traveling and outside the workplace.
- Secure handling of data during meetings (virtual and physical).
- Safe use of printers, scanners, and photocopiers.
- Procedures for the Secure Destruction of Data.
- Risks of sharing documents and information through unsecured communication channels.
- Cyber risks related to the use of external storage media.

Managing Login Identities and Permissions:

Cybersecurity requirements related to access identity management and permissions should, at a minimum, cover:

- Strict restriction to allow a minimum number of employees to access, access and share data based on lists of powers limited to Saudi employees except under an exception by the authority holder (the head of the entity or his authorized representative) and that these lists are approved by the authorized person.
- Prevent the sharing of approved lists of powers with unauthorized persons.
- The lists of approved powers and the powers used to handle the data should be reviewed according to the duration specified for each level.

Protection of systems and information processing devices:

The cybersecurity requirements for Information System and Information Processing Facilities Protection must include at least the following:

- Apply update packages and security fixes from the time they are launched to systems used to handle data according to the duration specified for each level.
- Review and fortify factory settings (such as static passwords, and default background) of technical assets used to handle data.
- Disable Print Screen or Screen Capture for devices that create or process documents.

Data and Information Protection:

Data and information protection cybersecurity requirements should, at a minimum, cover:

- Use the watermark feature to encode the entire document when creating, storing, and printing, on the screen and each copy so that the code can be tracked at the user or device level.
- Prohibit the use of data in any environment other than the production environment except after a risk assessment and the implementation of controls to protect such data, such as data masking or data scrambling.
- Use the Trademark Protection Service to protect the entity's identity from plagiarism.

Secure destruction of data:

The cybersecurity requirements for secure data disposal must cover at least the following:

- Identify techniques, tools, and procedures for the implementation of secure data destruction by data classification level.
- When storage media needs to be reused, the data must be securely erased, so that it cannot be recovered.
- Keep a record of the destruction or safe deletion of data that has been performed.
- The application of the requirements for the secure destruction of data in the entity must be reviewed according to the period specified for each level.

Third-party cybersecurity

The cybersecurity requirements for third-parties cybersecurity must include at least the following:

- The existence of contractual safeguards for the ability to delete the entity's data in secure ways with the third party upon termination/termination of the contractual relationship with the provision of evidence to this effect.
- Document all data sharing with third parties, including justifications for data sharing.
- When sharing data outside the Kingdom, the host entity's ability to protect that data must be verified, and the consent of the authorized person must be obtained, in addition to compliance with the relevant legislative and regulatory requirements.
- Oblige third parties to report directly to the entity when a cybersecurity incident occurs that may affect the data shared or generated.
- Reclassify data to the lowest level that achieves the objective, before sharing it with third parties using data masking or data scrambling.
- Cybersecurity requirements when dealing with consultants for strategic projects with high sensitivity at the national level should cover at a minimum, the following:
    - Conducting a screening or vetting survey for consulting services company employees with access to data.
    - Contractual safeguards are in place, including the obligation of consulting staff not to disclose information as well as the ability to securely delete entity data with consulting firms upon termination/termination of the contractual relationship with evidence thereof.
    - Document all data sharing with consulting firms, including justifications for data sharing.
    - Oblige consulting services companies to report to the entity directly when a cybersecurity incident occurs that may affect the data shared or generated.
    - Reclassify data to the lowest level that achieves the objective, before sharing it with consulting firms, using data masking or data scrambling.
    - Allocating a closed room for employees of consulting services companies to perform their work, with the provision of dedicated devices owned by the entity through which data is shared and processed.

- Activating access and exit control systems from the closed hall, provided that only authorized persons.
- Preventing the exit of devices, storage units, and documents from the closed hall, and preventing the entry of any electronic devices into the hall.

9. Critical Systems Cybersecurity Controls (CSCC)

Cybersecurity Governance

SCFHS shall define data prerequisites for software and application development projects concerning the organization's critical systems, which must encompass the following:

- **Secure Data Migration Procedures:** SCFHS shall establish reliable and verified procedures for migrating data from testing environments to production environments. Prior to migration, all data, IDs, or passwords associated with the testing environment will be securely wiped to prevent unauthorized access or exposure of sensitive information during the migration process.

