

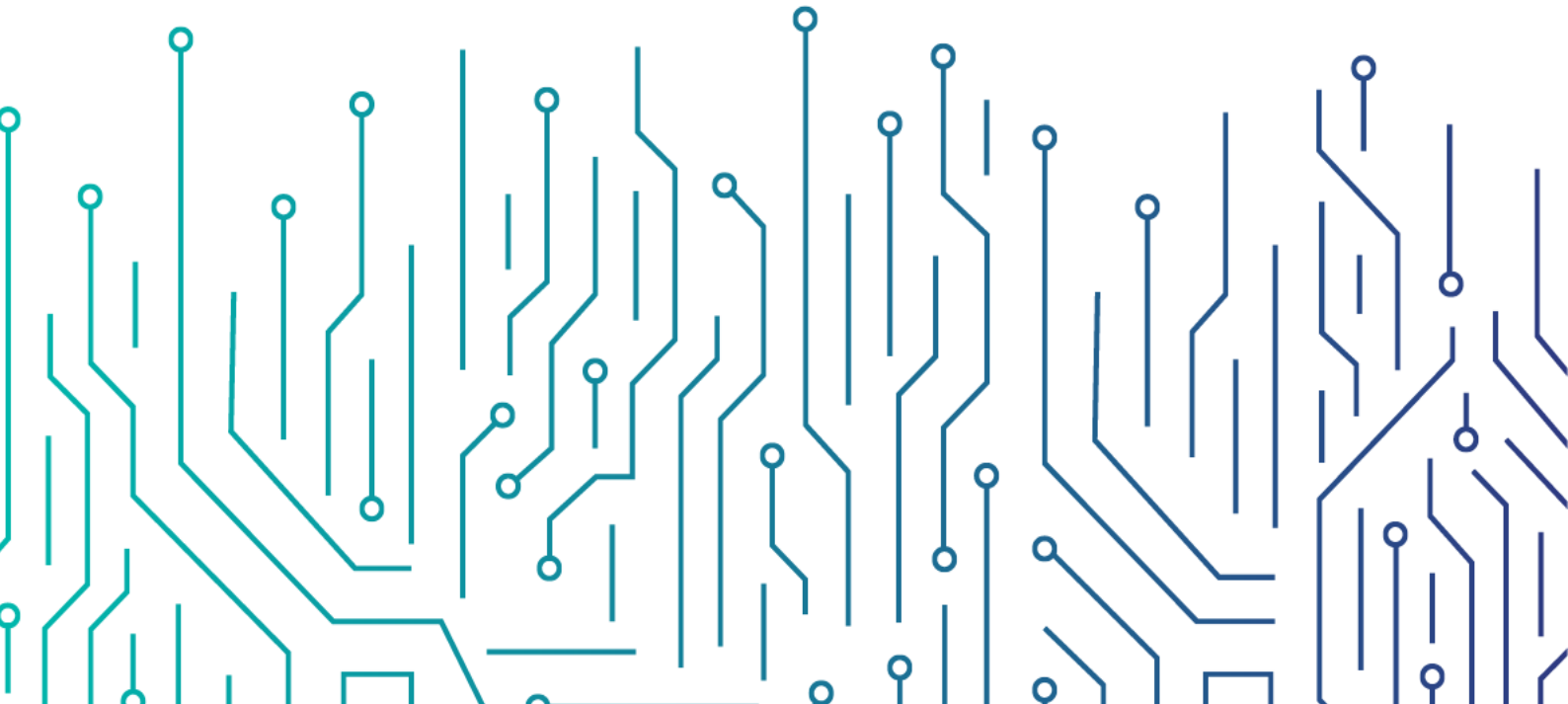


الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Data Cybersecurity Controls

(DCC -1:2022)

Sharing Indicator: **White**
Document Classification: **Public**



In the Name of Allah,
The Most Gracious,
The Most Merciful

DISCLAIMER: The following controls will be governed by and implemented in accordance with the laws of the Kingdom of Saudi Arabia, and must be subject to the exclusive jurisdiction of the courts of the Kingdom of Saudi Arabia. Therefore, the Arabic version will be the binding language for all matters relating to the meaning or interpretation of this document.

