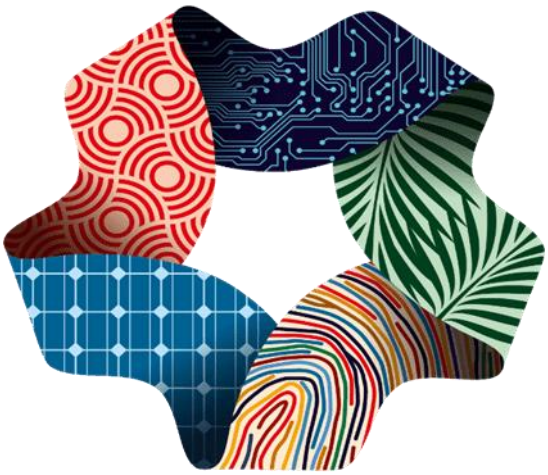

NEOM نيوم

DATA CLASSIFICATION AND PROTECTION FRAMEWORK

Revision Control

Issue	Revision	Date	Details of Revision	Revised by
1	0.1	10 June 2022	Initial Draft	
2	0.2	20 June 2022	Changes to document structure and adding more details to identified sections	
3	0.3	05 July 2022	Changes to document structure and adding more details to identified sections	
4	1.0	18 July 2022	Final draft version for review	
5	1.1	22 July 2022	Reviewed final draft version for review	
6	1.2	29 July 2022	Additions to document content for final version sharing	
7	1.3	18 August 2022	Changes to Governance Structure	
8	1.4	19 August 2022	Updates to RACI model	
9	1.5	21 August 2022	Updates to address comments	
10	1.6	23 August 2022	Changes to address comments	
11	1.7	24 August 2022	Updates to destruction definitions	
12	1.8	31 August 2022	Updates following FW presentation to Authority, IT Services, Audit, & eGRC	

Approval

Issue	Date	Issued by	Signature	Approved by	Signature

Table of Contents

Table of Figures

Table of Tables

1. INTRODUCTION

1.1. PURPOSE & BACKGROUND

Optimally protecting data, is an element of utmost importance for any organisation in today's ever-evolving digital society. Considering the sheer volume of data created and managed in every mature digital environment and the possible grave consequences to be endured if data are, for example, corrupted or accessed by an authorized source, it is necessary to develop a precise set of data security practices. For this purpose, NEOM has set out the Data Classification & Protection Framework, in which, the fundamental principles and practices to ensure the confidentiality, security, and availability of all NEOM's data, are set out and defined.

The Data Classification and Protection Framework establishes the building blocks for mature data classification and protection practices within NEOM and eventually help to achieve the following desired objectives: Risk Management, Compliance Management, Business Enablement, Cost Reduction, and Operational Excellence.

This Framework introduces new data classification scheme with all the necessary classification levels and detailing recommended data handling controls. The Framework addresses areas of utmost importance for optimized data classification and protection at NEOM, including but not limited to data retention, data access, and data metrics reporting.

1.2. SCOPE & APPLICABILITY

It should be noted that the current document outlines and thoroughly describes all fundamental elements of the designed Framework, while also working in conjunction with additional supporting documents, artifacts and templates, which facilitate specific mandates and key activities; these artifacts are included within this document, at the Annexes.

All the practices defined and presented within this Framework are applicable to all data produced, received, processed or managed by NEOM or authorized third parties, aiming to ensure an effective and consistent data governance model of all data types covering the creation, usage, storage, retention and the disposal phase. The data in reference include electronically stored data locally or on cloud, data on removable storage devices, and physical paper records throughout their lifecycle. All employees in NEOM must be familiar with the practices developed within this Framework and are accountable as per their roles and responsibilities to follow the practices correctly. All employees in NEOM, with no exception, must comply with this Framework.

Furthermore, this Framework has been developed in accordance with the National Data Management Office (NDMO) of the Kingdom of Saudi Arabia (KSA), as well as with further requirements that set out in other regulations, standards and best practices from the region and abroad. The ownership of this Framework falls under to the CISO Office responsibility, which therefore must ensure that the content of this Framework is constantly in line with best practices and regulations, while the Framework must be always updated, based on all future changes that will occur to these sources.

It should be noted that as a cornerstone of this Framework is the data classification scheme, defining the possible classification levels by which all data elements will be sorted considering the business need for sharing and relative level of confidentiality, along with the necessary integrity measures to assure their availability.

This Framework defines the roles and responsibilities of multiple stakeholders across NEOM who all cover different responsibilities within the Data Classification and Protection program. Moreover, the Framework defines the data handling controls which outline the minimum necessary practices to ensure that throughout their lifecycle data are managed in a safe and secure manner. In addition, the Framework integrates information related to data access practices, to data retention schedule, and key performance indicators to evaluate the effectiveness of the practices defined in this Framework.

1.3. DRIVERS FOR THE FRAMEWORK

The main **drivers** for the development of the Data Classification & Protection Framework are:

- Defining and communicating on an organization-wide level the sensitivity of the data managed by NEOM, which this Framework addresses through the Data Classification Scheme
- Defining and communicating on an organization-wide level the appropriate protection level of of the data managed by NEOM, which this Framework addresses through the Data Handling Controls Matrix
- Establishing visibility on who has access to data, which this Framework addresses through implementation of the High-Level Access Matrix
- Establishing visibility on where data are stored and retained, which this Framework addresses through the implementation of the Data Retention Schedule
- Establishing appropriate rules for the appropriate protection of data throughout its full lifecycle, from creation to disposal

It should also be noted that apart from the core drivers for the current document, the Data Classification & Protection Framework is also an important facilitator for **additional business needs and drivers** of NEOM, including:

- Managing potential impact, of varying nature and levels for NEOM, deriving from potential data-related incidents and issues
- Enhancing NEOM's overall security posture via appropriate data protection
- Cost containment of operational practices relevant to data management, by establishing consistent and organisation-wide practices
- Enhancing the efficiency of managing and administering data protection activities
- Supporting compliance and alignment with key regulatory mandates and best practices
- Enabling risk reduction, aligning with NEOM's overall risk posture
- Enabling integration of data protection with overall data governance capabilities of NEOM
- Raising user awareness on data protection and appropriate handling of data in a secure and consistent manner

2. DEFINITIONS & ABBREVIATIONS

The following table contains the terms mentioned in this document and their corresponding definitions within this context.

Data	A collection of facts in a raw or unorganized form such as numbers, characters, images, video, voice recordings, or symbols.
Personal Data	Personal data can be defined as any piece of information that can be used to identify a person, such as: o First and last name, o Address, o ID card/passport number, o Income, o Cultural profile, o Internet Protocol (IP) address.
Sensitive Personal Data	Sensitive Personal Data can be referred to as any distinct personal data such as: o Racial or ethnic origin, o Political opinions, o Religious and philosophical beliefs, o Trade union membership, o Genetic data, o Biometric data for the purpose of uniquely identifying a natural person, o Data concerning health, o Sex life and sexual orientation.
Personal Identifiable Information (PII)	Personal Identifiable Information is information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.
Data Source	An element (single documents, set of documents, assets etc.) which contains data.
Data Confidentiality	The state of keeping data secret by preserving authorized restrictions on data access and disclosure.

Data Integrity	The state of ensuring data validity by guarding against improper information modification or destruction.
Data Availability	The state of making data accessible and usable when needed in a timely and reliable manner.
Data Classification	Grouping data into levels based on the assessment of impact relating to unauthorized disclosure of the data or its content.
Data Handling	A set of controls to ensure that throughout its lifecycle data are secured proportionately to their classification level.
Data Retention	Definition of how and for how long are data saved for compliance or regulatory reasons, as well as how it disposes of data once it is no longer required.
Data Lifecyle	The data life cycle is the sequence of stages that a particular data source goes through from its initial generation to its eventual archival and / or deletion. In the context of this Framework the lifecycle stages are the following: o Creation, o Transfer, o Storage, o Usage, o Retention & Disposal.
KPI	Key Performance Indicator.
Structured Data	Structured data are data that have been predefined and formatted to a set structure before being placed in data storage, which is often referred to as schema-on-write.
Unstructured data	Unstructured data are data stored in their native format and not processed until they are used, which is known as schema-on-read. It comes in a myriad of file formats, including email, social media posts, presentations, chats, IoT sensor data, and satellite imagery.
NDMO	National Data Management Office of the Kingdom of Saudi Arabia

Table 1 Definitions & Abbreviations

3. DATA CLASSIFICATION & PROTECTION GOVERNANCE STRUCTURE

3.1. GOVERNANCE STRUCTURE DESCRIPTION

The governance structure defines the allocation of the appropriate roles within the Data Classification & Protection activities and program, along with their interrelations, collaboration principles and overall synergies. As depicted in the diagram below, there are multiple independent lines of collaboration, with the CISO Office holding a central facilitator role, and with a Data Classification Protection Working Group overseeing the strategic direction, governance, operations and management of Data Classification and Protection Program. . The core and fundamental roles for Data Classification and Protection specific responsibilities are:

- Data Owner
- Data Custodian
- Data User

To support their duties, there are multiple teams that are essential for efficiently and effectively completing the Data Classification and Protection activities and duties to be described in the following chapters (specifically Data Classification described in chapter 4.2, Data Impact Analysis in chapter 4.3, and Data Handling in chapter 5.2).

On the one hand there are involved units from a business governance side. Their roles aim at supporting the Data Classification and Protection implementation, by collaborating mainly from a governance and compliance standpoint.

On the other hand, there are teams involved from an IT standpoint, and their role within the Data Classification and Protection is of a more technical nature.

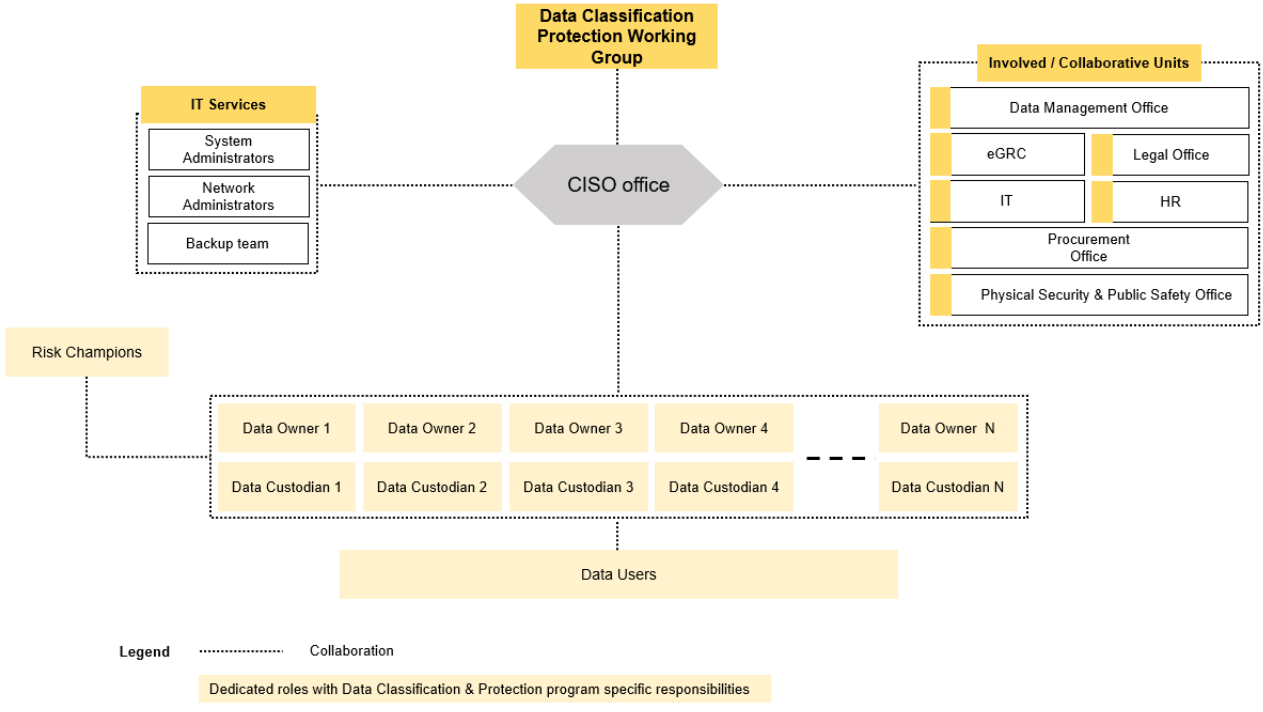

Figure 1 NEOM Governance Structure

3.2. KEY ROLES AND RESPONSIBILITIES

As presented in the schematic diagram, there are dedicated roles for Data Classification and Protection with specific responsibilities on this matter and there are several related roles in support of this.

The following tables explicitly defines all the duties associated with each of the roles directly and indirectly related to the Data Classification & Protection process.

Roles	Type of Involvement	Definition of the Role
CISO Office	Core role	The Chief Information Security Officer (CISO) Office facilitates NEOM's Data Classification and Protection program on a strategic level. Moreover, The CISO is responsible for the overall wellbeing of the cybersecurity program. The responsibilities include: • Oversee the overall performance of the cybersecurity program, and therefore of data classification and protection, within NEOM. • Provide security governance and advising to sectors and departments • Evaluating the relevant data classification and protection processes and identify areas for improvement from information security point of view. • Assess the reported Data Classification and Protection performance measures (key performance indicators) and create the appropriate reporting dashboard tools to be presented to the Working Group.
Risk Champions	Core role	Risk Champions are to be viewed as Point of Contacts for all departments and sectors managing and working with cybersecurity related data. The responsibilities include: • Coordinate with CISO office on information security awareness and communication to their respective departments and offices. • Enable and infuse awareness of data classification and protection matters within NEOM • Closely collaborate with Data Owners in assessing the appropriate data handling controls to be implemented • Provide input to cyber security risk management team on the best way to implement risk management in specific areas of the business and at what pace

Roles	Type of Involvement	Definition of the Role
		• Assist in project management processes by providing relevant and required information for cyber security related initiatives • Act as “translator” between risk management and their technical department
Data Classification & Protection Working Group	Core role	The Data Classification & Protection Working Group is the governing body of the key stakeholders / dedicated roles within the Data Classification & Protection program. It should be noted that he Data Classification & Protection Working Group does not aim to introduce a new, standalone committee, whereas can be embedded within existing working groups or committees that may provide adequate overview and decision making. The responsibilities include: • Overseeing and supporting the program on critical issues • Develop and support the implementation of strategic decisions for the Data Classification & Protection program • Assess the reported Data Classification and Protection performance measures (key performance indicators) and create the appropriate reporting dashboard tools. Moreover, address critical issues deriving from KPI assessment The committee must have representatives from, at least, the following entities within NEOM: • Data Management Office • eGRC • Legal Office • IT • HR • Physical Security & Public Safety Office
Data Owner	Dedicated role	The Data Owners are usually a member of senior management who have ultimate responsibility for the data collected and maintained by their sectors and departments. The Data Owner is accountable for the classification, protection, use, and quality of one or more data sources and remains liable for their data’s integrity, availability, and confidentiality. Data

Roles	Type of Involvement	Definition of the Role
		owner can be directly in charge of remediating issues with data or delegate those tasks to a data custodian. The responsibilities include: • Classify data collected or generated by the department or sector (with advice from the Data Custodian). • Determine the storage location of this data. • Determine access rights to this data. • Ensure, with the support of the CISO Office, that the data is secured in accordance with the defined controls (these compliance checks is done in conjunction with Data Custodian). • Evaluate the necessity of reclassification. • Maintain the Data Inventory up to date. • Conduct exercises to verify the validity of the established retention periods and initiate the disposal phase if needed. • Support the development of training and awareness material for data users on data classification & protection. • Ensure that data shared from own sector or department to others will be consistently handled as per defined security requirements. • Accountable, together with the Data Custodian, of ensuring data exception management, including assessing practical considerations or impact on the related business process.
Data Custodian	Dedicated role	The Data Custodian holds technical responsibility for implementing and maintaining security controls for a given data source in order to meet the requirements specified by the Data Owner. In fact, the Data Custodian holds the role of technical assistant / advisor of a Data Owner and the actual technological / technical handler of the data under Data Owner's supervision. The Data Custodian proposes and monitors the implementation of the handling controls ensuring the effective governance and protection of the data by suggesting security, scalability, availability, accuracy, technical standards to be used. The responsibilities include:

Roles	Type of Involvement	Definition of the Role
		• Advises Data Owners regarding data classification to make sure that appropriate security controls are in place. • Ensure, in alignment with Data Owner, that data is secured by applying the appropriate technical controls relevant to each classification level throughout the data life cycle. • Ensure that proper access controls are implemented, in alignment with what has been determined by the Data Owner. • Ensure the correct processing, storage and the availability of data to all employees who are authenticated and authorized to have access. • Protect the data under their custody from unauthorized disclosure, access, alteration, destruction, or usage. • Maintain data quality by using the Data Classification and Protection performance metrics. Moreover, they are responsible to communicate any data issues to those impacted. • Ensure compliance with data security practices, by maintaining communication with the eGRC and Legal Office.