Cybersecurity Defense

- Asset Management

SCFHS shall incorporate data-driven prerequisites for enhancing the management of information technology assets, focusing on the following aspects:

- **Dynamic Asset Inventory:** SCFHS shall maintain an annually-updated data inventory of assets associated with critical systems. This comprehensive dataset shall encompass relevant asset details, specifications, and their connections to critical systems. Regular updates to the inventory will ensure accurate asset management, facilitating effective monitoring and control.
- **Involvement of Asset Stakeholders:** SCFHS shall identify asset stakeholders and involve them in the data management lifecycle for critical systems. Asset stakeholders will be responsible for overseeing and managing assets throughout their lifecycle, from acquisition to retirement. By engaging asset stakeholders, SCFHS ensures accountability and proper data-driven management of critical systems' assets, leading to efficient resource allocation and risk mitigation.

- Identity and Access Management

SCFHS shall integrate data-oriented prerequisites to enhance identity and access management for critical systems, focusing on the following aspects:

- **Robust Password Handling:** SCFHS shall employ secure data methods and algorithms, such as hashing functions, for storing and processing passwords. This data-centric approach enhances data protection and significantly reduces the risk of unauthorized access or exposure of sensitive credentials.
- **Controlled Database Access:** SCFHS shall implement strict data access controls, disallowing regular users from direct access and interaction with

databases, except for authorized database administrators. By adopting this data-driven measure, SCFHS ensures that access to critical systems' databases is controlled and limited solely to personnel with proper authorization, minimizing potential security vulnerabilities.

- Information System Protection

SCFHS shall integrate data-centric requirements to strengthen the protection of critical systems and information processing facilities, with a focus on the following aspects:

  - **Vulnerability Management:** SCFHS shall proactively address vulnerabilities by conducting data-driven reviews and modifications of default configurations. Furthermore, SCFHS will eliminate hard-coded, backdoor, and default passwords from critical systems where applicable, ensuring data security is prioritized and reducing potential points of exploitation.
  - **Data Integrity and Confidentiality:** SCFHS shall implement data-oriented measures to secure systems' logs and critical files, thereby maintaining data integrity and confidentiality. These data protection measures will safeguard against unauthorized access, tampering, illegitimate modification, or deletion, thus ensuring the authenticity and reliability of critical system data.

- Securing Mobile Devices and BYOD Practices

SCFHS shall integrate data-centric requirements to enhance the security of mobile devices and BYOD practices, with a focus on the following aspect:

  - **Full Disk Encryption:** SCFHS shall enforce full disk encryption for devices with access to critical systems to safeguard the data stored on these devices. By employing this data-oriented security measure, sensitive information on mobile devices remains protected and inaccessible to unauthorized individuals, reducing the risk of data breaches or unauthorized access to critical system data.

- Safeguarding Data and Information Integrity

In its commitment to data protection, SCFHS shall incorporate the following cybersecurity requirements:

  - SCFHS shall employ data leakage prevention techniques to protect classified data of critical systems, preventing unauthorized disclosure or access to sensitive information.
  - SCFHS shall identify the appropriate retention period for data associated with critical systems in accordance with relevant legislation. Only the necessary data required for production environments shall be retained.
  - To minimize the risk of data breaches and unauthorized access, SCFHS shall strictly prohibit the transfer of any critical systems' data from the production environment to any other environment.

- Cryptography for Enhanced Data Protection

To bolster data protection, SCFHS shall integrate the following cybersecurity requirements for cryptography:

- SCFHS shall ensure that all data-in-transit for critical systems is encrypted, ensuring a secure transmission of information between systems and networks.
- Data-at-rest for critical systems shall be encrypted at the level of files, databases, or specific columns within databases. This robust encryption mechanism safeguards the stored data, preventing unauthorized access or disclosure.
- SCFHS shall employ secure and up-to-date methods, algorithms, keys, and devices for encryption, adhering to the guidelines issued by the National Cybersecurity Authority (NCA). This ensures the use of approved cryptographic techniques that meet industry standards and best practices.