Traffic Light Protocol (TLP):

This marking protocol is widely used around the world. It has four colors (traffic lights):

 Red – Personal, Confidential, and for the Intended Recipient only

The recipient has no rights to share information classified in red with any person outside the defined range of recipients, either inside or outside the organization, beyond the scope specified for receipt.

 Amber – Restricted Sharing

The recipient may share information classified in amber only with intended recipients inside the organization and with recipients who are required to take action related to the shared information.

 Green – Sharing within the Same Community

The recipient may share information classified in green with other recipients inside the organization or outside it within the same sector or related to the organization. However, it is not allowed to exchange or publish this information on public channels.

 White – No Restrictions

Table of Contents

Executive Summary	5
Introduction	6
Objectives	7
Scope of Work and Applicability	7
DCC Scope of Work	7
DCC Statement of Applicability	7
Implementation and Compliance	8
Update and Review	8
DCC Domains and Structure	9
Main domains and subdomains of DCC	9
Structure	10
DCC Controls	11
Appendices	20
Appendix (A): Relationship with the Essential Cybersecurity Controls	20
Appendix (B): Terms and Definitions	22
Appendix (C): List of Abbreviations	24
Appendix (D): Relationship with Data Lifecycle	25

List of Tables

Table 1: DCC Structure	10
Table 2: Terms and Definitions	22
Table 3: List of Abbreviations	24
Table 4: Relationship with Data Lifecycle	25

List of Figures and Illustrations

Figure 1: DCC Main Domains and Subdomains	9
Figure 2: Controls Coding Scheme	10
Figure 3: DCC Structure	10
Figure 4: Guide to Colors of Subdomains in Figure 5	20
Figure 5: DCC and ECC Subdomains	21

Executive Summary

The Kingdom of Saudi Arabia's vision 2030 aims to achieve a number of economic, development and security goals, thereby enhancing the performance of national organizations, and encouraging the diversification of the economy and the use of data-based services. National data is one of the most important assets contributing to the success of the strategic goals of Vision 2030 through decision support and is an economic resource to support competitiveness at the national level, where national organizations collect and process vast amounts of data that may be vulnerable to cyber threats and risks that negatively impact national security, the Kingdom's economy, reputation, external relations, or critical infrastructures, which raises the urgency to put cybersecurity requirements to protect against such threats and risks.

The NCA's mandate as per the Royal Decree number 6801, dated 11/2/1439H, makes NCA the cybersecurity regulator in the Kingdom and the national reference for anything related to cybersecurity. NCA's mandate and duties fulfill the strategic and regulatory cybersecurity needs related to the development of cybersecurity national policies, governance mechanisms, frameworks, standards, controls and guidelines. The NCA's mandate and duties also fulfill the need to continuously monitor the compliance of organizations to support the important role of cybersecurity, which has increased with the rise of security risks in cyberspace more than any time before. NCA's mandate states that its responsibility for cybersecurity does not absolve any government, private or other organization from its own cybersecurity responsibilities as confirmed by Royal Decree number 57231, dated 10/11/1439H, which states that "all government organizations must improve their cybersecurity level to protect their networks, systems and data, and comply with NCA's policies, framework, standards, controls and guidelines". In order to reach a secure and reliable Saudi cyberspace that enables growth and prosperity and in addition to the Essential Cybersecurity Controls (ECC-1: 2018), NCA has developed Data Cybersecurity Controls (DCC-1: 2022) to set the minimum cybersecurity requirements to enable organizations to protect their data during its entire data lifecycle. This document highlights the details of the Data Cybersecurity Controls (DCC), objectives, scope of work, compliance and monitoring.

All organizations within the scope of these controls must implement all necessary measures to ensure continuous compliance with the DCC as per item 3 of article 10 of NCA's mandate and as per the Royal Decree number 57231, dated 10/11/1439H.