Data User	Dedicated role	The Data User is a NEOM employee that interacts with, accesses, uses or updates data for the purpose of performing a task authorized by the Data Owner.
		
		Data Users are provided with an Acceptable Use Policy, and before being given access to NEOM data must be aware of the legal consequences of data violations.
		
		The responsibilities include:
		
		• Use NEOM data in a manner consistent and limited to the purposes intended in adherence to:
		  ○ Data Classification Policy
		  ○ Data Classification Handling Controls
		  ○ Any other relevant business rules
		  ○ Privacy requirements.
		• Participate in the Training and Awareness activities related to Data Classification and Protection.

Roles	Type of Involvement	Definition of the Role

Data Management Office	Involved unit	The responsibilities include:
		• Infuse data governance within data classification and protection program
		• Managing the availability, usability, integrity and security of data in NEOM.
		  ○ ensures that data is consistent
		  ○ ensure data is trustworthy
		  ○ ensure data does not get misused.
		• Ensuring data quality as well as its security by maintaining the Data Inventory up to date.
		• Ensuring the wellbeing of data flows within NEOM's teams and sectors, and with the approved vendors

eGRC	Involved unit	• Maintain the risk register in relation to data privacy and protection matters • Ensure that compliance mandates and requirements are followed for matters related data privacy and data protection. • Ensure that data retention controls implementation take place when mandates communicated by Legal Office and other departments and offices
Legal Office	Involved unit	• Ensure that compliance mandates communication with the CISO, the Working Group, and sectors and departments take place promptly and appropriately in case of new national or international laws to be followed in matters of data privacy and data protection • Support departments and offices in defining regulatory requirements to their business lines. • Ensure that data retention mandated communication takes place promptly and appropriately in case of new national or international laws
IT	Involved unit	IT provides required IT resources to ensure appropriate implementation of data classification and protection technology as well as required support. In addition, IT must enable Helpdesk to support in:

Roles	Type of Involvement	Definition of the Role
		• Troubleshoot, diagnose, and resolve technical hardware and/or software issues • Provide resolutions • Provide needed information on IT products or services • Keep record of problems and their resolution • Maintain technical documentation and service catalog on installation of software, configuration of hardware and problem troubleshooting
HR	Involved unit	The HR (human resources) office, within the limits of the Data Classification & Protection program, is responsible for handling and security the personal data of staff. This data derives from the hiring process, payroll, managing pensions and benefits administration etc. • Moreover, within the HR office there are officers dedicated to the support of development of cybersecurity training material and awareness sessions support.
Procurement Office	Involved unit	The Procurement Office is responsible for sourcing products/services needed by NEOM to best help achieve its goals. These purchases generate a large amount of data, even personal data of third parties and vendors.
Physical Security & Public Safety Office	Involved unit	Physical Security and Public Safety Office is responsible of protecting personnel, organization's assets, and preventing workplace crime. Within the limits of the Data Classification and protection activities, the focus of the Physical Security and Public Safety Office is about security data both in a preventive manner and also by recognizing potential threats and prevent them from becoming realized. Moreover, the Office is responsible to physically protect organization's technological and physical assets. Everything that is stored and / or operates within organization's premises, is subjected to Physical's Security and Public Safety Office supervision.

Table 2 Key Roles and Responsibilities

3.3. RASCI MATRIX

The RASCI matrix depicts the actions of the roles involved in the Data Classification & Protection process.

(R)esponsible	The individual responsible for delivering a task.
(A)ccountable	The individual held accountable for delivery of the task.
(S)upport	The individual who will support the completion of the task.
(C)onsulted	The individual to provide input / be consulted in relation to delivering a task.
(I)nformed	The individual to be kept informed of progress throughout delivery of a task.

	Core Roles					Involved / Collaborating Roles							
	Data Classification & Protection Working Group	CISO Office	Data Owner	Data Custodian	Data Users	Data Management Office	Risk Champions	Legal Office	eGRC	IT	HR	Procurement Office	Physical Security & Public Safety Office
Actions	**Responsibilities**												
Identify national regulatory requirements and mandates in collaboration with Data Owners	**C**	**C**	**C**			**C**		**R/A**	**C**	**I**	**I**		
Define NEOM-specific data classification and protection regulations and mandates in collaboration with Data Owners	**C**	**C**	**C**			**C**		**R/A**	**C**	**I**	**I**		
Oversee the wellbeing of the Data Classification & Protection program	**R/A**	**C**				**C**			**C**				
Evaluating the business processes and identify areas for improvement	**R/A**	**I**	**C**				**C**						

	Core Roles					Involved / Collaborating Roles							
	Data Classification & Protection Working Group	CISO Office	Data Owner	Data Custodian	Data Users	Data Management Office	Risk Champions	Legal Office	eGRC	IT	HR	Procurement Office	Physical Security & Public Safety Office
Define strategic direction and decisions for the Data Classification & Protection program	R/A		C				C						
Communicate strategic directions and decisions to NEOM departments and Sectors	I	A				C	R						
Classify and reclassify collected data sources		C	R/A	S/C	I	I			C				
Evaluate the necessity of reclassification			R/A	I		I							
Define information security controls and assess implementation of defined controls	A		C			I			C				
Implement information security controls		C	S/C	R/A		S	S		C	C			S
Establish Retention period	I		R/A	S/C	I			C	C	I			
Ensure that the appropriate access controls are enabled		C	A	R		S				S			
Update data inventory			R	I	C	A	S						
Ensure data quality			C	C		R/A	I						
Ensure data flow security	I					R/A	S/I		C				
Ensure compliance with data security laws and regulations		C/I	C/I	C/I					R/A		C		
Ensure data exceptions management		C/I	A	R	I		C/I		S				

	Core Roles					Involved / Collaborating Roles							
	Data Classification & Protection Working Group	CISO Office	Data Owner	Data Custodian	Data Users	Data Management Office	Risk Champions	Legal Office	eGRC	IT	HR	Procurement Office	Physical Security & Public Safety Office
Ensure classification and protection of data shared with vendors and third parties		C	C			I					C	R/A	
Ensure non-digital data security		C	C	I		S			C				R/A
Ensure that data protection software's are procured		I								C/I		R/A	
Ensure technology is available to enforce data classification and protection requirements	C	C	I		I		I			R/A			
Troubleshoot of technical issues relating to Data Classification & Protection hardware and Software		I	C	S	I		C/I			R/A			
Development of Data Classification & Protection training and awareness material	C	R	S	S							A		
Assess KPIs wellbeing and produce necessary documentation & reporting	I	R/A	S	S			I						

Table 3 RASCI Matrix

4. DATA CLASSIFICATION & PROTECTION OVERVIEW

4.1. KEY PRINCIPLES

The Data Classification & Protection Framework is developed based on key principles which are the fundamentals for the appropriate protection of NEOM's data in a consistent and cohesive manner. The principles listed below define the general rules.

1. **Appropriate & Timely Classification of Data:** The classification level attributed to a data source must be based on the process as described within this Framework, in order to ensure standardized and appropriate data classification. Moreover, the classification process must be initiated upon being made aware of or upon receive a data source, and the exercise is timebound.
2. **Exhaustive & Unimpaired Handling Control implementation:** The controls attributed to the data source in accordance with the classification level defined must be put in place as detailed, ensuring they are properly implemented and remain unimpaired, in order to guarantee the proposed safeguarding of the data.
3. **Segregation of Duties:** The Data Custodian has the responsibility of checking that data has been correctly classified and shall conduct audit. Data must not be reclassified by another person unless authorized by the Data Owner. In addition, duties of participants in the classification process must not overlap in terms of classifying data, approving a classification decision, granting authorization for access or usage of data, accessing data, protecting data, or disposal of data – in a way that does not lead to overlapping specialization or dissipation of liability.
4. **Need to Know & Least Privilege:** Access to data must be provided only if there is a legitimate requirement for usage based on authorization and access controls. Moreover, user access rights to data must be limited to the minimal according to the user's role and specific requirements to perform their duties.
5. **Purpose & Retention Limitation:** Data sources must be available only for specified and legitimate purposes. Moreover, it cannot be retained longer than data retention requirements.

In terms of logic and strategy introduced, the Data Classification & Protection Framework has been developed in an agile manner, enabling varying modes of classification for NEOM in the different maturity stages of the overall journey. Specifically, the Framework initially relies on user-based classification, while also setting the necessary prerequisites for enabling automatic classification, based on content, as the Framework is slowly integrated in the day-to-day practices of NEOM.

Data Quality

The overarching principle regulating the Data Classification & Protection Framework is data quality assurance, an element which is mandatory for Data Owners and Users to take into consideration, throughout the operationalisation of the Framework. Simply put, data quality indicates the usability, reliability, and availability of a particular data source and whether it is in line with a predefined quality degree. It is essential to undertake the practice of data quality assurance throughout all sectors of NEOM insofar using unreliable or incomplete data would lead to low quality and untrustworthy results.

To assure data quality, the following principles shall be taken into consideration:

1. **Usability** – The usability principle considers the ability to derive useful information from the data. This is to say that data holds a specific structure and must be recognized for its own purpose and perform tasks effectively and efficiently. Users must therefore be able to recognize the data sources used for and derived from tasks, essentially making all data sources effective for performing different tasks.
2. **Reliability** – The data principles of reliability refer to how data must be consistent and uniform across multiple records, programs, or platforms, even when it comes from multiple sources. This is because it is of utmost importance to have trustworthy data sources which accurately conform to the actual real situation they intend to represent. This inherently requires for data to derive from verifiable sources that can be confirmed, in order to also ensure its completeness. All in all, it is about consistency and uniformity.
3. **Availability** – Authorized users are able to access the necessary data whenever required. There must be authentication mechanisms with defined access channels so that not only the data is protected, but that it is available with timeliness. Similarly, this principle requires for networks, systems and applications to be up and accessible, particularly in relation to critical business processes.

Figure 2 Data Quality Assurance - Key Principles

4.2. DATA CLASSIFICATION SCHEME

Data classification is the process of organizing data into categories in order to both use it and protect it more efficiently. Classification levels are well differentiated and hold inherent specific qualities that discern them from one another. Therefore, by the classification level attributed to a data source it is possible to, at minimum, identify the sensitivity and the value that it holds, while also understanding the impact that the altering, stealing, or destroying of the data would have. In other words, it is an immediate and simple practice by which it can be understood what data is sensitive, what is less so, and what is not, and consequently it is possible to adequately protect it (protection control practices are described in chapter 5.2 – Data Handling).

Within this context, NEOM has planned that all the data it manages and receives is appropriately classified throughout its lifecycle as appropriately to its value by establishing a structured and comprehensive Data Classification Scheme.

The scheme in question has different levels and sub-levels (where appropriate), in order to capture all possible data types received, used, managed, or stored by NEOM. The following table offers a concise overview of the classification levels and sub-levels with their impact level:

Data Classification Level	Data Classification Sub-Levels	Impact
Top Secret	VIP Human Safety (TS – VIP)	CRITICAL HIGH
	Government / Organizations Operations (TS – GOV)	
Secret (S)		HIGH
Confidential	Confidential External (CE)	MEDIUM
	Confidential Internal (CI)	
	Confidential Internal Specific (CI – Sn*)[1]	
Internal (I)		LOW
Public (P)		NONE

Table 4 Data Classification Scheme

The classification levels are to be understood in a hierarchical and sequential manner, starting from Top Secret data all the way down to Public data. Top Secret data refers to the smallest percentage of NEOM data and which

[1] ***n*** to be replaced with specific sector acronym. E.g., Confidential data from and for the Human Resources sector shall be identified as "CI – HR"

will be available only to selected and essential individuals, while Public data refers to that which for all intents and purposes is to be shared with all, regardless of a direct relationship with NEOM or its individuals. It is essential to note that all data before being classified are considered as Internal. However, as all data must undergo the classification process, this is a provisional classification which can change either decreasing or increasing (it will remain classified as Internal only if appropriate).

It should be noted that, the above Classification Scheme covers the full list of envisioned levels, part of the current Framework, whereas NEOM can opt to phase the implementation (roll-out of classification levels) to the users, enabling optimal awareness and expansion. The aforementioned process, in no way affects the completeness and integrity of the scheme and its usage, as per the below chapters.

The classification attributed to data must not be perceived as static, but rather it must be reviewed on a periodic basis by the Data Owner, at least annually. The review of the data may also occur before the determined standard review period, in case of new legal or business requirements. Moreover, if newly acquired data presents characteristics that are not represented in the scheme, these must be noted to evaluate it accordingly.

Aside from the review of data, the Data Owner has ultimate ownership over all data within its sector, therefore also holds responsibility of ensuring that all data is classified, that appropriate controls are applied through its lifecycle (more on the topic of data handling controls in chapter 5.2), and that the data is not retained for longer than its intended purposes (more on the topic of data retention in chapter 5.4).

In order to proceed with the classification of data, the Data Owner must make direct use of the following logics to determine the appropriate classification.