- Backup and Recovery Management for Data Resilience

To ensure data resilience, SCFHS shall incorporate the following cybersecurity requirements for backup and recovery management:

- SCFHS shall ensure comprehensive scope and coverage of online and offline backups, encompassing all critical systems. This involves backing up the necessary data and components essential for the seamless restoration of critical systems.
- Backups shall be performed at planned intervals, as determined by the organization's risk assessment. As recommended by the National Cybersecurity Authority (NCA), SCFHS shall conduct daily backups for critical systems, minimizing the potential loss of data.
- SCFHS shall implement robust measures to secure the access, storage, and transfer of critical systems' backups and storage media. These measures are designed to protect the backups from destruction, unauthorized access, or modification, ensuring the integrity and confidentiality of the backed-up data.

In pursuit of data resilience, SCFHS shall conduct periodic tests, at least once every three months, to evaluate the efficiency of recovering critical systems' backups. These tests serve to validate the effectiveness of the backup and recovery processes, ensuring that the necessary data and components can be successfully restored in the event of a system failure or data loss. By adhering to these requirements, SCFHS reinforces its ability to swiftly recover critical systems and safeguard valuable data in the face of potential disruptions or cyber incidents.

- Cybersecurity Event Logs and Monitoring Management

SCFHS shall integrate data-driven cybersecurity requirements to enhance event logs and monitoring management for critical systems, focusing on the following aspects:

- **File Integrity Management:** SCFHS shall specifically focus on activating and monitoring alerts and event logs for file integrity management. This data-centric proactive measure aims to facilitate the timely detection of any unauthorized modifications or tampering of critical system files. By leveraging data-oriented event monitoring, SCFHS can quickly identify potential security incidents and respond promptly to mitigate risks.
- **Safeguarding Security Event Logs:** SCFHS shall prioritize the security of event logs for critical systems. These logs will contain comprehensive data,

including timestamps, dates, IDs, and affected systems, serving as invaluable sources for security investigations and audits. Protecting the integrity and accessibility of these logs ensures that critical information remains intact and available when needed, enabling effective incident response and facilitating compliance with regulatory requirements.

SCFHS shall adhere to a minimum retention period of 18 months for cybersecurity event logs of critical systems, in strict compliance with relevant legislative and regulatory mandates. This data-driven approach ensures the preservation of essential security event logs over an extended duration, facilitating effective forensic investigations, incident response, and compliance with regulatory obligations. By retaining logs for an extended period, SCFHS enhances its ability to monitor, analyze, and detect potential threats or breaches, thus bolstering the overall security of critical systems.

- Application Security Enhancement
  - SCFHS shall adopt data-oriented measures to enhance application security, ensuring the integrity, confidentiality, and availability of data and functionality within these applications. The focus will be on incorporating essential data-driven security controls, protocols, and measures to elevate the overall security posture of critical systems and mitigate potential risks associated with internal applications.

The data-centric cybersecurity protocols for internal applications of critical systems, as specified by SCFHS, encompass the following key elements:

- **Data-Oriented Multi-tier Architecture:** SCFHS shall adopt a data-oriented multi-tier architecture principle for internal applications of critical systems, ensuring a minimum of three tiers. This data-centric architectural approach enhances security by promoting the separation of presentation, business logic, and data layers. It effectively reduces the risk of unauthorized access, supports scalability, and simplifies maintainability.
- **Data Protection through Secure Communication:** SCFHS shall prioritize data protection through secure protocols, such as HTTPS, for all communication within internal applications of critical systems. These data-centric secure protocols provide encryption and authentication mechanisms, effectively safeguarding sensitive data and preventing unauthorized interception or tampering.
- **Data-Driven Secure Session Management:** SCFHS shall emphasize data-driven secure session management for internal applications, employing measures such as session authenticity, session lockout, and session timeout. These data-centric safeguards effectively prevent unauthorized access, session hijacking, and mitigate the risk of sensitive data exposure.

Third-Party and Cloud Computing Cybersecurity

- Cloud Computing and Hosting Cybersecurity

In addressing Cloud Computing and Hosting Cybersecurity, SCFHS shall develop and implement a set of robust requirements governing the utilization of hosting and cloud computing services. These requirements shall encompass the following key stipulations:

- SCFHS shall consider the classification of the hosted data to implement appropriate security measures based on data sensitivity. The classification process shall guide the deployment of tailored security protocols to protect data based on its sensitivity level.