Introduction

The National Cybersecurity Authority (referred to in this document, as "NCA") developed the Data Cybersecurity Controls (DCC-1: 2022) after conducting a comprehensive study of multiple national and international cybersecurity standards, frameworks and controls, studying related laws and regulations, reviewing cybersecurity best practices and analyzing cybersecurity risks, threats, previous incidents and attacks at the national level. These controls support organizations to counter the ever-increasing cybersecurity threats and minimize the negative impacts in order to protect the vital interests of the kingdom, national security, critical infrastructures, high priority sectors and governmental services and activities.

While developing the Data Cybersecurity Controls, the NCA carefully aligned the controls with the Essential Cybersecurity Controls (ECC-1: 2018), which are pre-request for compliance for organizations. Compliance with DCC cannot be achieved without achieving continuous compliance with ECC, where applicable as they are linked to relevant national legislative and regulatory requirements. Thus, based on the regulatory tools issued by the Saudi Data and Artificial Intelligence Authority (SDAIA), data is classified into four levels based on its sensitivity and protection needs, which are: Public, Confidential, Secret, and Top Secret.

The Data Cybersecurity Controls consist of the following:

- 3 Main Domains.
- 11 Subdomains.
- 19 Main Controls
- 47 Subcontrols

Objectives

The main objectives of the DCC are to:

- Raise the level of cybersecurity in order to protect national data.
- Support organizations' cybersecurity throughout the data lifecycle in order to protect their data and information assets from cybersecurity threats and risks.
- Raise the level of awareness on handling data securely.

Scope of Work and Applicability

DCC Scope of Work

These controls are applicable to government organizations in the Kingdom of Saudi Arabia (including ministries, authorities, establishments and others) and its companies and entities, as well as private sector organizations owning, operating or hosting Critical National Infrastructures (CNIs), which all referred to herein as "The organization". These controls are also applicable to all forms of physical and digital data, including structured data (such as databases, data tables) and unstructured data (such as documents and records).

NCA strongly encourages all other organizations in the Kingdom to leverage these controls to implement best practices to protect data.

DCC Statement of Applicability

These controls have been developed after taking into consideration the cybersecurity needs of organizations and sectors in the kingdom. Every organization within the scope of these controls must comply with all applicable controls in this document.

Implementation and Compliance

In order to comply with item 3 of article 10 of NCA's mandate and as per the Royal Decree number (57231) dated 10/11/1439H, all organizations within the scope of these controls must implement whatever necessary to ensure continuous compliance with the controls, which cannot be achieved without achieving continuous compliance with the Essential Cybersecurity Controls (ECC – 1: 2018) where applicable.

NCA evaluates organizations' compliance with the DCC through multiple means such as self-assessments by the organizations, and/or external assessments, in accordance with the mechanisms deemed appropriate by NCA.

Update and Review

NCA will periodically review and update (as needed) the DCC as per the cybersecurity requirements and related industry updates.

DCC Domains and Structure

Main domains and subdomains of DCC

Figure (1) below shows the main domains and subdomains of the Data Cybersecurity Controls, while Appendix (A) highlights the relationship between these controls and the Essential Cybersecurity Controls (ECC).

1. Cybersecurity Governance	1-1	Periodical Cybersecurity Review and Audit	1-2	Cybersecurity in Human Resources
	1-3	Cybersecurity Awareness and Training Program		
2. Cybersecurity Defense	2-1	Identity and Access Management	2-2	Information System and Information Processing Facilities Protection
	2-3	Mobile Devices Security	2-4	Data and Information Protection
	2-5	Cryptography	2-6	Secure Data Disposal
	2-7	Cybersecurity for Printers, Scanners and Copy Machines		
3. Third-Party and Cloud Computing Cybersecurity	3-1	Third-Party Cybersecurity		

Figure 1: DCC Main Domains and Subdomains

Structure

Figures (2) and (3) below show the meaning of controls codes:

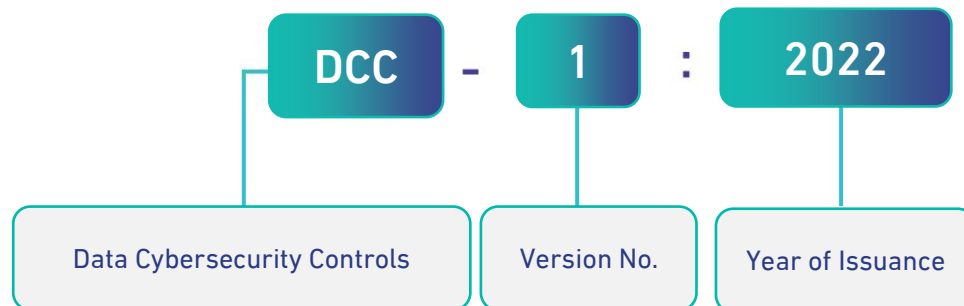


Figure 2: Controls Coding Scheme

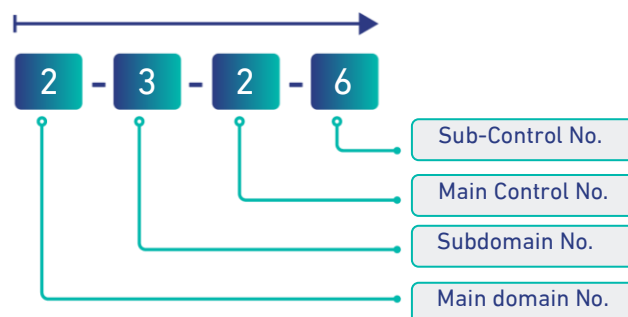


Figure 3: DCC Structure

Table (1) below shows the methodological structure of DCC

1		Name of the Main Domain			
Reference Number of the Main Domain					
Reference No. of the Subdomain					
Objective					
Controls		Data Classification Level			
		Public	Confidential	Secret	Top Secret
Control Reference Number	Control Clauses				

Table 1: DCC Structure

Data Cybersecurity Controls

1 Cybersecurity Governance

1-1	Periodical Cybersecurity Review and Audit					
objective	To ensure that cybersecurity controls are implemented and in compliance with organizational policies and procedures, as well as related national and international laws, regulations and agreements.					
Controls			Data Classification Level			
			Public	Confidential	Secret	Top Secret
1-1-1	With reference to ECC control 1-8-1, the cybersecurity function in the organization must review the implementation of the Data Cybersecurity Controls periodically as specified for each data classification level.		At least annually			
1-1-2	With reference to ECC control 1-8-2, cybersecurity review and audit must be conducted periodically by independent parties outside the organization’s cybersecurity function as specified for each data classification level.		At least every 2 years		At least annually	
1-2	Cybersecurity in Human Resources					
objective	To ensure that cybersecurity risks and requirements related to personnel (employees and contractors) are managed efficiently prior to employment, during employment and after termination/separation as per organizational policies and procedures, and related laws and regulations.					
Controls			Data Classification Level			
1-2-1	In addition to the subcontrols in the ECC control 1-9-3, cybersecurity requirements in human resources prior to employment, during employment and after termination/separation must include at least the following:		Public	Confidential	Secret	Top Secret
	1-2-1-1	Screening and vetting candidates in jobs related to data handling.			✓	✓
	1-2-1-2	A signed agreement by personnel pledging to not use social media, communication applications or personal cloud storage to create, store or share the		✓	✓	✓

		organization's data, with the exception of secure communication applications approved by relevant authorities.				
1-3	Cybersecurity Awareness and Training Program					
objective	To ensure that personnel are aware of their cybersecurity responsibilities and have the required cybersecurity awareness. It is also to ensure that personnel are provided with the required cybersecurity training, skills and credentials needed to accomplish their cybersecurity responsibilities and to protect the organization's information and technology assets.					
Controls			Data Classification Level			
1-3-1	In addition to the subcontrols in ECC control 1-10-3, the cybersecurity awareness program must cover topics related to data protection, including the following:		Public	Confidential	Secret	Top Secret
	1-3-1-1	Risks of data leakage and unauthorized access to data during its lifecycle.	✓	✓	✓	✓
	1-3-1-2	Secure handling of classified data while traveling and outside the workplace.		✓	✓	✓
	1-3-1-3	Secure handling of data during meetings (virtual and in-person).		✓	✓	✓
	1-3-1-4	Secure use of printers, scanners and copy machines.		✓	✓	✓
	1-3-1-5	Procedures for secure data disposal.		✓	✓	✓
	1-3-1-6	Risks of sharing documents and information through non-secure channels.	✓	✓	✓	✓
	1-3-1-7	Cybersecurity risks related to the use of external storage media.	✓	✓	✓	✓