Classification Levels (Sub - Level)		Definition	Examples
TOP SECRET	**VIP Human Safety (TS – VIP)**	Top Secret VIP Human Safety data must be accessible only by a highly restricted and selected group of individuals. Unauthorized access to or disclosure of the sensitive data relating to VIP security and safety adversely and exceptionally affects: Individuals' health by also endangering their safety and security at a massive scale in a way that it is difficult to recover,	1. Personally Identifiable Information (PII) such as address, social security numbers, phone numbers, license numbers, and Special Category status (e.g., medical/ financial/ religious or political beliefs, biometric identifiers) of high-level executives of NEOM 2. Information on movements of VIPs and of high-level executives of NEOM

		NEOM's interest, reputation, and diplomatic relations.	
	Government / Organizations Operations (TS – GOV)	Top Secret Government / Organization Operations data must be accessible only by a highly restricted and selected group of individuals. Unauthorized access to or disclosure of this sensitive data adversely and exceptionally affects in a way that is difficult to resolve: - NEOM's (and KSAs) interest, operations, assets, public security, economic wellbeing, reputation, diplomatic relations, operational efficiency of the security or intelligence operations of military forces, infrastructure, and governance functions, - Functionalities causing damage to the interest, - Individuals' health and safety at a massive scale, - The environment and/or natural resources causing catastrophic damage.	1. Military operations details and plans 2. Official political information on the international relationships and conventions or treaties and all related discussions, studies, and preparations 3. Information related to the activities, measures and structure of security and intelligence bodies (e.g., information on the encryption keys) 4. Information on terrorism crimes and aggressive plans 5. Information on weapons and ammunitions or strategic military locations or any source of deterrent force 6. Information on movements of armed forces or internal security forces

SECRET (S)		Unauthorized access to or disclosure of such data or its content adversely and severely affects: - NEOM's interest, reputation, diplomatic relations, operational efficiency of the security or intelligence operations of military forces, economy, infrastructure, and governance functions, - Financial loss that leads to bankruptcy or the inability to perform defined purposes, - Individuals' life causing them significant harm or injury, - The environment and/or natural resources causing them long-term damage.	1. Information that could disclose designs, configurations or vulnerabilities exploitable of critical infrastructure 2. Information on MoU's with international companies to establish commercial, strategic, or economic interests for NEOM 3. Information related to bilateral agreements and diplomatic MoU's between NEOM and other countries 4. Copy-righted materials such as source code 5. Information such as NEOM earnings estimates
CONFIDENTIAL	**Confidential External (CE)**	Unauthorized access to or disclosure of such data or its content, which can be shared on a need-to-know basis with third parties, adversely affects not strictly within NEOM environment: - NEOM's and/or third party/vendor operations and economy to a contained extent, - Functionalities of assets with limited financial loss, - Individuals' interests, - The environment and/or natural resources causing contained damage in the short-term.	1. Requests for proposals and tender documents 2. Product specification prior to public release (product information generated for the client) 3. Presentations for potential engagements 4. Third Party / Vendor Passwords and PIN codes / VPN tokens 5. Vendor contracts and quotations, together with non-disclosure agreement 6. Personally Identifiable Information (PII) such as name, phone numbers, email, etc. of third party / vendor users and personnel

	Confidential Internal (CI)	Unauthorized access to or disclosure of such data or its content, which can only be shared on a need-to-know basis within NEOM, adversely affects in the NEOM environment: - NEOM's and/or third party/vendor operations and economy to a contained extent, - Functionalities of assets with limited financial loss, - Individuals' interests, - The environment and/or natural resources causing contained damage in the short-term.	1. Employee's salary information 2. Information related to products under manufacturing, which may damage fair competition. Moreover, results of practical research and studies before publication thereof 3. Documents such as tactical level plans, marketing programs prior to public release, technology innovation plans 4. Accounting data and internal financial reports 5. Passwords and PIN codes / VPN tokens of internal users 6. Design & implementation details of security systems (firewalls, access control, network diagrams, etc.) 7. Internal Communications/Memos for specific teams 8. Personally Identifiable Information (PII) such as address, social security numbers, phone numbers, license numbers, and Special Category status information of NEOM
	Confidential Internal Specific (CI – Sn)	Unauthorized access to or disclosure of such data or its content, which can only be shared on a need-to-know basis within specific sectors, adversely affects in the NEOM environment: - NEOM's and/or third party/vendor operations and economy to a contained extent,	1. Information related to products under manufacturing, which may damage fair competition. Moreover, results of practical research and studies before publication thereof 2. Documents such as tactical level plans, marketing programs prior to

		- Functionalities of assets with limited financial loss, - Individuals' interests, - The environment and/or natural resources causing contained damage in the short-term	public release, technology innovation plans 3. Accounting data and internal financial reports 4. Passwords and PIN codes / VPN tokens of sector specific software's 5. Design & implementation details of security systems (firewalls, access control, network diagrams, etc.) 6. Internal Communications / Memos for specific sectors
INTERNAL (I)		Unauthorized access to or disclosure of such data or its content, which can be shared without restriction within NEOM, minimally affects: - NEOM's operations, economy, and assets, with insignificant financial loss, - The interest of internal NEOM users' interests, - The environment and/or natural resources.	1. Training material 2. Policies, procedures, and standards 3. Staff circulars 4. Internal Communications/Memos for general use

PUBLIC (P)	Unauthorized access to or disclosure of such data or its content has no impact on: - Interest, economy, assets, reputation of NEOM, - Individuals, - Environment.	1. NEOM's strategic trends 2. NEOM's statistics on population, environment, businesses by industry etc. 3. Public development, economic studies and financial results 4. Information on public services provided to citizens 5. NEOM's contact persons 6. Advertisement for job postings 7. Public Announcements 8. Press releases 9. Product presentations for the public 10. Public relations information 11. Information on NEOM's webpage

Table 5 Data Classification Scheme

The above table of data classification scheme can be found in **Annex 8.1 – Data Classification Scheme**.

4.3. DATA IMPACT ANALYSIS

In conjunction with the Data Classification Scheme described earlier, the Data Owner must closely employ the Data Impact Analysis matrix in order to ensure that data within its sector is appropriately classified.

The matrix defines and establishes the effects that the loss of confidentiality, integrity, and availability of data from a specific classification level has on different impact categories. Its goal is to exemplify the impact that potential breaches to data classified at a specific level would have.

For NEOM, the data impact analysis develops across three dimensions: the classification level, a macro area of impact, and specific impact categories.

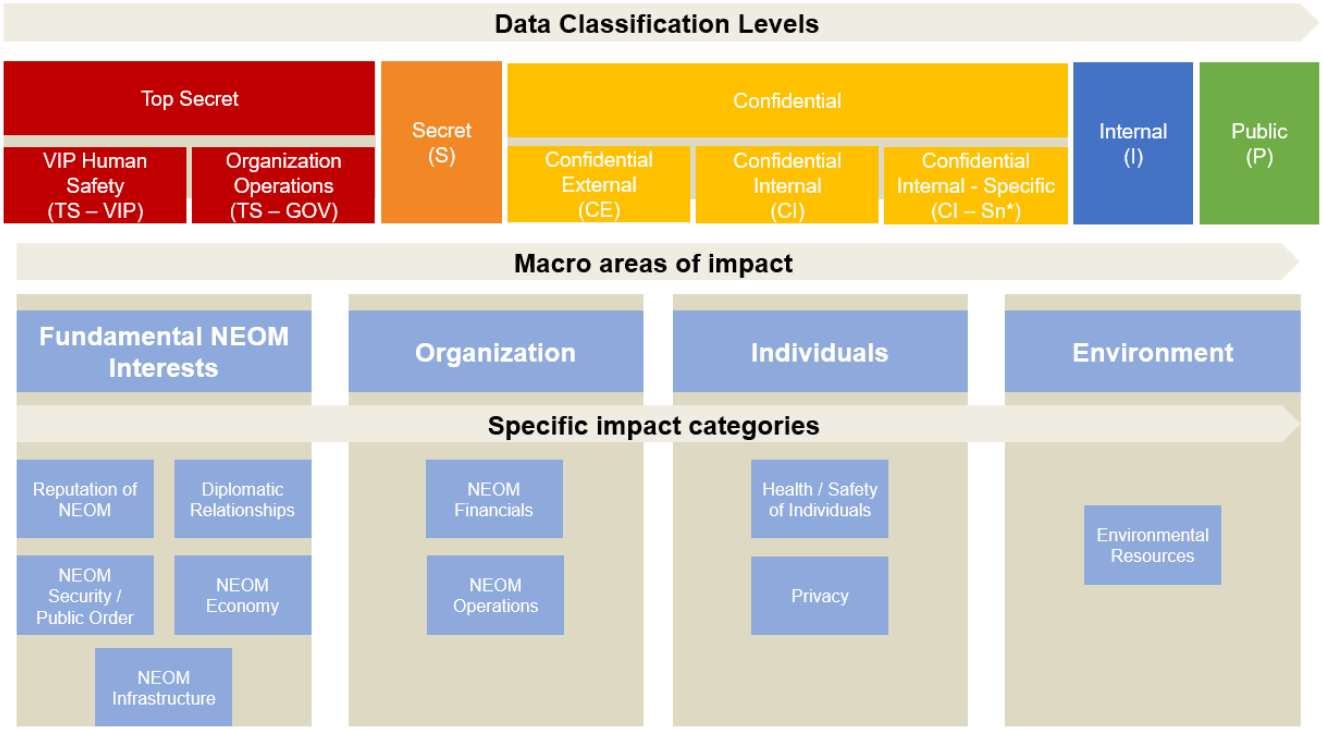

Figure 3 Data Classification Levels & Affected Areas

The impact level or severity decreases consistently with the decrease of the classification level attributed to the data, therefore – for example – the effect that the disclosure of Top Secret data is of the highest intensity (hereby rereferred to as causing adversely and expectation effects) all the way to the disclosure of public data which is considered as having no effect.

Following the detailed Data Impact Matrix:

	Top Secret		Secret (S)
	VIP Human Safety (TS – VIP)	Government / Organization Operations (TS – GOV)	
Impact Categories	Fundamental NEOM Interests		
Reputation of NEOM	Reputation beyond NEOM's environment is adversely and exceptionally affected. National and international media coverage is expected. Reputation within NEOM's environment is adversely and exceptionally affected. General loss of confidence and credibility by stakeholders and partners.		Reputation beyond NEOM's environment is severely affected and a national and / or an international media coverage is expected. Reputation within NEOM's environment is severely affected. Loss of confidence and credibility by stakeholders and partners.
Diplomatic Relationships	The diplomatic relationships of NEOM are adversely and exceptionally affected even with friendly countries in the long term. General loss of confidence and credibility which affects NEOM's ability to participate in international / diplomatic cooperation with potentially restrictive measures / sanctions.		The diplomatic relationships of NEOM are severely affected potentially even with friendly countries in the long term. Substantial loss of confidence and credibility which might affects NEOM's ability to participate in international / diplomatic cooperation with potentially restrictive measures / sanctions.
NEOM Security / Public Order	NEOM's security is adversely and exceptionally affected. Moreover, a disarray of NEOM's public order is to be expected. Emergencies response mechanism of NEOM are affected and interrupted (defence mechanism, intelligence bodies, emergency response agencies, etc.		NEOM's security is severely affected. Moreover, a disarray of NEOM's public order is to be expected. Emergencies response mechanism of NEOM are affected and potentially interrupted (defence mechanism, intelligence bodies, emergency response agencies, etc.).

NEOM Economy	Long-term unrecoverable adverse effects on the economy of NEOM (employment rate, inflation rate, GDP, etc.). All economic sectors are gravely affected.	Long-term recoverable severe effects on the economy of NEOM (employment rate, inflation rate, GDP, etc.). Several economic sectors / divisions are severely affected.
NEOM Infrastructure	Failure and long interruption of NEOM's critical infrastructure assets and operations. The failure occurs across all sectors and normal functioning cannot be easily restored. Critical vulnerabilities in the premises, services, information systems and infrastructure of the organization are exposed.	Failure and long interruption of NEOM's critical infrastructure assets and operations. The failure occurs on several sectors and normal functioning cannot be easily restored. Critical vulnerabilities in the premises, services, information systems and infrastructure of the organization are exposed.
Organization		
NEOM Financials	NEOM's financial standing is adversely and substantially affected, causing damage to the entities interest and financial reserves which may lead to the collapse of the economy.	NEOM's financial standing is severely affected, causing damage to the entities interest and heavy financial loss which may lead to bankruptcy.
NEOM Operations	NEOM's operations are adversely and substantially damaged. This damage causes a massive degradation/loss of organizational capability, to the extent that NEOM's sectors are no longer able to perform their functions. Moreover, there is a major and sustained disruption to the delivery of critical company services.	NEOM's operations are severely affected. This damage causes a severe degradation/loss of organizational capability, to the extent that localized sectors are no longer able to perform their functions and there is a loss of competitiveness.
Individuals		
Health / Safety of Individuals	The health and safety of individuals in NEOM is adversely and exceptionally affected. There are risks to human life that could reasonable be excepted, such as discrimination, mistreatment, humiliation or undermining people’s dignity or safety. Moreover, a breakdown of social cohesion will occur.	The health and safety of individuals in NEOM is severely affected. There are risks to human life that could reasonable be excepted, such as discrimination, mistreatment, humiliation or undermining people’s dignity or safety.

Privacy	The privacy of NEOM's high-level executives is adversely and exceptionally affected. Personal data of individuals have been disclosed resulting in invasion of privacy and resulting in non-compliance to data privacy regulations.	The privacy of NEOM's executives is adversely and exceptionally affected. Personal data of individuals have been disclosed resulting in invasion of privacy and resulting in non-compliance to data privacy regulations.
Environment		
Environmental Resources	The environmental resources are adversely and exceptionally affected. The effects are persistent and severe over a large area, and there is a direct effect on the supply of critical natural resources needed for the operations of NEOM's functions. Environmental recovery is not possible.	The environmental resources are severely affected. The effects are persistent and major over a large area, and there is a direct effect on the supply of critical natural resources needed for the operations of NEOM's functions. Environmental recovery would require extensive financial resources.

	Confidential		
	Confidential External (CE)	**Confidential Internal (CI)**	**Confidential Internal – Specific (CI – Sn)**
Impact Categories	**Fundamental NEOM Interests**		
Reputation of NEOM	Reputation is affected particularly beyond NEOM's environment. Loss of confidence and credibility by stakeholders and partners is expected.	Reputation is affected particularly within NEOM's environment, also at a local level. Loss of confidence and credibility by stakeholders and partners is expected.	
Diplomatic Relationships	Diplomatic relationships are affected with potentially negative consequences.		
NEOM Security / Public Order	NEOM's security is affected, and its efficiency is impaired. The emergency response mechanisms of NEOM (defence mechanism, intelligence bodies, emergency response agencies, etc.) are obstructed and under-functioning.		

NEOM Economy	Effects on the economy of NEOM (employment rate, inflation rate, GDP, etc.) with a quick recoverable decrease in the GDP. Several economic sectors / divisions might be impaired.
NEOM Infrastructure	NEOM's infrastructure, critical and non, will suffer from failures and short interruptions. The effects are localized to certain sectors. Minor vulnerabilities in the premises, services, information systems and infrastructure of the organization are exposed.
Organization	
NEOM Financials	NEOM's financial standing is affected, causing limited financial loss within a single organizational sector.
NEOM Operations	NEOM's operations are severely affected. This damage causes the degradation/loss of organizational capability, to the extent that localized departments are no longer able to perform their primary functions.
Individuals	
Health / Safety of Individuals	The health and safety of individuals in NEOM is affected. There are limited risks to human life that could reasonable be excepted.
Privacy	The privacy of NEOM's vendors is adversely and exceptionally affected. Disclosure of personal data of individuals and invasion of privacy results in non-compliance with data privacy regulations.
Environment	
Environmental Resources	The environmental resources are affected in a long term yet localized manner. There is a temporary direct effect on the supply of critical natural resources needed for the operations of NEOM's functions. Environmental recovery is possible as the effect is confined.

	Internal (I)	**Public (P)**
Impact Categories	**Fundamental NEOM Interests**	
Reputation of NEOM	Reputation and confidence beyond and within NEOM's environment may be lightly and temporarily affected.	Reputation is not affected.