10. Other Framework Statements

General Data Protection and Privacy Principles

- SCFHS shall develop and implement a data classification scheme and ensure that data residing in SCFHS environment is classified accordingly.
- Assets shall be classified in accordance to the class of data processed, stored or transmitted through them.
- Data protection and privacy requirements specific to each class of data shall be identified and implemented.
- SCFHS shall ensure that information and data is handled according to their classification and labelling mechanism. All data and information have ownership defined and documented.
- Access to SCFHS data shall be provided based on need-to-know basis only. Data access requests shall specify the objective or purpose for which access to data is required.
- The data on receipt of access shall be utilized for the specified and approved purposes only.
- SCFHS shall implement encryption measures to ensure protection of SCFHS information as per the Cryptography Policy. This shall also include the policy on the use, management, lifetime and protection of cryptographic keys throughout their whole lifecycle.
- SCFHS shall define backup and restore policy and procedure which define the rules to ensure the business and other organization critical data continuity and to support the retrieval and restoration of archived data in the event any interruption to normal business.
- SCFHS shall prevent the transmission of production data/information into non-production environment without proper justification. SCFHS shall prevent usage of critical systems data in test and development environments.
- Any sensitive production data being transferred into systems which deal with external parties shall be protected using controls such as data masking, data anonymization and data scrambling.

- SCFHS shall define and implement third-party responsibilities with respect to protection of SCFHS data. Such responsibilities shall be included as part of third-party contracts.

Data Collection, Use, Transfer and Return

- SCFHS shall collect data, whether technical, process, business or personal for lawful purposes and in a fair manner.
- Data shall be processed only for legally permissible business purposes.
- SCFHS data shall be protected against any unauthorized or illegal access by internal or external parties.
- SCFHS data shall not be stored for more than a specified amount of time that is defined as per SCFHS data retention specified in the Backup and Restore Policy.
- The minimum necessary amount of personal data shall only be collected for purposes defined in the relevant privacy notice(s).
- Where SCFHS is established as the “Data Controller”, the method(s) for collecting personal data shall be approved prior to their use to ensure that personal data is being collected fairly and lawfully.
- Personal data collected from third parties, shall be adequately assessed for its reliability and that the methods employed by the third party are fair and lawful.

Management

- The Data Protection and Privacy Policy and the consequences of noncompliance with such a policy shall be made available to all SCFHS staff, temporary/contract staff, and third parties upon and throughout their engagement with the SCFHS.
- Formal annual Data Protection and Privacy training and awareness session shall be provided to all key SCFHS staff involved with the collection, use, retention, disclosure, and destruction of personal data.
- An ongoing data protection and privacy awareness regime, using a variety of communication mechanisms, shall be implemented to encourage and mature a data protection and privacy-awareness culture throughout the SCFHS.
- Changes to the Data Protection and Privacy Policy or related mandates shall be reviewed and approved by the head of SCFHS Cybersecurity Steering Committee, and reflected, in a timely manner, across all Data Protection and Privacy training and awareness materials.
- Personal data, related processes, systems and third parties involved in the processing of such information shall be identified, and personal data shall be classified into categories according to its type and sensitivity.
- An appropriate risk assessment process shall be used to identify, assess, and address potential data protection and privacy related risks that may have impacts on both data subjects and SCFHS.
- Requests for Changes (RFCs) and releases into production environment(s) shall be evaluated for potential privacy impacts and authorised by the Data Protection and Privacy Department.

- A Data Protection and Privacy related incident and breach management program shall be defined and implemented.
- The Data Protection and Privacy Policy and related mandates shall be reviewed for their appropriateness and completeness, against internal and external constraints, at least on an annual basis or in the event that findings from a Data Protection and Privacy compliance review or data breach highlight weaknesses sooner.