2 Cybersecurity Defense

2-1	Identity and Access Management					
objective	To ensure the secure and restricted logical access to information and technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks.					
Controls			Data Classification Level			
2-1-1	In addition to the subcontrols in ECC control 2-2-3, cybersecurity requirements for identity and access management must cover at least the following:		Public	Confidential	Secret	Top Secret
	2-1-1-1	Strict restriction to allow only the minimum number of personnel accessing, viewing and sharing data based on lists of privileges limited to Saudi-national employees unless exempted by the Authorizing Official (the head of the organization or his/her delegate) and those lists are approved by the Authorizing Official.			✓	✓
	2-1-1-2	Prohibiting the sharing of approved lists of privileges with unauthorized persons.		✓	✓	✓
2-1-2	Managing identities and access rights to view data using Privileged Access Management systems.			✓	✓	✓
2-1-3	In addition to ECC subcontrol 2-2-3-5, the approved lists of privileges and privileges used to handle data must be reviewed as specified for each data classification level.		At least annually		At least every 3 months	
2-2	Information System and Information Processing Facilities Protection					
objective	To ensure the protection of information systems and information processing facilities (including workstations and infrastructures) against cyber risks.					
Controls			Data Classification Level			
2-2-1	In addition to the subcontrols in ECC control 2-3-3, cybersecurity requirements for Information System and Information Processing Facilities Protection must include at least the following:		Public	Confidential	Secret	Top Secret
	2-2-1-1	Applying security patches and updates from the time of announcement on systems used to handle data as specified for each data classification level.	At least every month		Immediately	

	2-2-1-2	Reviewing the security configuration and hardening of systems used to handle data as specified for each data classification level.	At least annually		At least every 6 months	
	2-2-1-3	Reviewing and hardening the default configuration (e.g., default passwords and backgrounds) of the technology assets used to handle the data.	✓	✓	✓	✓
	2-2-1-4	Disabling the Print Screen or Screen Capture features on the devices that create or process documents.			✓	✓
2-3	Mobile Devices Security					
objective	To ensure the protection of mobile devices (including laptops, smartphones, tablets) from cyber risks and to ensure the secure handling of the organization’s information (including sensitive information) while utilizing Bring Your Own Device (BYOD) policy.					
Controls			Data Classification Level			
2-3-1	In addition to the subcontrols in ECC control 2-6-3, cybersecurity requirements for mobile devices must cover at least the following:		Public	Confidential	Secret	Top Secret
	2-3-1-1	Centrally managing the organization’s owned mobile devices using Mobile Device Management (MDM) system and activating the remote wipe feature.	✓	✓	✓	✓
	2-3-1-2	Centrally managing BYOD devices using Mobile Device Management (MDM) system and activating the remote wipe feature.	✓	✓	Use of BYOD devices is prohibited	
2-4	Data and Information Protection					
objective	To ensure the confidentiality, integrity and availability of organization’s data and information as per organizational policies and procedures, and related laws and regulations.					
Controls			Data Classification Level			
2-4-1	In addition to the subcontrols in ECC control 2-7-3, cybersecurity requirements for data and information protection must cover at least the following:		Public	Confidential	Secret	Top Secret