Diplomatic Relationships	Diplomatic relationships may be lightly and temporarily affected.	No effect on diplomatic relationships.
NEOM Security / Public Order	NEOM's security and / or public order may be lightly and temporarily affected and only minor complications to the emergency response mechanisms shall be expect	No effect on NEOM's security and / or public order.
NEOM Economy	NEOM's economy and sectors may be lightly and temporarily affected.	No effect on NEOM's economy.
NEOM Infrastructure	NEOM's non-critical infrastructure may be lightly and temporarily affected.	No effect on NEOM's infrastructure.
Organization		
NEOM Financials	NEOM's financial standing may be lightly and temporarily affected.	No effect on NEOM's financial standing.
NEOM Operations	NEOM's operations are minimally affected. This causes a limited loss of organizational capability, to the extent that localized departments are no longer able to perform their primary functions for a brief amount of time and with limited noticeable effects.	No effect on NEOM's functions.
Individuals		
Health / Safety of Individuals	The health and safety of individuals may be lightly and temporarily affected.	No effect on the health and safety of individuals.
Privacy	The privacy of the individuals of NEOM may be lightly and temporarily affected.	No effect on the privacy of individuals.
Environment		
Environmental Resources	The environmental resources of NEOM may be lightly and temporarily affected, but environmental recovery is promptly foreseen.	No effect on the environmental resources.

Table 6 Data Impact Analysis

The above table of Data Impact Analysis can be found in **Annex 8.2 – Data Impact Analysis Matrix**

5. DATA HANDLING

5.1. DATA LIFECYCLE STAGES

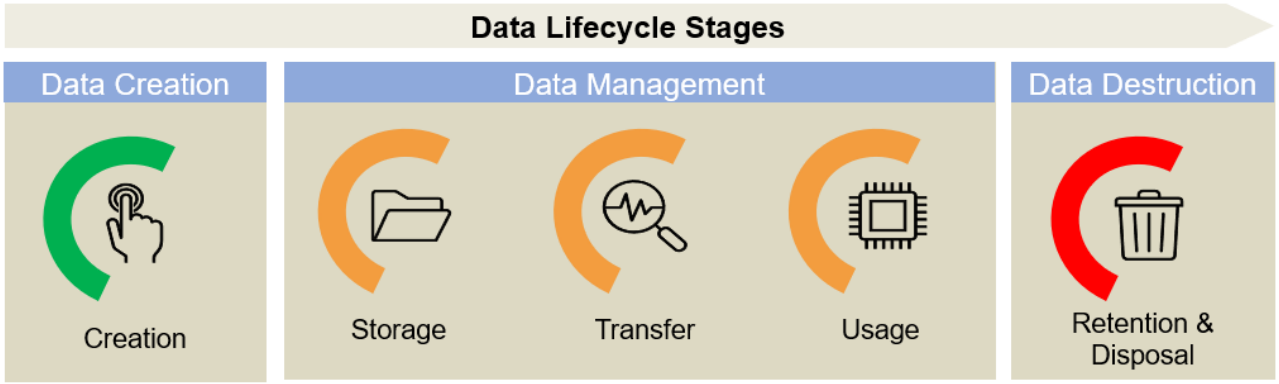

Figure 4 Data Lifecycle Stages

Creation

The first stage is referred to as “Creation”. The sources of data are abundant - structured and unstructured data are continuously being created by users, devices, applications, and IoT devices among other means. For example, users continuously create data from web and mobile applications, forms and surveys. Considering that a large amount of data produced in a myriad of different ways, it is important to ensure its appropriately managed guaranteeing that the least amount of it gets lost, mishandled, or corrupted.

Therefore, the data creation stage consists of data capture and acquisition. At this stage, the data types are defined, specifying where they are used, what they are used for, and who can use them. Moreover, at this point also the sensitivity of the created data is identified considering the data classification scheme level of Top Secret, Secret, Confidential, Internal or Public.

Storage

Following there is the “Storage” stage. Data must be stored in a stable environment and properly maintained to ensure its integrity, security and protection. During this phase, the data are typically processed in some way, such as being encrypted, compressed, cleansed or transformed. This phase also ensures that systems are in place to guarantee availability and reliability and to implement redundancy and disaster recovery.

Data can also differ in the way they are structured, which has implications on the type of data storage that a company uses. Once the type of storage is identified for the data source, the infrastructure can be evaluated for any security vulnerabilities and the data can undergo different types of data processing, such as data encryption and data transformation, to safeguard organization from malicious actors. This type of data munging also ensures

sensitive data meet the privacy and governmental requirements for governmental policies, like, Personal Data Protection Law, NDMO, NCA, GDPR, etc., by allowing businesses to avoid any costly fines deriving from violation of these types of regulations and legislations.

Transfer

The “Transfer” stage is regarding the data flow between departments, business units and external stakeholders or third parties that collaborate within or with NEOM. Data are not generated, created or edited to be present only within the same environment, but rather to be consistently shared and moved. In an interconnected word, where everything are data and connection between them, or dependencies upon them, the need of transfer is of high importance. Therefore, this stage must be executed in an appropriate manner, with all the required controls enforced to protect data. There are different classification levels that NEOM has implemented and categorized its data and as a result, all data must adhere to the protection measures that have been defined. In addition, except from the classification levels, another important factor that must be taken into consideration, is the access rights and the assigned roles of the users. As a result, based on classification level and user’s access rights and role, the following table represents the minimum requirements for both electronic and physical data that must be followed to transfer data effectively and securely within NEOM or with external bodies and stakeholder or contractors / third parties.

Usage

Most notable is the “Usage” stage. Data are valuable only if authorized users can work with them as needed to carry out their day-to-day operations. During this phase, users access and modify data as needed and carry out other data-related operations, such as collaboration, business intelligence, etc. Data usage can also result in additional data being created, which must then be stored and perhaps further processed. In effect, this phase is the enabler for authorized users to perform their tasks.

Additionally, data usage is not necessarily restricted to internal use only. For example, externals may be required to receive data for purposes such as marketing analytics, collaboration, or internal business units, etc.

Retention and Disposal

Lastly, there is the “Retention and Disposal” stage. Data must only be kept for as long as required to meet operational, business and legal needs. It is a legal requirement established by various national and international legal and regulatory Frameworks / regulations (e.g., Personal Data Protection Law, NDMO, NCA, GDPR, CEPA, PCI DSS, etc.) to only retain data, and especially data containing personal information, for as long as it is strictly necessary, since NEOM can be subject to enforcement action for failing to comply. By having clearly defined guidelines for the data retention, NEOM must demonstrate corporate responsibility and compliance in the management of its data.

NEOM’s data must be retained as per the following requirements:

- Data must be stored and archived in a suitable format to retain quality, relevance, accessibility, durability and reliability. Any transfer to another format must have due regard to retaining these qualities,
- Data must be kept securely to ensure the confidentiality and importance of the content, being protected from unauthorised or unlawful disclosure,
- Data must be accessible and retrievable as required to support business efficiency and continuity,
- Data must be retained or disposed in compliance with the Data Retention Schedule (refer to chapter 5.4),
- Data retention periods must be reviewed at least quarterly by Data Owners,
- Data must be subject to clearly defined arrangements for appraisal to select those worthy of permanent preservation (e.g., data of historical significance for NEOM),
- Data retention must be decided during the initial use / storage of data,
- Data must undergo appropriate destruction when no longer required, in an organised, efficient, timely and secure manner based on their classification level.

NEOM's data retention period must be defined based on the following criteria:

- Any legal requirements indicating specific mandates for the retention period of specific data types (e.g., trade law, tax law, employment law, etc.),
- Any legislation, regulation or Framework, indicating specific mandates for the retention period of personal data (e.g., Personal Data Law, NDMO, NCA, GDPR, CEPA, PCI DSS, etc.),
- Any local laws mandating specific retention period of data in general (e.g., NDMO),
- NEOM's business and sectorial needs and requirements,
- Necessity of crucial data's retention that will support NEOM's business continuity process,
- Data classification level.

Data owners must agree on the retention periods which they are responsible for, by using the Data Retention Schedule. Retention periods of data must be reviewed at least quarterly to determine whether any retention periods changes have occurred. Once the retention period has expired, relevant action must be taken.

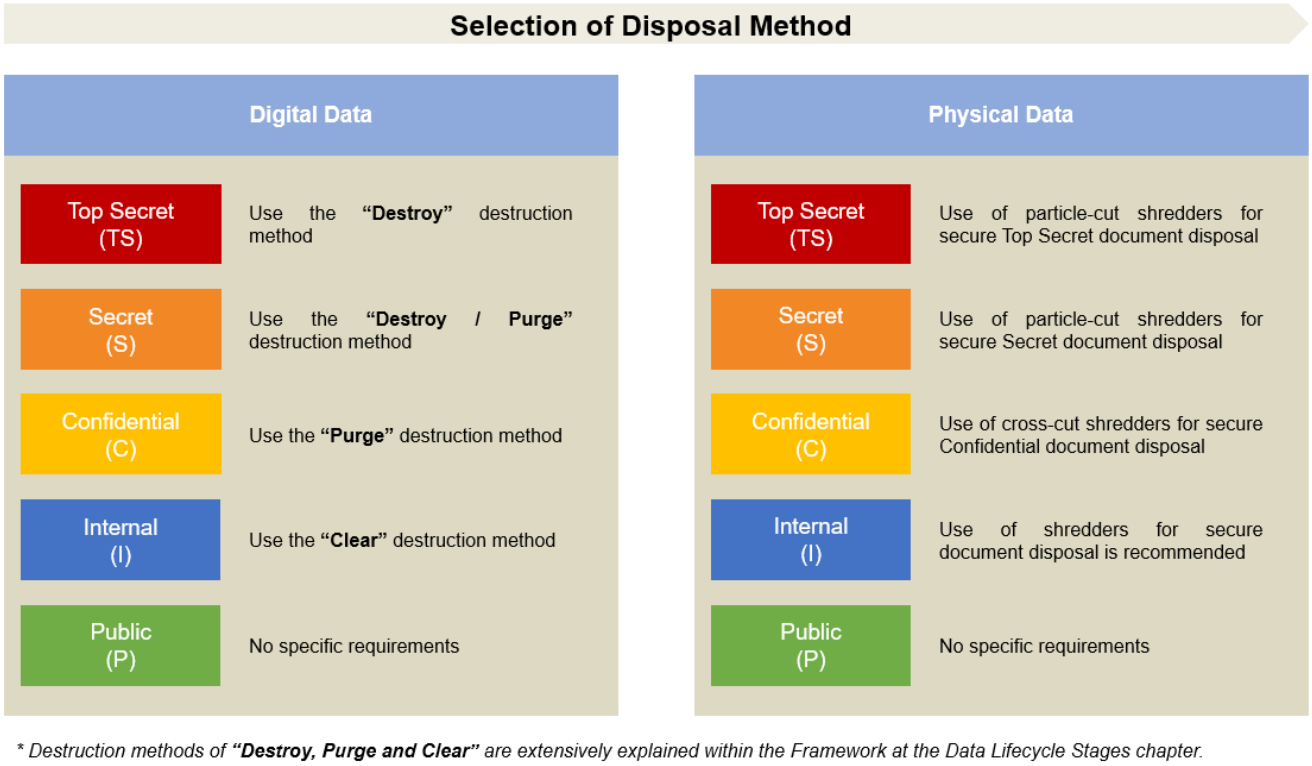

Figure 5 Disposal Method Selection

The last of the key fundamental phases within each data's lifecycle is the disposal phase. During disposal, it is examined the validity of the set retention period, and by the time that the retention period change to a non-valid period, the disposal phase is initiated. Hence, when data reach the end of their retention period, actions must be taken from their data owners and the appropriate interconnected NEOM's business units, to initiate the data disposal operation. In addition, after the expiration of the applicable retention period, personal data do not necessarily have to be completely erased. It is sufficient to anonymise the data. This can be achieved by:

- Erasing the unique identifiers which allow the identification of a unique person,
- Erasing single pieces of information that identify the data subject (whether alone or in combination with other pieces of information),
- Separating personal data from non-identifying information (e.g., an order number from the customer's name and address),
- Aggregating personal data in a way that no identification of any individual is possible.

The data owners are responsible for ensuring that data are disposed in a timely and secure manner, and that the Data Management Office is aware that the destruction phase is taking place. All data copies, including security copies, and backup copies held in any format must be destroyed at the same time, after data's retention period ending.

In addition, destruction of physical data must be carried out in a way that takes full account of the data's confidentiality using the data classification scheme of NEOM, as displayed above. With respect to the destruction of electronic data, it is vital that all the various locations that a file could be stored have been considered. The destruction of an electronic data occurs via the usage of specific and dedicated software such as file erasers, file shredders, etc. and based on the required measures that needs to be taken based on data's classification level. Destruction of an electronic file includes the destruction of all backups. Data may be stored indicatively (not exhaustive list) within:

- NEOM's shared folders, on premise, cloud repositories, and servers, etc.,
- NEOM's employees' mobile devices,
- NEOM's databases,
- Potential cloud suppliers (externals) whose services are provided to NEOM,
- Emails and email attachments,
- NEOM's employee's devices such as laptops, desktops, hard drives, and removable media.

Physical data must also be safely disposed after the end of their retention period. Based on their classification level, physical data must be deleted securely via the usage of appropriate shredders per case and classification level or by utilizing a third-party to handle the destruction phase of the physical data.

When data reach end-of-life, they must be permanently deleted, but it must be done securely and without violating applicable data protection regulations. In this final stage of the data lifecycle stages, data is purged from the records and destroyed securely.

Data destruction encompasses a wide variety of media, including electronic and paper records. The choice of destruction method must be based on the risk posed by the sensitivity of the data being destroyed and the potential impact of unauthorized disclosure.

There are three fundamentals destruction categories that are applicable to digital data:

- **Clear -** A method of destruction that applies software-based techniques to clear data in all user-addressable storage locations, typically by executing read and write commands to the storage device.
- **Purge -** A method of destruction that applies logical techniques to purge data and render target data recovery infeasible by using media degaussing techniques. Physical techniques can also be used.
- **Destroy -** A method of destruction that renders target data recovery infeasible by using data storage media physical destruction that results in the subsequent inability of data storage media usage.

In addition, data owners within NEOM must be cautious when dispose data and when granting data access to external and third parties. No matter which method of destruction data owners will choose, they must consider the following recommended best practices for data destruction, especially when the data include PII and sensitive personal data:

- When drafting written agreements with third parties, include provisions that specify that all PII that was provided to the third party must be destroyed when no longer needed for the specific purpose for which it was provided, including any copies of the PII that may reside in system backups, temporary files, or other storage media.
- Ensure accountability for destruction of PII by using certification forms which are signed by the individual responsible for performing the destruction and contain detailed information about the destruction.
- Remember that PII may also be present in physical data. NEOM must manage physical data in a similar fashion to its data. When data are no longer required, destroy physical data by using secure means to render it safe for disposal or recycling. Commonly used methods include cross-cut shredders, pulverisers, and incinerators.
- When destroying data, use appropriate data deletion methods to ensure that data cannot be recovered. Please note that simple deletion of the data is not effective. Often, when a data file is deleted, only the reference to that file is removed from the media. The actual data file remain on the disk and are available for recovery until overwritten. Collaboration with the IT department is required to ensure proper deletion of records consistent with technology best practice standards.
- Avoid using file deletion, disk formatting, and “one way” encryption to dispose sensitive data – these methods are not effective because they leave most of the data intact and vulnerable to being retrieved by a determined person with the right tools.
- Address in a timely manner sanitization of storage media which might have failed and need to be replaced under warranty or service contract. Many data breaches result from storage media containing sensitive information being returned to the manufacturer for service or replacement.