Notice

Where the SCFHS is established as the "Data Processor" of the personal data on behalf of Business Sector Areas:

Business Sector Areas should formally issue a notice to affected individuals (Data Subjects), that:

- Describes the types of personal data collected, the methods of collection, the sources of such information and the purposes for which it is collected, used, retained, and disclosed.
- Confirms their personal data shall only be used for the purpose(s) defined in the privacy notice.
- Informs Data Subjects that they are responsible for providing accurate and complete personal data to the SCFHS and describes how the Data Subjects may obtain access to their personal data (Subject Access Request) and supply updates or corrections to this information.
- Informs Data Subjects of any breach notification actions that would be taken when personal data information is compromised.

Where the SCFHS is established as the "Data Controller" of the personal data:

The SCFHS shall formally issue a notice to affected data subjects (e.g. employees), that:

- Describes the types of personal data collected and the methods of collection, the sources of such information and purposes for which it is collected, used, retained, and disclosed.
- Confirms their personal data shall only be used for the purpose(s) defined in the privacy notice.
- Informs Data Subjects that they are responsible for providing accurate and complete personal data to the SCFHS and describes how the Data Subjects may obtain access to their personal data (Subject Access Request) and supply updates or corrections to this information.
- Identifies third parties "Data Processors" to whom the Data Subject's personal data will be disclosed and why.
- Provide a general description of precautions in place to protect their personal data.
- Describes how the Data Subject should contact the SCFHS if they wish to lodge a formal complaint.
- Informs Data Subjects of any breach notification actions that would be taken, and the extent of data subjects personal data information is compromised.

Choice and Consent

Where the SCFHS is established as the "Data Controller" of the personal data and exemptions do not apply:

- Data Subjects shall be informed, prior to collection of their personal data, of the choices available to them and whether their implicit or explicit consent is required to collect, use, retain and disclose their personal data.
- Where sensitive personal data (Appendix B) is collected, used, retained or disclosed; explicit consent, from the affected Data Subjects, shall be obtained prior to collection.
- Consent for any subsequent changes to the processing of personal data shall be sought from affected Data Subjects.

Where the SCFHS is established as the "Data Processer" of the personal data on behalf of Business Sector Areas:

- Data Subjects shall be informed, prior to collection of their personal data, of the choices available to them and whether their implicit or explicit consent is required to collect, use, retain and disclose their personal data.
- The Data Subject shall have the right to object on legitimate grounds to the processing of the data.
- Personal data may be processed only if the data subject has unambiguously given consent or processing is necessary.
    - For the performance of a contract to which data subject is party.
    - For compliance with a legal obligation to which the controller is subject.
    - To protect the vital interests of the data subject.
    - For the performance of a task carried out in the public interest.
    - For the purposes of the legitimate interests pursued by the controller.

Use, Retention and Disposal

- Personal data shall only be used in conformity with the purposes specified in the relevant privacy notice(s), in agreement with the obtained consent and in compliance with legal frameworks.
- Personal data shall not be retained for longer than necessary to fulfil the specified purposed in the relevant privacy notice(s) unless a law or regulation requires otherwise.
- A formal SCFHS personal data Records Retention Schedule shall be defined and maintained.
- Retaining records on a 'just in case' basis shall not be acceptable.
- Records that are no longer required for the purposes defined in the relevant privacy notice(s) or exceed the retention requirements as per SCFHS Records Retention Schedule; shall be archived securely or destroyed in accordance with a suitable destruction process and a Certificate of Destruction issued.

- Personal data (original, archived or backup copies) that is no longer retained shall be anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.
- Any third parties engaged to provide destruction facilities shall be deemed a Data Processor and therefore formal disclosure procedures and legal framework requirements defined in this policy shall apply.
- Using personal data for the purposes of testing new developments or changes to existing information systems is prohibited unless the personal data is masked or scrambled and does not identify the Data Subject.

Access

- A formal Subject Access Request (SAR) process shall be defined and implemented within the SCFHS to ensure that responses to such requests are consistent, fair, understandable, and responded to in an appropriate and timely manner.
- Individuals submitting Subject Access Requests shall be appropriately authenticated prior to their request being actioned.
- Non-Disclosure Agreement shall be signed by internal SCFHS employees prior have access to Data Subject's personal data.
- Non-Disclosure Agreement shall be signed by external clients of SCFHS prior have access to Data Subject's personal data.
- Access of personal data must be based on Need-To-Know and Least Privilege principles.
- Database administrators shall not be permitted to delete any sensitive data from database unless approved from multiple authorized levels including data owner.
- All DBAs operations (select, update/modify, etc.) shall be logged and the logs access is forbidden for the DBAs.
- The logs of DBAs activities (DB2, PDS, etc.) shall be reviewed on periodic basis as per the Identify and Access Management related procedures.