	2-4-1-1	Using Watermark feature to label the whole document when creating, storing, printing, on the screen and on each copy so that the symbol can be traced to the user or device level.			✓	✓
	2-4-1-2	Using Data Leakage Prevention technologies and Rights Management technologies.		✓	✓	✓
	2-4-1-3	Prohibiting the use of data in any environment other than the production environment, except after conducting a risk assessment and applying controls to protect that data, such as: data masking or data scrambling techniques.		✓	✓	✓
	2-4-1-4	Using brand protection service to protect the organization's identity from impersonation.	✓	✓	✓	✓
2-5	Cryptography					
objective	To ensure the proper and efficient use of cryptography to protect information assets as per organizational policies and procedures, and related laws and regulations.					
Controls			Data Classification Level			
2-5-1	In addition to the subcontrols in ECC control 2-8-3, cybersecurity requirements for cryptography must cover at least the following:		Public	Confidential	Secret	Top Secret
	2-5-1-1	Using secure and up-to-date cryptographic methods and algorithms when creating, storing, transmitting data, and for overall network communication medium; as per the requirements of the “advanced level” in the National Cryptographic Standards (NCS-1:2020).			✓	✓

	2-5-1-2	Using secure and up-to-date cryptographic methods and algorithms when creating, storing, transmitting data, and for overall network communication medium; as per the requirements of the “moderate level” in the National Cryptographic Standards (NCS-1:2020).		✓		
2-6	Secure Data Disposal					
objective	To ensure a secure data disposal as per organizational policies and procedures, and related laws and regulations.					
Controls			Data Classification Level			
2-6-1	Cybersecurity requirements for secure data disposal must cover at least the following:		Public	Confidential	Secret	Top Secret
	2-6-1-1	Identification of technologies, tools and procedures for the implementation of secure data disposal according to the data classification level.		✓	✓	✓
	2-6-1-2	When storage media is no longer needed, it must be securely disposed by using the technologies, tools and procedures identified in subcontrol 2-6-1-1.		✓	✓	✓
	2-6-1-3	When storage media needs to be re-used, data must be securely erased (secure erasure) in a manner it cannot be recovered.		✓	✓	✓
	2-6-1-4	Implementation of secure data disposal or erasure operations referred to in sub-controls 2-6-1-2 and 2-6-1-3 must be verified.		✓	✓	✓
	2-6-1-5	Keeping a record of all secure data disposal and erasure operations that have been conducted.		✓	✓	✓
2-6-2	The implementation of the secure data disposal requirements must be reviewed as specified for each data classification level.		At least annually		At least every 6 months	

2-7	Cybersecurity for Printers, Scanners and Copy Machines				
objective	To ensure secure handling of data when using Printers, Scanners and Copy Machines.				
Controls		Data Classification Level			
		Public	Confidential	Secret	Top Secret
2-7-1	Cybersecurity requirements for protecting printers, scanners and copy machines must be defined, documented and approved.		✓	✓	✓
2-7-2	Cybersecurity requirements for printers, scanners and copy machines must be implemented.		✓	✓	✓
2-7-3	Cybersecurity requirements for printers, scanners and copy machines must cover at least the following:				
	2-7-3-1 Disabling the temporary storage feature.			✓	✓
	2-7-3-2 Enabling authentication on centralized printers, scanners and copy machines and requiring it before usage.			✓	✓
	2-7-3-3 Securely retaining (for a period not less than 12 months) logs of printers, scanners and copy machines usage.			✓	✓
	2-7-3-4 Enabling and protecting CCTV logs which are used to monitor centralized printers, scanners and copy machines areas.			✓	✓
	2-7-3-5 Using cross-shredding devices, to securely dispose documents when no longer needed.			✓	✓
2-7-4	Implementation of cybersecurity requirements for printers, scanners and copy machines must be reviewed as specified for each data classification level.	At least every 3 years		At least annually	