5.2. DATA HANDLING CONTROL MATRIX

NEOM must ensure that all data sources processed by its employees or authorized third parties are adequately protected at all times against unauthorized access, disclosure, modification and / or loss. For this purpose, NEOM has defined and must implement certain baseline data controls specific to each data classification level, in order for all data to receive a level of security that is proportionate to its value. Therefore, the data handling controls have been developed by taking into consideration the following two dimensions: the data classification levels (as described in chapter 4.2.) and the data lifecycle stages (as described in chapter 5.1).

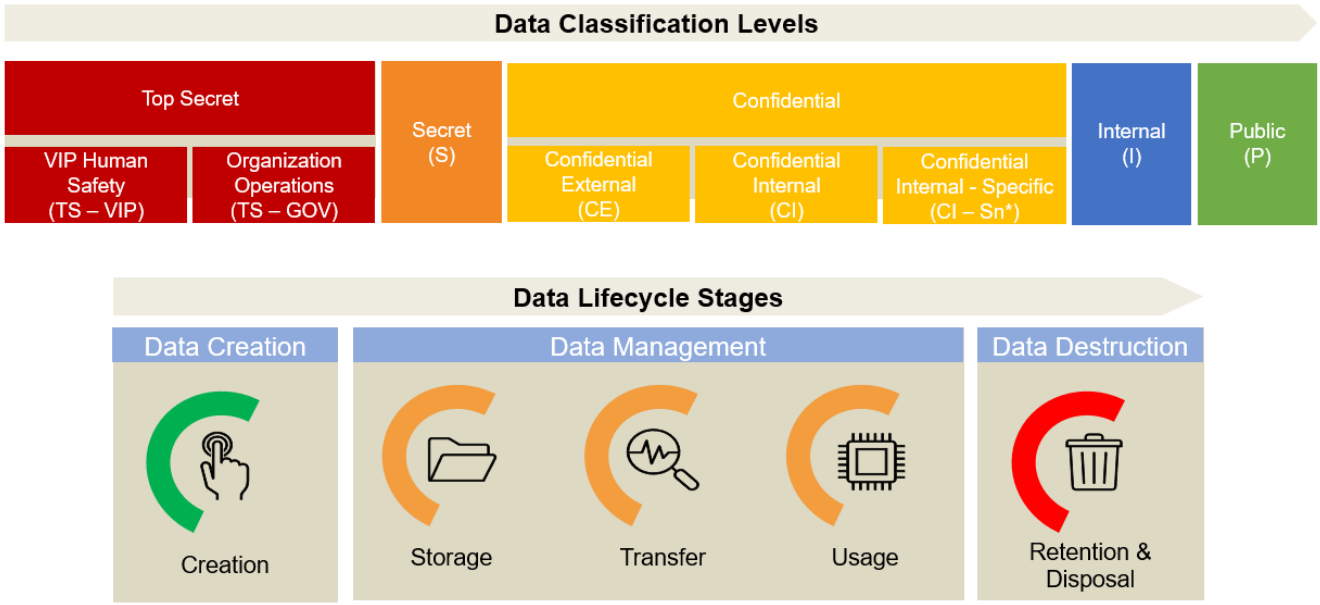

Figure 6 Classification Levels & Lifecycle Stages

The data controls are technical and organizational in nature and aim at identifying, at a minimum, the practices and measures that a data source of a specific type, with a specific classification level, and at a specific point in its lifecycle, must follow in order for it to be adequately protected. These controls are detective (e.g., alerting mechanism for logical access violation), preventive (e.g., DLP implementation), corrective (e.g., access rights removal and re assignment after a predefined period of time [indicatively 6 months]) and deterrent (e.g., penalties and disciplinary actions for employees and external third parties who violate NEOM's policies / procedures) measures aimed at reducing and avoiding the likelihood of a potential impact derived from a specific event or action occurred against a data source. Controls and measures must not be interpreted independently but rather than a layered approach of security to sufficiently protect all aspects of a data source.

The data handling controls are determined according to the defined classification level that must be applied to data sources throughout their lifecycle, regardless of the type of data, with no exception. However, the controls stand as a guidance and are therefore non-exhaustive. The final set of implemented controls are to be defined on a case-by-case manner. In fact, the defined controls are baseline requirements that must not be taken at face value,

but rather that serve as a starting point on which to further add controls after an ad-hoc additional evaluation of the specific data source.

The data handling controls are not static and will often reviewed and assessed to maintain their relevance for the protection of the specific data source. The review must be performed by the Data Owner along the eGRC involved to consult on the relevant controls to be implemented for the protection of data. On the other hand, the security and IT administrators are responsible for the implementation and monitoring of the operational effectiveness of the defined controls, which are checks that must be periodically performed via, for example, penetration tests and / or vulnerability assessments (internally and via independent third parties).

The set of data handling controls defined for each different data classification level indicatively includes:

- Controls to protect data at rest (stored), which refer to controls that safeguard data that are at an inactive state (i.e., not in use or in transit [transfer]),
- Controls to protect data in transit, which refer to controls that safeguard data that are transferred through various means (e.g., via e-mail, via an SFTP server etc.),
- Controls to protect data in use, which refer to controls that safeguard data that are actively accessed, used and modified (read, edited etc.) by an authorized individual (employee or third party),
- Controls to facilitate data disposal, which refer to controls that ensure that data will be deleted and into an irrecoverable state after their destruction / deletion.

In other words, data handling controls have been defined for all the data life cycle stages in the following way:

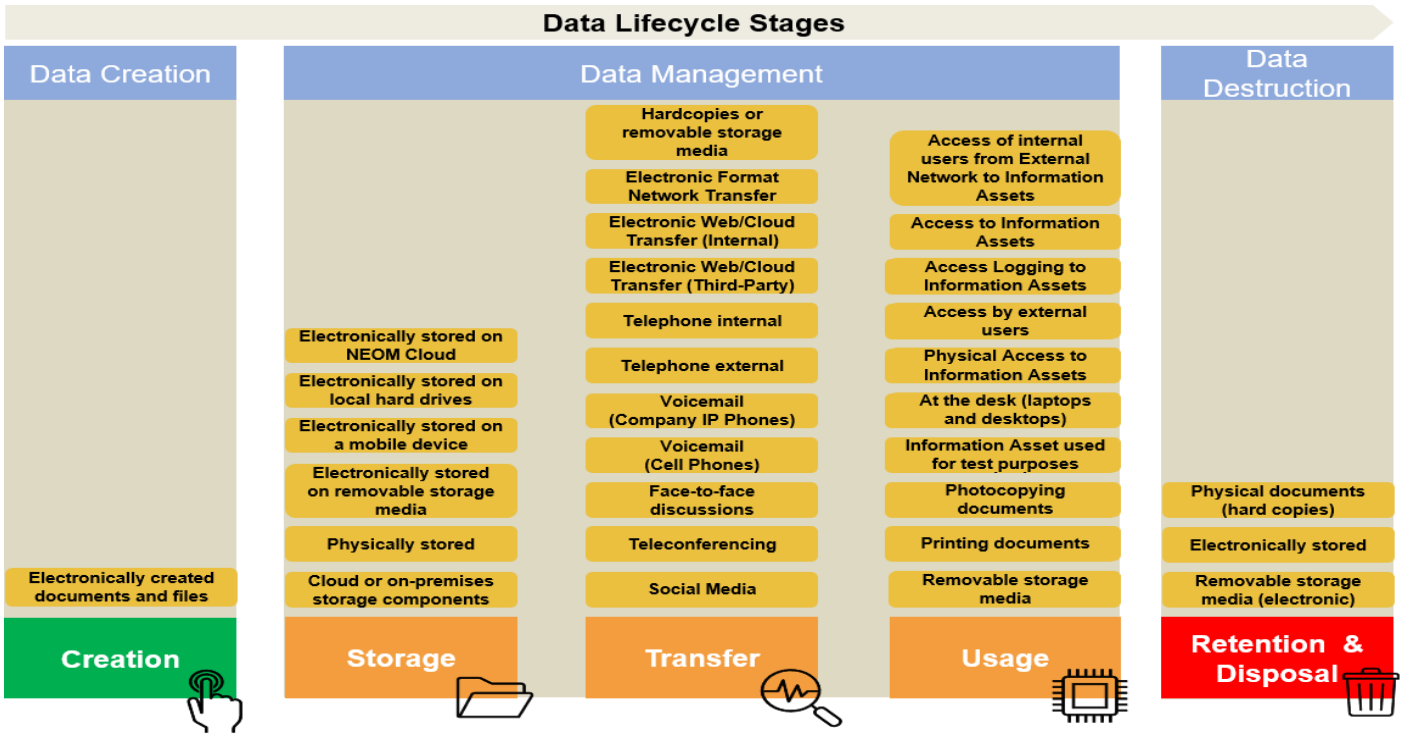

Figure 7 Data Lifecycle Stages & Handling Cases

In summary, NEOM's data handling controls are illustrated in the following table - The complete Data Handling Matrix is depicted in **Annex 8.3 – Data Handling Matrix**. This is a reference document that includes the full version of the above summary table:

Classification Levels (Sub - Level)		Electronic Data	Physical Data
TOP SECRET	VIP Human Safety (TS – VIP)	***Data at rest*** Double encryption for NEOM cloud premises where data reside No local disk storage is allowed No mobile storage is allowed No removable media storage is allowed Data access controls enforcement Data labelling or tagging mechanism enforcement ***Data in transit*** No transfer outside NEOM is allowed (unless specific approval is granted and only to authorised recipients) Transmission only through encrypted channels following approval Use only of encrypted and labelling enabled removable media Data Loss Prevention solution E-mail encryption and "Do not Forward" functionality via DLP Automated generation of violation alerts of implemented security controls No third-party unsanctioned apps are allowed	***Data at rest*** Clear-desk policy Storage in locked cabinets Labelling ("Top Secret") in each document page Documents stored in restricted areas (physical security zone segmentation) / areas where access cards are required to enter, CCTV is implemented and logs from access cards are kept ***Data in transit*** Documents in sealed envelopes No transfer outside NEOM is allowed (unless specific approval is granted for authorised recipients) Documents to be sent only by authorised personnel and delivered directly to the intended recipient ***Data in use*** No copying / scanning allowed (unless specific approval granted)

	Government / Organizations Operations (TS – GOV)	***Data in use*** Limited access to authorized employees based on the "Need-to-Know" principle Disallow printing (unless specific approval from Senior Management is granted) Only use printers with access control capabilities (e.g., access card) Employees authorized to access **Top Secret** data must sign a non-disclosure agreement (NDA) Log all events and monitor all activities via SIEM Access to external users is not permitted Access to internal users from external network is not permitted ***Data disposal*** Secure disposal ensuring data are not recoverable	Employees authorized to access **Top Secret** data must sign a non-disclosure agreement (NDA) ***Data disposal*** Use of particle-cut shredders for secure **Top Secret** document disposal

SECRET	***Data at rest*** Double encryption for NEOM cloud premises where data reside No local disk storage is allowed Personal or NEOM mobile device storage is allowed only with MDM or MAM enforcement Removable media storage is allowed only for encrypted and password protected media Data access controls enforcement Data labelling or tagging mechanism enforcement ***Data in transit*** No transfer outside NEOM is allowed (unless specific approval is granted and only to authorised recipients) Transmission only through encrypted channels following approval Use only of encrypted and labelling enabled removable media Data Loss Prevention solution E-mail encryption and “Do not Forward” functionality via DLP Automated generation of violation alerts of implemented security controls No third-party unsanctioned apps are allowed	***Data at rest*** Clear-desk policy Storage in locked cabinets Labelling (“Secret”) in each document page Documents stored in restricted areas (physical security zone segmentation) / areas where access cards are required to enter, CCTV is implemented and logs from access cards are kept ***Data in transit*** Documents in sealed envelopes No transfer outside NEOM is allowed (unless specific approval is granted for authorised recipients) Documents to be sent only by authorised personnel and delivered directly to the intended recipient ***Data in use*** No copying / scanning allowed (unless specific approval granted) Employees authorized to access **Secret** data must sign a non-disclosure agreement (NDA) ***Data disposal*** Use of particle-cut shredders for secure **Secret** document disposal

		Data in use Limited access to authorized employees based on the “Need-to-Know” principle Disallow printing (unless specific approval from Senior Management is granted) Only use printers with access control capabilities (e.g., access card) Employees authorized to access **Secret** data must sign a non-disclosure agreement (NDA) Log all events and monitor all activities via SIEM Access to external users is not permitted Access to internal users from external network is not permitted ***Data disposal*** Secure disposal ensuring data are not recoverable	
CONFIDENTIAL	**Confidential External (CE)**	***Data at rest*** Encryption for NEOM cloud premises where data reside Local disk storage is allowed only to encrypted and labelled disks	***Data at rest*** Clear-desk policy Storage in locked cabinets Labelling (“Confidential”) in each document page Physical Access where hard copies are located shall be strictly controlled

	Confidential Internal (CI – N)	Personal or NEOM mobile device storage is allowed only with MDM or MAM enforcement Removable media storage is allowed only for encrypted and password protected media Data access controls enforcement Data labelling or tagging mechanism enforcement ***Data in transit*** Transfer outside NEOM is allowed only with granted approval Transmission only through encrypted channels following approval	***Data in transit*** Documents in sealed envelopes No transfer outside NEOM is allowed (unless specific approval is granted for authorised recipients) Documents to be sent only by authorised personnel or courier service ***Data in use*** No copying / scanning allowed (unless specific approval granted) Employees authorized to access **Confidential** data should sign a non-disclosure agreement (NDA) ***Data disposal*** Use of cross-cut shredders for secure **Confidential** document disposal
	Confidential Internal Specific (CI – Sn*)	Use only of encrypted and labelling enabled removable media Data Loss Prevention solution Third-party unsanctioned apps require approval and encryption enforced ***Data in use*** Limited access to authorized employees based on the “Need-to-Know” principle Log all events and monitor all activities via SIEM Access to external users is not permitted (unless specific approval is granted) Access to internal users from external network is not permitted without the usage of VPN and MFA Printing should be allowed only with specific approval	

		Only use printers with access control capabilities (e.g., access card) Employees authorized to access **Confidential** data should sign a non-disclosure agreement (NDA) ***Data disposal*** Secure disposal ensuring data are not recoverable	

INTERNAL	***Data at rest*** Encryption for NEOM cloud premises where data reside Local disk storage is allowed only to encrypted and labelled disks Personal or NEOM mobile device storage is allowed only with MDM or MAM enforcement Removable media storage is allowed only business purposes Data access controls enforcement is recommended Data labelling or tagging mechanism enforcement recommended ***Data in transit*** Transfer outside NEOM is allowed only with granted approval Transmission only through encrypted channels following approval Use only of encrypted and labelling enabled removable media Data Loss Prevention solution ***Data in use*** Log all events and monitor all activities via SIEM Access to external users is not permitted Access to internal users from external network is not permitted without the usage of VPN and MFA	***Data at rest*** Clear-desk policy Storage in locked cabinets is recommended ***Data in transit*** Transfer outside NEOM is allowed following approval and only for authorised recipients) Documents to be send by authorised personnel or courier service is recommended ***Data in use*** Copying / scanning is allowed following approval ***Data disposal*** Use of shredders for secure document disposal is recommended

	Printing shall be limited and for business purposes only ***Data disposal*** Secure disposal ensuring data are not recoverable	
PUBLIC	***Data at rest*** No specific requirements ***Data in transit*** No specific requirements ***Data in use*** No specific requirements ***Data disposal*** No specific requirements	***Data at rest*** No specific requirements ***Data in transit*** No specific requirements ***Data in use*** No specific requirements ***Data disposal*** No specific requirements

Table 7 Data Handling Control Matrix

The above table of data handling controls depict a summarized version of the controls that can be found in **Annex 8.3 – Data Handling Matrix**.