Security for Privacy

- To ensure and assure that personal data is adequately protected, logically and physically, from unauthorised exposure, disclosure, loss, alteration, or deletion/destruction.
- In accordance with its sensitivity, format, storage medium and method of transfer, personal data shall be adequately protected from loss, misuse, unauthorized access, disclosure, alteration, and destruction.
- Transmission of data shall be encrypted in compliance with The Cryptography Policy (by depending of its nature and criticality).

Data Sharing with Third Parties

As Saudi Commission for Health Specialties (SCFHS) is the regulatory body for healthcare professionals and healthcare institutions in Saudi Arabia, Its main role is to ensure the quality of healthcare services in the country and to regulate the education, training, and licensure of healthcare professionals., Data from many sectors are stored and hosted within SCFHS technical environments. Usually, some sectors (third parties) asking to share data related to other sectors, in this case the following measures should be met prior to share any data:

- Data shall be classified prior to sharing it and based on its classification decision of sharing it or not should be taken. (ref. NDMO)
- Data shall be shared for legitimate purposes based on a legal basis or a justified need aiming to achieve a public interest without causing any harm to the national interests, the privacy of individuals or the safety of the environment.
- The original owner of data (creator of data) approval shall be obtained.
- A memorandum (an agreement) between original owner of data, or SCFHS if the authorization is given to SCFHS by the original data owner, (first party) and the data sharing requester (second party) shall be signed in compliance with NDMO regulation.
- All parties involved in data sharing shall apply appropriate security controls to protect data and share it in a safe and reliable environment in accordance with the relevant laws and regulations, and according to what is issued by NCA.
- Identity of personal data must be hidden, unless it is necessary for the purpose of sharing, with the determination of the necessary controls to maintain the privacy of the data owners in accordance with the privacy personal data.
- SCFHS shall keep records of data-sharing requests and decisions related to them through Archer tool.
- Personal data shall not be stored or transferred outside KSA unless approval taken from NDMO.
- In case of conflicts, NDMO shall be requested to resolve the issue.

Quality

- SCFHS shall take all reasonable steps to ensure that personal data, collected by the SCFHS, is complete, accurate and relevant for the purposes for which it is to be used.
- Appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up to date.
- SCFHS honours requests from users to review all Personally Identifiable Information maintained in reasonably retrievable form, which currently consists of employee name, address, e-mail address telephone number and will correct any such information which may be inaccurate. Users may verify that appropriate corrections have been made.

Monitoring And Enforcement

- A formal process to deal with privacy-related enquires and complaints shall be defined and implemented throughout the SCFHS.
- A suitable ongoing Data Protection and Privacy compliance program shall be introduced across the SCFHS with appropriate means to identify, assess, report, and monitor progress of Data Protection and Privacy related weaknesses (i.e. against this framework, its related mandates and the latest NDMO regulatory Guideline) within the SCFHS's operational environment.
- The act of processing personal data and its business purpose shall always be recorded and maintained (e.g., data flows, interface agreement documents, records of processing activities, etc.).

Privacy-by-Design

- Privacy by Design (PbD) is critical and shall be implemented to address both privacy needs of data subject and legitimate increases and objectives of SCFHS.
- SCFHS shall implement technical and organizational measures, at the earliest stage of the design of the processing operations in such way that safeguards privacy and Data Protection principles right from the start and ensure the protection of the rights of data subjects. PbD should be followed each time one of the following occurs:
    - SCFHS intends to launch a new project.
    - SCFHS needs to make significant changes to the infrastructure or architecture of an existing project.

11. References

1. NDMO Regulation.
2. NCA-ECC Essential Cybersecurity Controls
3. NCA-DCC Data Cybersecurity Controls
4. NCA-CSCC Critical Systems Cybersecurity Controls
5. National Center for archives and regulation (NCAR)
6. ISO 27001