5.3. HIGH LEVEL ACCESS MATRIX

NEOM, understanding the significant challenges arising from the continuous increase in the volume of data which are processed for its business purposes, as well as the number and variety (e.g., internal, external, temporary, etc.) of users who undertake and are involved in the aforementioned processing, aims at the optimal management and access control of the users' to NEOM's resources.

In this regard, NEOM must take and follow significant actions towards the adoption of a controlled access management approach of users. Moreover, the approach significantly strengthens NEOM's ability to ensure the confidentiality, integrity, availability, and privacy of key resources and data types; therefore, it is considered of utmost importance to be included in NEOM's strategy in terms of overall security and data protection posture enhancement.

Apart from the benefits that a controlled access management approach provides in terms of enhancing security for NEOM, it also provides significant facilitators in terms of supporting business needs and ensuring potential regulatory compliance. Such elements may be identified in terms of cost reduction, efficiency enablement, fraud abuse avoidance and overall procedural standardisation of business processes and protection enhancement.

The current Framework supports and defines the adoption and optimization of users' accesses management on an organizational (user) type level and data classification level. In addition, Framework's objective is to ensure that all kind of users, access NEOM's resources and data while NEOM is appropriately handle and manage access rights based on NEOM's needs and data classification levels.

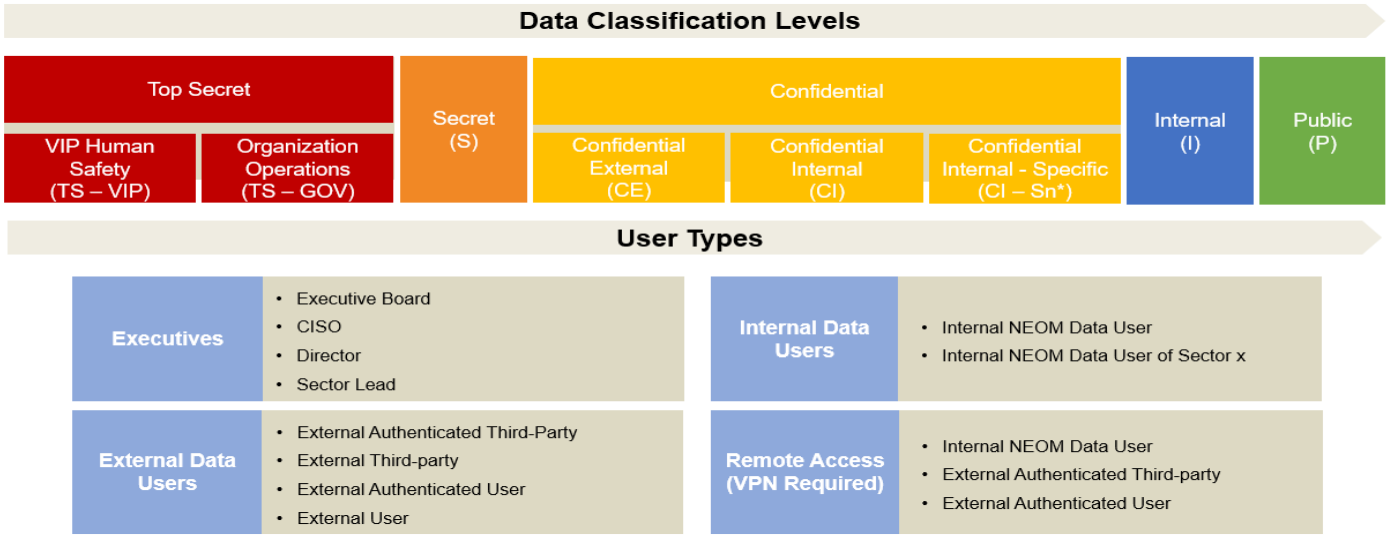

Figure 8 NEOM User Types

The scope of users' access management extends to all users within NEOM, both internal and external, along with the full extent of information systems, data, and any other resources. In **Annex 8. 6 – High Level Access Matrix** it is included the full access matrix which depicts the users, the data classification levels and the associated access rights per case.

5.4. DATA RETENTION SCHEDULE

The data retention schedule holds great importance as it defines the specific period of time according to which stored data must be kept in order to comply with industry regulations. The specified time period is defined considering the different types of data, and the schedule ultimately defines how the data are to be disposed of at the end of their life cycle.

The core idea of data retention is that data must only be maintained for as long as they are required for business needs. Storage for an indefinite period of time, leads to a constantly increasing amount of stored data which ultimately rise expenditure related to data file management. Data retention is critical for modern organizations. Without it, NEOM might continuously gather and store too much unnecessary information, which would lead to operational inefficiencies, increased costs, legal and security risks and potentially could cause legal repercussions.

Different regulations, legislation and laws, mandate different predefined periods of data retention, based on the data type, the sensitivity and the necessity of the retention. Therefore, all data must be assessed and mapped to all applicable regulations and laws to avoid fines and violations of laws, that could lead to NEOM's reputational damage or suffer a collaboration crisis with other parties.

NEOM, in order to alleviate and tackle the data retention requirement, adopts a specific data retention schedule for each data type and set the baseline rules regarding the data retention periods. For an effective retention strategy, the retention schedule cannot be the only ground rule of reference. Data owners must contribute to the data retention definition, by performing regular checks on data sources under their supervision. More specifically, data owners must perform the following checks in order to effectively update and follow the required retention period of NEOM's data, under each data owner responsibility:

- **Periodic checks at regular intervals –** Periodic checks are especially important when the retention period is long, and the classification levels are different. By performing periodic checks, data owners can ensure that the conditions affected the retention period are still appropriate, while extra attention is given to higher classification levels' (Top-Secret, Secret and Confidential) retention. Periodic checks enable data owners to timely identify lapsed retention periods and get notified with the need of disposal, especially for the highly classified data, in order to avoid any regulation / legislation violation, to protect the confidentiality of these data (which can be exposed while remaining on NEOM's premises) and prevent NEOM from any reputational damage that may occurred based on the aforementioned cases. In addition, special care must be given to personal data, a type of data further discussed in the following paragraph
- **End of life checks –** This check is to determine whether there are still business, operational or regulatory needs in place which NEOM is required to abide by, and the data retention period has to be extended. A decision to extend data's retention period can only be taken from the data owners, who are responsible for the data under their supervision, while a parallel close collaboration with all the related business units (e.g., eGRC, Legal Office, etc.) is required. In addition, any retention's period expansion needs to be well documented and must always adhere to local laws and regulations, and extra attention must be given to personal data.

Data owners must rely on the data retention schedule template and populate it with case-by-case considerations and regulatory requirements in order to avoid business or regulatory violations by creating an appropriate data retention plan. Furthermore, personal's data retention period must be created with extreme cautious. NEOM must manage its strategy ensuring compliance with the dynamic environment of national and international legal and regulatory Frameworks. These directly impact the operations of the data that NEOM handles (indicatively: Personal Data Protection Law, NDMO, NCA, Saudi Arabian Monetary Authority, PCI DSS, PSD2, etc.) and therefore must be periodically reviewed to ensure that all the applicable laws and regulations are taken into consideration in their most updated form. NEOM must also consider cases where the organization interacts, process and uses data, especially personal data, interconnected with European and other Countries, where NEOM could be liable in parallel to additional regulations and legislations (indicatively: Personal Data Protection Law, NDMO, NCA, GDPR, ECPA, CCPA, etc.) regarding the retention and disposal of that kind of data. Deviations from the predefined data retention periods will drive NEOM to liabilities and potential fines, that could harm future collaborations and national relationships.

The final required key element of the data's retention schedule is the deletion and disposal of the data. Immediately after the end of the retention period, and whether the retention period has not been suspended due to pending or actual litigation, data that have reached the end of their retention period must be destroyed in a consistent and timely manner under NEOM's responsibility and based on the data classification level, with the appropriate controls. The deletion / destruction of both electronic and physical data must be executed in an appropriate and secure manner, so that the data could not be read (based on classification level) and make it impossible to recover data, after destruction, by any technical or other means. In addition, at the end of the retention period, data must be deleted not only from any digital format that they actively exist, but also from any backup maintained by NEOM. Therefore, the disposal phase of an electronic file lifecycle, includes the destruction of all backups that contain the specified data.

An indicatively and non-exhausting retention period for data within NEOM can be found on the **Annex 8.4 – Data Retention Schedule**. As it has mentioned, different data types have different retention periods based on different regulations and legislations.

Data Types	Data Category	Personal Data Inclusion	Data Owner	Data Storage Location	Data Format	Retention Period	Retention Period Rationale

Table 8 Data Retention Schedule Template

In addition, the above visual representation of data retention schedule depicts the structure of the template that can be found in **Annex 8.4 – Data Retention Schedule Template.** The template (Excel) is attached to be used as a reference document for future data retention schedule within NEOM and NEOM's departments.

5.5. DATA INVENTORY

A data inventory is a complete record of the data sources that are stored, processed, and managed by NEOM. It allows to track all essential data sources in a streamlined and well-defined manner throughout all sectors, ensuring that the available information on all data sources is accessible and consistent.

Via the data inventory, NEOM gains an understanding regarding the types of the data that are being collected, where they are stored and how they are protected. Furthermore, this practice allows to identify potential gaps or risks and to mitigate them accordingly in order to comply with business needs and / or any local laws / regulations / legislations.

Considering the data lifecycle, and therefore understanding that new data sources are gained with time and that others get disposed of, the data inventory is not a one-off process. Quite the contrary, the data inventory must be constantly updated and maintained by the Data Owners, as they are the ones that know the data sources within their scope the best. Moreover, another challenge that may arise during the creation and maintenance of the data inventory is that the vast amount of information within NEOM, information that is handled and stored from different teams and sectors, shall be, without delay or exception, reported in the data inventory. A data inventory therefore has latent issues related to incomplete or missing information, duplicates, or inaccuracy, which can only be addressed via the training of Data Owners on the correct way of using the data inventory to perform, among other activities, data quality checks.

All in all, the advantage of having a data inventory is to ensure that NEOM has a clear understanding of the data residing within all its sectors with all relevant details relating to type of data, owners, uses, description, and retention among others. However, the data inventory can also be a major liability if not properly managed as it could host inaccurate, incomplete, or inadequate information. Therefore, NEOM must support a continuing effort to appropriately maintain a robust data inventory.

NEOM has defined a specific data inventory template to collect all the most important information regarding data sources is uses and manages.

In addition, the following visual representation of data inventory depicts the structure of the template that can be found in **Annex 8.5 – Data Inventory Template.** The template (Excel) is attached to be used as a reference document for a continually data retention scheduling exercise within NEOM and NEOM's departments.

General Information					**Data Information**				
Sector	*Data Owner*	*Data description*	*Format*	*Asset source*	*Classification Level*	*Impact Level*	*Personal Data*	*Storage location / format*	*Data Retention period*
Data Retention					**Dependencies**				
Data Retention period		*Reason / legal requirement for retention period*		*Disposal method*	*Cross border transfers*				

Table 9 Data Inventory Template

6. DATA CLASSIFICATION & PROTECTION PROCESSES AND PROCEDURES

6.1. DATA CLASSIFICATION & PROTECTION PROCESS

The following table details all the steps describing in sequential order the activities to be pursued within the Data Classification and Protection program, from the initial classification of data all the way to Its disposal.

#	Steps	Responsibility	Frequency	Chapter / Annex References
DATA CLASSIFICATION & PROTECTION PROCESS				
Step 1: Data to classify (or reclassify) has been identified				
1a	The Data Owner identifies a new data source within its sectors that requires classification. The Data Owner holds ultimate responsibility to ensure that all data is promptly classified. Such case may indicatively occur as a result of a newly introduced business process or function.	**Data Owner**	On Demand/ Annually	-
1b	The Data Owner is made aware that an existing data source within its sectors, for which he holds ultimate responsibility, must undergo reclassification. Such case may indicatively occur as a result of newly introduced business need to an existing process or function, or legal / regulatory mandates, after communication by the supporting Legal Office.	**Data Owner**	On Demand	-
Step 2: Initial Data Classification				
2a	In case of a new data source, this is temporarily considered as "*Internal*" until classified.	**Data Owner**	-	
Step 3: Data Classification and Data Impact				
3a	The Data Owner, in collaboration with the Data Custodian, must consider the classification levels and assess, considering the definitions and related examples, the appropriate classification level. - **Top Secret** – VIP Human Safety (TS – VIP) - **Top Secret** – Government / Organizations Operations (TS- GOV) - **Secret** (S) - **Confidential** – Confidential External (CE) - **Confidential** – Confidential Internal (CI) - **Confidential** – Confidential Internal Specific (CI-Sn) - **Internal** (I) - **Public** (P)	**Data Owner / Data Custodian**	On Demand/ Annually	Chapter 4.2 Data Classification Scheme Annex 8.1 Data Classification Scheme

#	Steps	Responsibility	Frequency	Chapter / Annex References
-	Once the proper classification has been attributed to the data under their ownership, the corresponding impact level is assigned to the data source, which depict the impact that the loss of confidentiality, integrity, and availability of the specific data would have on the different impact categories. The Data Custodian holds an advisory position in this matter and may be called upon by the Data Owner for support. - **Top Secret:** Critical High Level - **Secret:** High Level - **Confidential:** Medium Level - **Internal:** Low Level - **Public:** None	**Data Owner / Data Custodian**	On Demand/ Annually	Chapter 4.3 Data Impact Analysis Annex 8.2. Data Impact Analysis Matrix
3b.	The Data Owner, in collaboration with the Data Custodian, must consider the classification levels and assess, considering the definitions and related examples, the possible appropriate re-classification level. - **Top Secret** – VIP Human Safety (TS – VIP) - **Top Secret** – Government / Organizations Operations (TS- GOV) - **Secret** (S) - **Confidential** – Confidential External (CE) - **Confidential** – Confidential Internal (CI) - **Confidential** – Confidential Internal Specific (CI-Sn) - **Internal** (I) - **Public** (P) If the classification level changes, please follow to step 4. If the classification level does not change, the process comes to an end.	**Data Owner / Data Custodian**	On Demand/ Annually	Chapter 4.2 Data Classification Scheme Annex 8.1 Data Classification Scheme
Step 4: Data re-classification notification				
4	If the Data Owner, in collaboration with the Data Custodian, assessed the need of reclassification, and this involves classification lowering or the removal of the classification label, the system will generate a warning message requesting a justification to remove the label or lower its classification.	**Data Owner / Data Custodian + Automatic System Message**	-	-
Step 5: Implementation of Data Handling Controls				
5	Based on the attributed Classification Level the appropriate Data Handling Controls are enforced. These controls must be considered as protection guidelines for the entirety of the lifecycle of the specific data source.	**Data Custodian**	On Demand/ Annually	Chapter 5.2 Data Handling Control Matrix Annex 8.3 Data Handling Matrix

#	Steps	Responsibility	Frequency	Chapter / Annex References
Step 6: Data Retention periods				
6	Based on document's data type, business and legal needs, appropriate data retention period is assigned to the data	**Data Custodian**	On Demand/ Annually	Chapter 5.4 Data Retention Schedule Annex 8.4 Data Retention Schedule Template
Step 7: Data Usage				
7	While the classified data source is in use, the appropriate data handling controls must be applied to ensure it is appropriately handled	**Data Custodian**	-	Chapter 5.1 Data Lifecycle Stages
Step 8: Data Transfer				
8a	If the NEOM user is authorized to transfer the specific data source, it is permitted to proceed with the data transfer.	**Data User / Data Custodian**	-	Chapter 5.1 Data Lifecycle Stages
8b	If the NEOM user is not authorized to transfer the specific data source, they will receive a notification from the system prohibiting the transfer. In this case, the process comes to an end.	**Data User / Data Custodian**	-	Chapter 5.1 Data Lifecycle Stages
Step 9: Data Archival				
9	If the Data Source is not required to be active, it is archived until the end of retention period	**Data Custodian**	-	Chapter 5.1 Data Lifecycle Stages
RETENTION PERIOD VALIDITY				
Step 10: Review of Retention Period				
10	Whether the data sources have been already archived (step 9) or whether it is required to remain active, the validity of the retention period shall be assessed	**Data Owner / eGRC**	-	-
Step 11: Identify Data Type				
11	To pursue the review of the data retention period, it is necessary to identify the data type	**Data Owner**	-	-
Step 12: Identify Retention Period				
12	Identify the predefined retention period	**Data Owner**	-	-

#	Steps	Responsibility	Frequency	Chapter / Annex References
Step 13: Retention Period assessment				
13	If the defined retention period has not yet lapsed, the data source must be still stored. Moreover, periodic checks on the applicability of the retention period shall be performed. Execution of periodic checks will bring back to Step 12.	**Data Owner / NEOM Authority/eGRC**	-	Chapter 5.4 Data Retention Schedule Annex 8.4 Data Retention Schedule Template
DATA DISPOSAL				
Step 14: Disposal Phase				
14	When the retention period has lapsed it is necessary to proceed with the disposal phase.	**Data Owner**	-	-
Step 15: Identify Data Type				
15	To pursue the disposal of the data source, it is necessary to identify the data type	**Data Owner**	-	-
Step 16: Identify Classification Level				
16	Identify the classification level	**Data Owner**	-	-
Step 17: Disposal of data classified as Public				
17	If the data source has been classified as public, its disposal practice follows non-specific disposal practices	**Data Owner / Data Custodian**	-	Chapter 5.2 Data Handling Control Matrix Annex 8.3 Data Handling Matrix
Step 18: Disposal of data classified as non-public				
18	If the data source has been classified at any level other than public, its disposal practice follows level specific disposal practices, which must be consulted and closely followed	**Data Owner / Data Custodian**	-	Chapter 5.2 Data Handling Control Matrix Annex 8.3 Data Handling Matrix

Table 10 Data Classification & Protection Process

DATA CLASSIFICATION & PROTECTION PROCESS

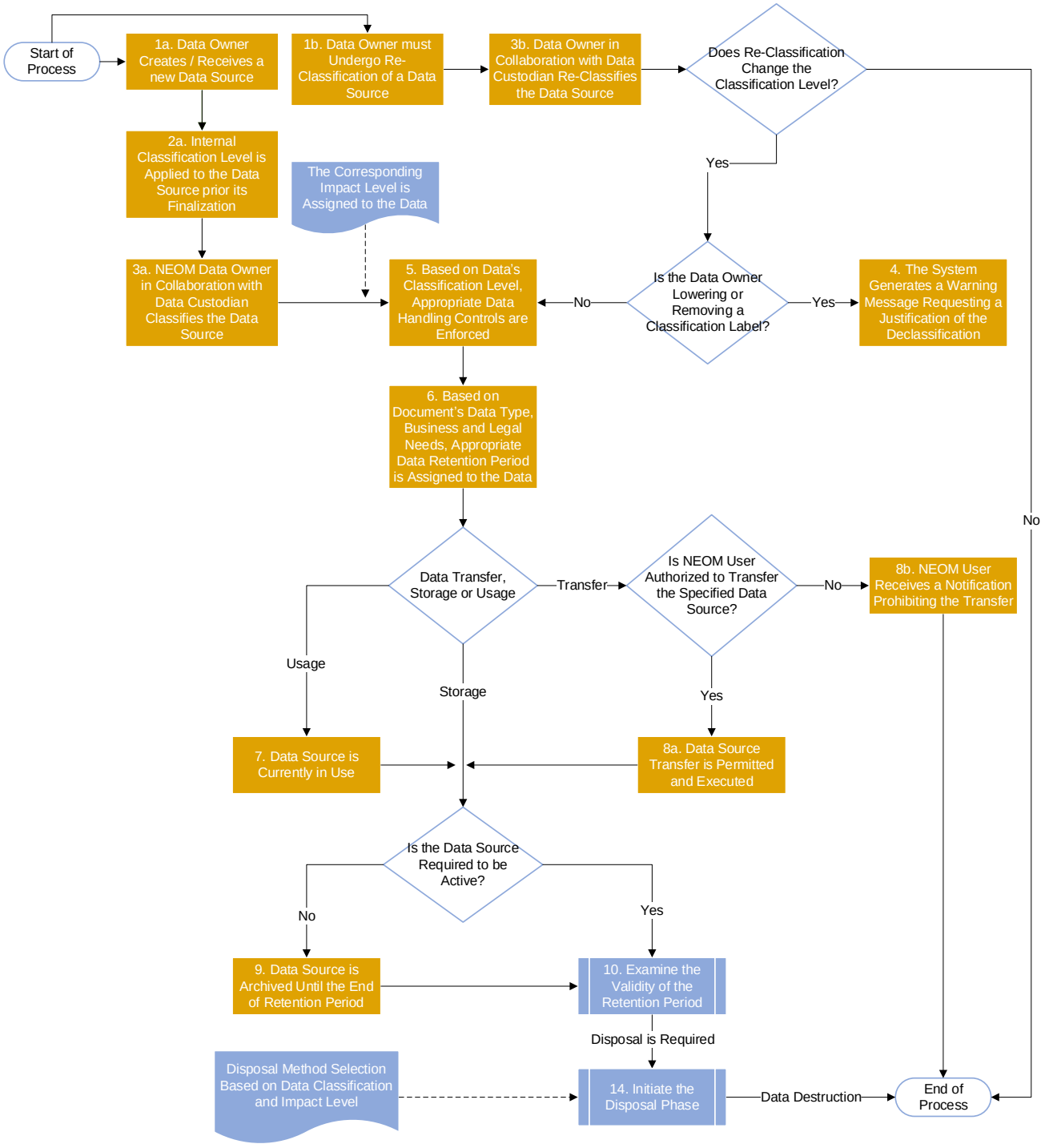

Figure 9 Data Classification & Protection Process

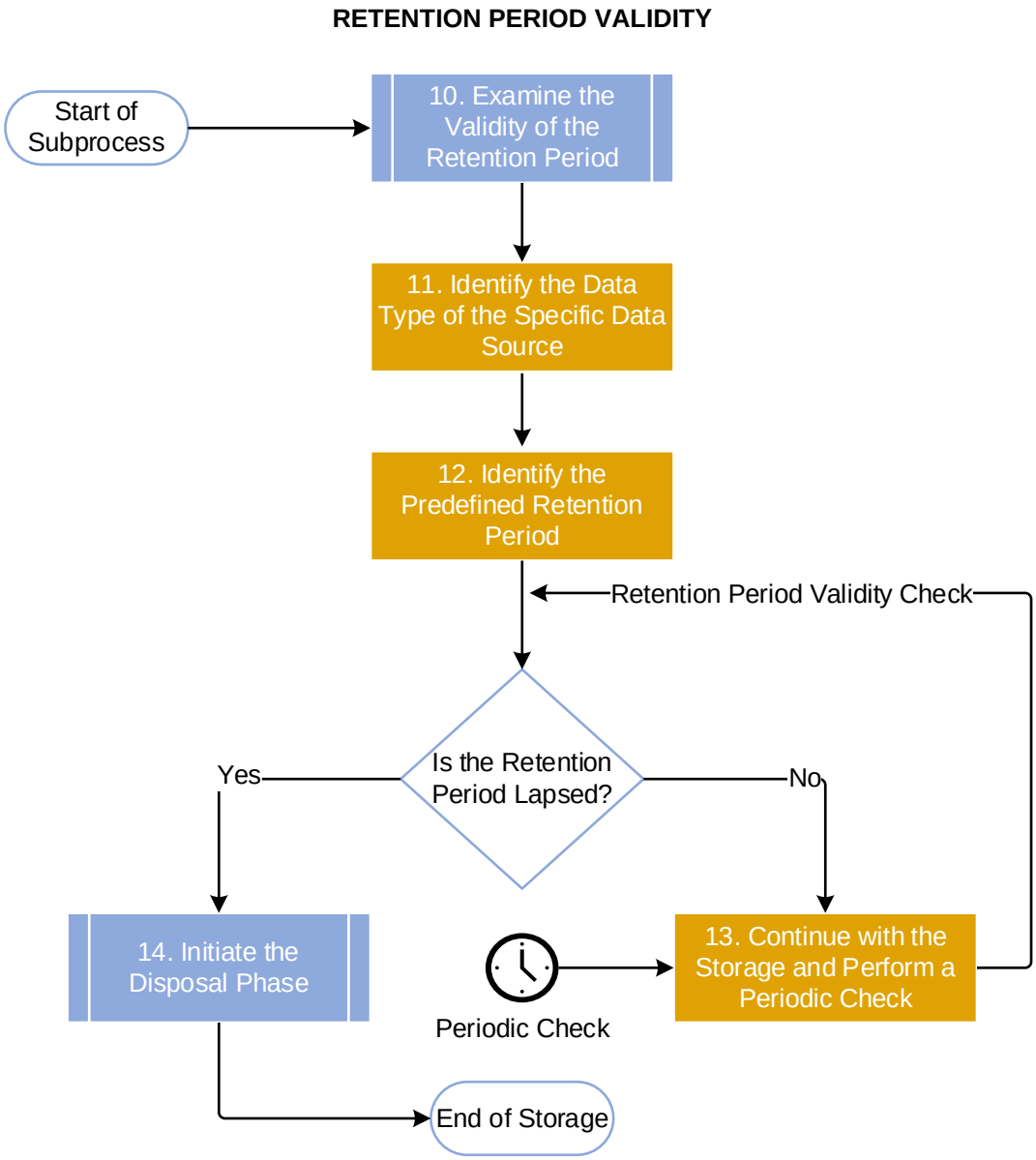

Figure 10 Retention Period Validity Subprocess

DATA DISPOSAL

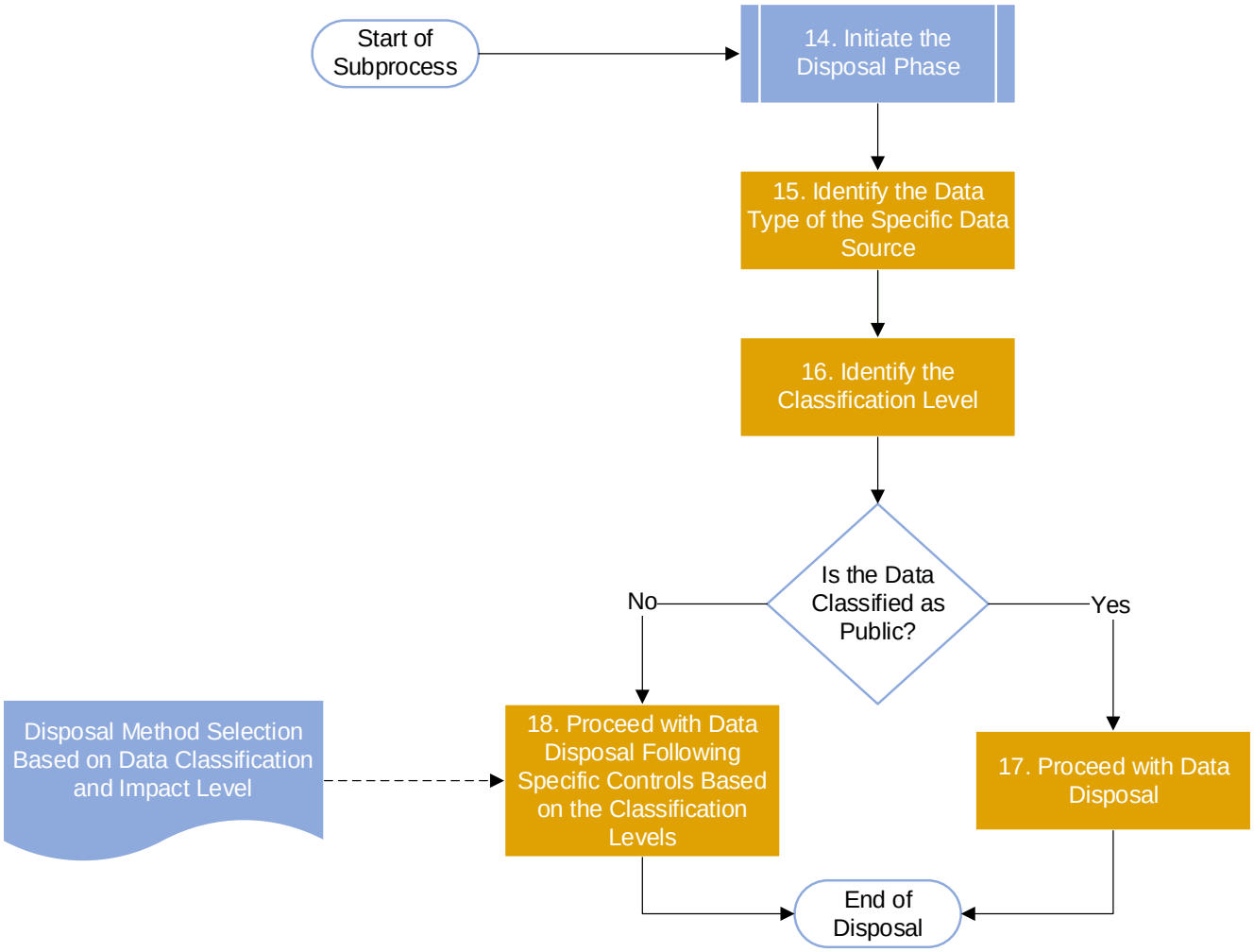

Figure 11 Data Disposal Subprocess

6.2. DATA CLASSIFICATION DECISION TREE

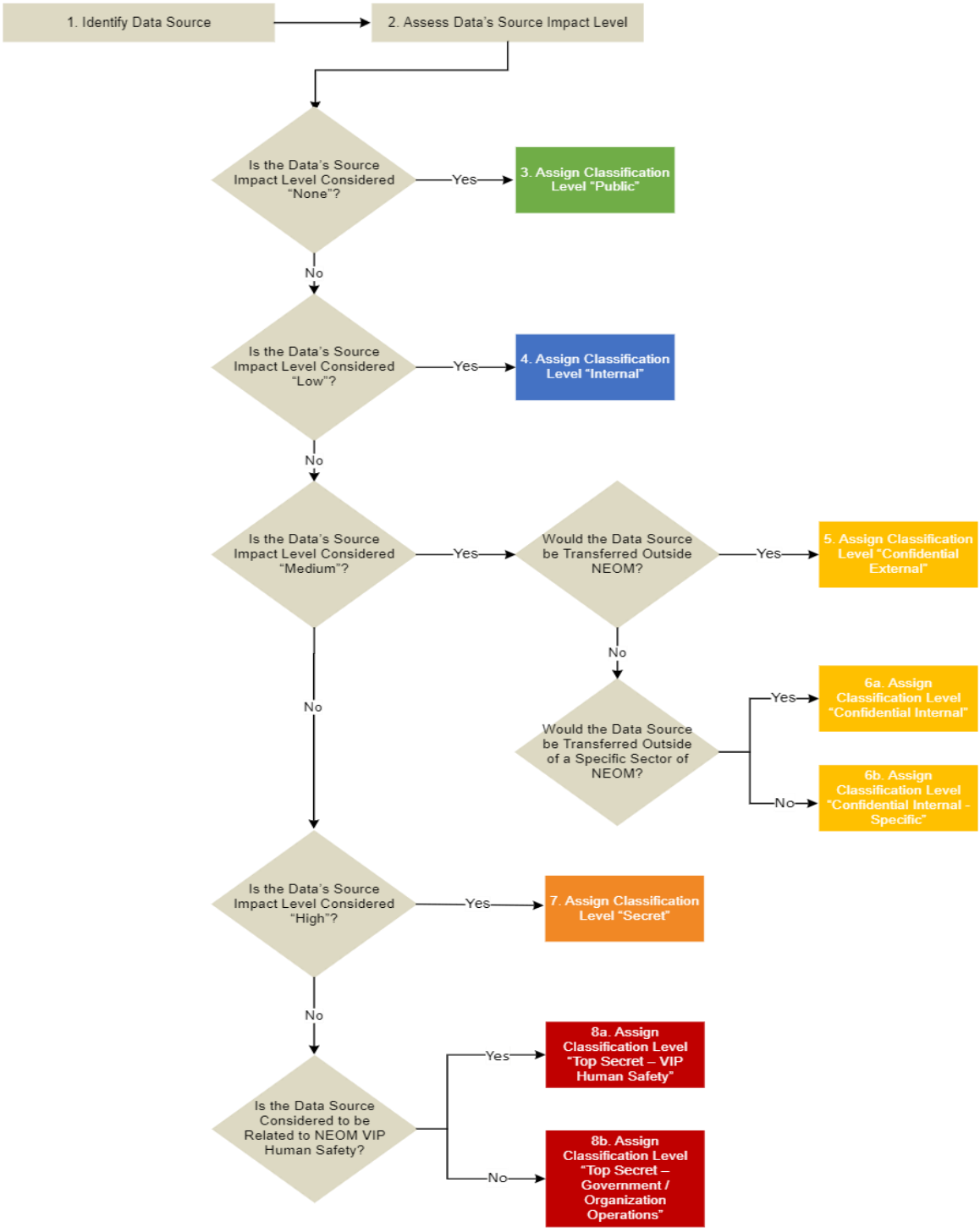

Figure 12 Data Classification Desicion Tree

7. DATA CLASSIFICATION AND PROTECTION PERFORMANCE INDICATORS

7.1. DATA CLASSIFICATION AND PROTECTION KEY PERFORMANCE INDICATORS

Data holds high value and is of vital importance to the functioning of NEOM, therefore it is mandatory to ensure it is treated and that it is secured appropriately. Often time, data becomes the main target of criminal activity which aims at disrupting the wellbeing of the organization at hand, in order to extract valuable information and gain access to restricted sources. For these reasons, NEOM should ensure that its security posture is strengthened appropriately, particularly in relation to the practices of Data Classification and Protection. To that end, NEOM has developed Performance Indicators to continuously oversee its security posture in matters of Data Classification and Protection in a standardized manner throughout its sectors.

Via performance Indicators, or more specifically Key Performance Indicators (KPIs), it is possible to articulate and provide insight into what NEOM needs to measure to be able to evaluate whether long-term objectives have been met. Therefore, KPI can be understood as measurements of performance commonly used to define and evaluate how successful a specific activity or practice is. Within the scope of this Framework, they help gauge, in a quantifiable manner, how effectively has NEOM achieved some objectives within the Data Classification and Protection program. By using KPIs, NEOM is self-assessing with a set frequency, which also allows to compare the gathered numerical values and track performance through time.

Therefore, the direct objective that NEOM has by using KPIs is to ensure of the effectiveness that practices within the Data Classification & Protection program have. However, aside from this direct objective, it is also possible to identify ancillary gains. In fact, by having standardized and controlled KPIs, NEOM also strengthens, between individuals of all ranks and responsibilities, the understanding of threats to NEOM's security and their significance, as well as their own responsibilities in order to avoid the arising risks. Moreover, with time passing, these indicators will become more embedded in NEOMs culture and therefore cybersecurity, and particularly Data Classification and Protection, will be continuously more understood as being everyone's responsibility to be cared for in all daily business operations.

The KPIs have been created taking into consideration the Key Principles of Data Classification and Protection (refer to chapter 4.1), in accordance with the logic that if these fundamentals which lie at the heart of the practice are protected, the Data Classification and Protection program and activities develop on a solid structure. The defined KPIs are therefore a crucial component of the efficient operation of the Data Classification and Protection program and shall be considered as applicable throughout NEOMs sectors.

Indicatively, the results expected to retrieve from the KPIs are:

- The Data Classification & Protection areas that need improvement in order to strengthen NEOMs security posture in this respect,
- The current status regarding how these indicators are addressed,

- The existing gaps between the desired and current status of NEOM's security posture in the field of Data Classification & Protection
- The most critical areas for which improvement is required to improve the security standing.

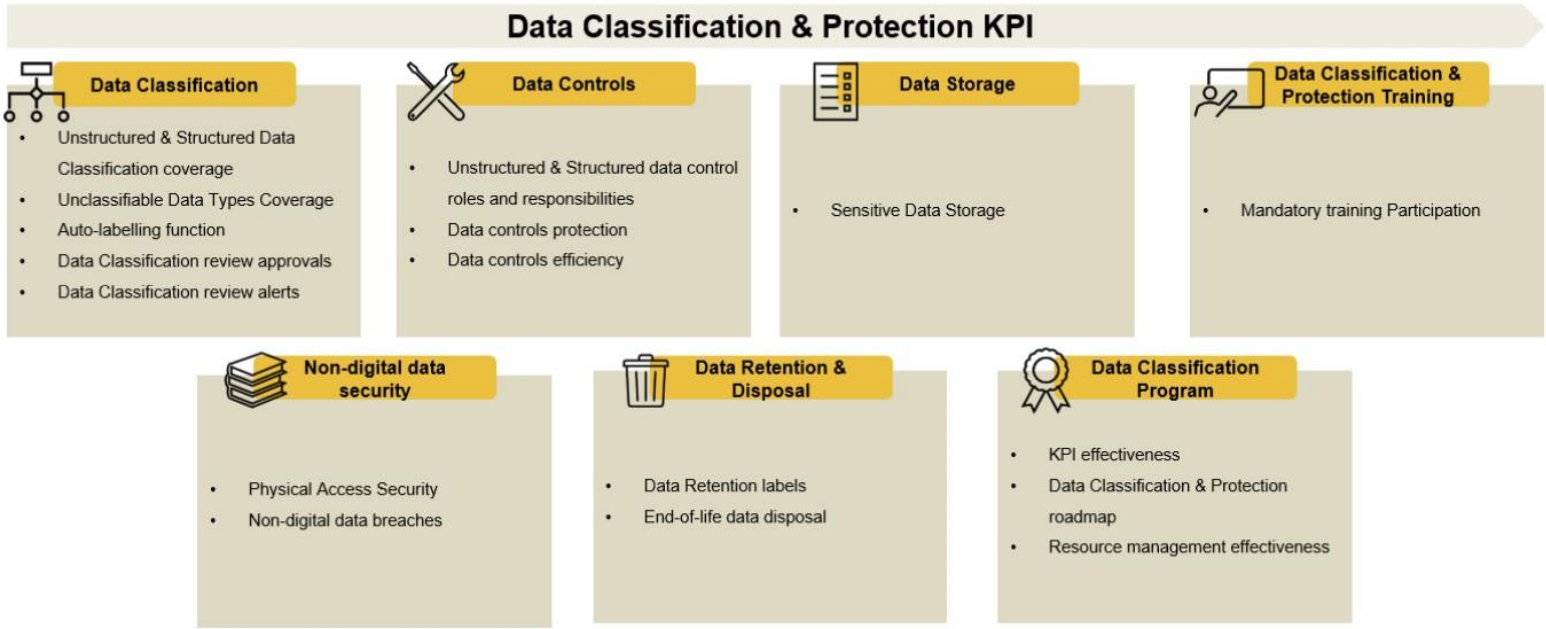

Figure 13 Data Classification & Protection Indicators

The above visual representation of the data classification and protection program KPI is a summarized view of the developed KPI that can found in a more detailed view in **Annex 8.7 – Data Classification and Protection performance indicators to monitor the data classification and protection program.**

7.2. PERFORMANCE REPORTING AND COMMUNICATION PROCESSES

Once the KPIs have been gathered, it is critical to proceed with the reporting of the results, denoting both successes and failures, to the relevant stakeholders within the Data Classification & Protection program. To reiterate, KPIs are specific measures that allow to quantify how effectively NEOM is performing against specific objectives, targets, and best practices. As valuable as the KPI results are, their strategic advantage is most noticeable at the reporting stage, where via different visual representations the results can be appreciated individually and also comparatively with previously reported ones.

During the reporting phase it is therefore expected for the results to be translated into visuals representations that support relevant stakeholders to grasp to its fullest extent the Data Classification and Protection program effectiveness against specific and selected key targets. Specifically, the results will be presented via a KPI Dashboard and shared directly with the CISO on a monthly basis. Moreover, this will also be shared with upper management on a quarterly basis and if necessary, considering the specific results of the KPIs, this can also be shared with a specific sector. Lastly, on an ad-hoc basis it will be reported to the Data Classification & Protection Working Group.

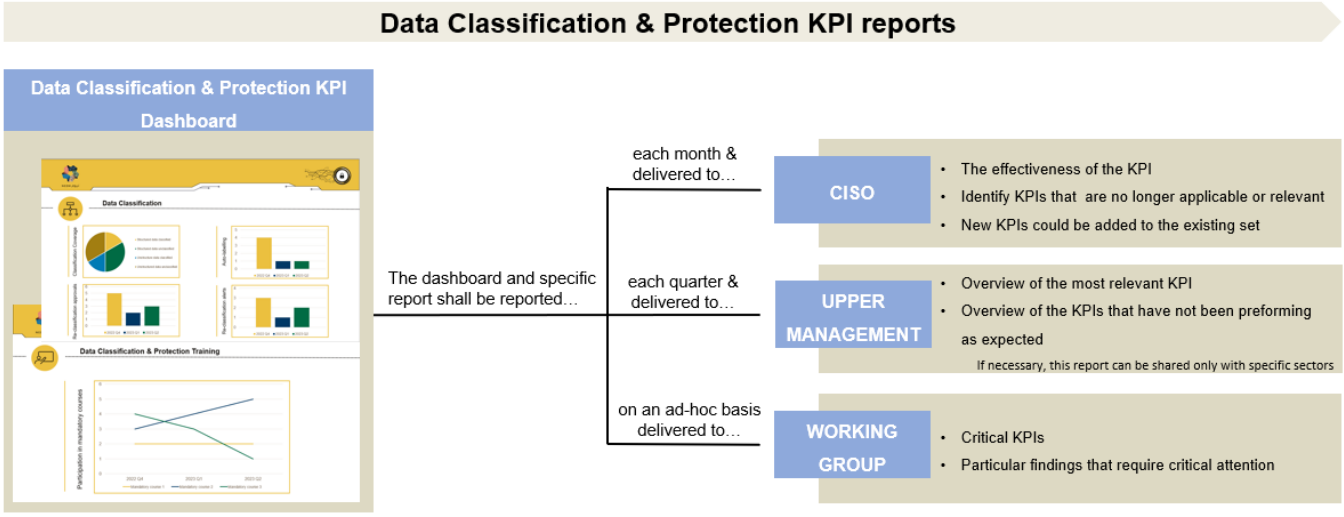

Figure 14 Data Classification & Protection KPI Reports

Using the data visualization tool of a dashboard makes communication easy and makes it simple to all track KPIs through time against business goals. Moreover, by regularly collecting the data for the KPIs and reporting them utilizing a specific and consistent dashboard, it is possible to point out irregularities in the KPIs as they are frequently used and assessed. Moreover, NEOM's CISO should review the defined KPIs on a consistent basis. The KPI irregularities that might be observed are, most notably, the following:

1. ***The effectiveness of the KPI -*** If the KPI is not showing valuable results, its objective may have missed the mark. In this case the KPI may be lacking a specific target or goal, and therefore without a needed degree of specificity, its effectiveness falls short. In this case it would be necessary for the CISO and its supporting team to review what exactly does the KPI wants to demonstrate.

On the other hand, it may also be that the KPI from a theoretical point of view is effective, however it fails because it is too hard to be measured. KPIs blend data, business objectives, and sector targets to act as guideposts, but they are abstract and conceptual. Often time it is not clear or apparent where shall the data be retrieved from, which causes for inconsistent KPI production. In this case, the KPI should be broken down into components that individually are easier to assess and consider.

2. ***The KPI is no longer applicable or relevant -*** Since KPIs are the guideposts that define what it means to be on track for a specific target if the target changes the KPI will no longer be applicable. With time ambitions change, therefore it should not be seen as problematic, but as a sign of development and growth. This situation shall be perceived as a good opportunity to perform an overall health check on the established goals and adjust them to reflect reality.

3. ***New KPIs could be added to the existing set -*** In the event that new strategic goals are identified within the Data Classification and Protection program, it is always possible to add new KPIs. In this case it is important not to fall in the trap of creating too many KPIs, which then causes problems at the time of collecting the data. Therefore, while adding new KPIs is undoubtedly consented, they shall be added with careful considerations. If new KPIs are to be added, this shall be done in agreement with the CISO.

8. ANNEXES

8.1. DATA CLASSIFICATION SCHEME

NEOM - Data Classification Scheme

8.2. DATA IMPACT ANALYSIS MATRIX

NEOM - Data Impact Analysis Matrix

8.3. DATA HANDLING MATRIX

NEOM - Data Handling Matrix

8.4. DATA RETENTION (SCHEDULE & TEMPLATE)

NEOM - Data Retention Schedule

NEOM - Data Retention Template

8.5. DATA INVENTORY TEMPLATE

NEOM - Data Inventory Template

8.6. HIGH LEVEL ACCESS MATRIX

NEOM - High Level Access Matrix

8.7. DATA CLASSIFICATION AND PROTECTION PERFORMANCE INDICATORS TO MONITOR THE DATA CLASSIFICATION AND PROTECTION PROGRAM

NEOM - Data Classification KPIs

8.8. REPORTING TEMPLATE AND DASHBOARD FOR THE DEVELOPED KPIS

NEOM - Reporting
Template and Dashbc

8.9. DATA CLASSIFICATION & PROTECTION PROCESS VISIO

NEOM - Data
Classification & Protec