Third-Party and Cloud Computing Cybersecurity

3-1	Third-Party Cybersecurity					
objective	To ensure the protection of assets against the cybersecurity risks related to third parties including outsourcing, managed services, and consultancy services as per organizational policies and procedures, and related laws and regulations.					
Controls			Data Classification Level			
3-1-1	In addition to the controls in ECC subdomain 4-1, cybersecurity requirements for third-parties cybersecurity must include at least the following:		Public	confidential	Secret	Top Secret
	3-1-1-1	Screening or vetting third-party employees who have access to the data.			✓	✓
	3-1-1-2	Requiring contractual commitment by third-parties to securely dispose the organization’s data at the end of the contract or in case of contract termination, including providing evidences of such disposal to the organization.		✓	✓	✓
	3-1-1-3	Documenting all data sharing operations within third-parties, including data sharing justification.		✓	✓	✓
	3-1-1-4	When transferring data outside the kingdom, the capability of the hosting organization abroad to safeguard data must be verified, approval of the Authorizing Official must be obtained and complying with related laws and regulations.		✓	✓	✓
	3-1-1-5	Requiring third-parties to notify the organization immediately in case of cybersecurity incident that may affect data that has been shared or created.		✓	✓	✓
	3-1-1-6	Reclassifying data to the least level to achieve the objective before sharing it with third-parties using data masking or data scrambling techniques.		✓	✓	✓
3-1-2	In alignment with related laws and regulations, and in addition to the applicable controls in ECC and controls within DCC domain (1), (2), and (3); cybersecurity requirements when dealing with consultancy services that works on high-sensitivity strategic projects at the national level must cover at least the following:					

	3-1-2-1	Screening or vetting consultancy services employees who have access to the data			✓	✓
	3-1-2-2	Requiring contractual commitment by consultancy services including employees non-disclosure agreements and secure disposal the organization's data at the end of the contract or in case of contract termination, including providing evidences of such disposal to the organization.		✓	✓	✓
	3-1-2-3	Documenting all data sharing operations within consultancy services, including data sharing justification.		✓	✓	✓
	3-1-2-4	Requiring consultancy services to notify the organization immediately in case of cybersecurity incident that may affect data that has been shared or created.		✓	✓	✓
	3-1-2-5	Reclassifying data to the least level to achieve the objective before sharing it with consultancy services using data masking or data scrambling techniques.		✓	✓	✓
	3-1-2-6	Dedicating a closed room for the consultancy services employees to perform their work, in addition to providing dedicated organization owned devices to share and process data.			✓	✓
	3-1-2-7	Activating access control system to allow only authorized access to the closed room.			✓	✓
	3-1-2-8	Preventing carrying out of devices, storage media and documents outside the closed room, as well as the entry of any other electronic devices.			✓	✓

Appendices

Appendix (A): The relationship with the Essential Cybersecurity Controls (ECC)

The Data Cybersecurity Controls (DCC-1:2022) is an extension to the Essential Cybersecurity Controls (ECC- 1: 2018) as illustrated in figures (4) & (5) below, where:

- (9) Subdomains, to which cybersecurity controls have been added for Data Cybersecurity Controls.
- (20) Subdomains, to which no additional cybersecurity controls have been added for Data Cybersecurity Controls.
- (2) New subdomains to which cybersecurity controls have been added for Data Cybersecurity Controls.

	Subdomains where cybersecurity controls have been added for Data Cybersecurity Controls.
	Subdomains where no additional cybersecurity controls have been added for Data Cybersecurity Controls.
	New Subdomain have been added for Data Cybersecurity Controls.

Figure 4: Guide to Colors of Subdomains in Figure 5

1.Cybersecurity Governance	Cybersecurity Strategy		Cybersecurity Management	
	Cybersecurity Policies and Procedures		Cybersecurity Roles and Responsibilities	
	Cybersecurity Risk Management		Cybersecurity in Information Technology Projects	
	Cybersecurity Regulatory Compliance		1-1	Periodical Cybersecurity Review and Audit
	1-2	Cybersecurity in Human Resources	1-3	Cybersecurity Awareness and Training Program
2.Cybersecurity Defense	Asset Management		2-1	Identity and Access Management
	2-2	Information System and Information Processing Facilities Protection	Email Protection	
	Networks Security Management		2-3	Mobile Devices Security
	2-4	Data and Information Protection	2-5	Cryptography
	Backup and Recovery Management		Vulnerabilities Management	
	Penetration Testing		Cybersecurity Event Logs and Monitoring Management	
	Cybersecurity Incident and Threat Management		Physical Security	
	Web Application Security		2-6	Secure Data Disposal
	2-7	Cybersecurity for Printers, Scanners and Copy Machines		
3.Cybersecurity Resilience	Cybersecurity Resilience aspects of Business Continuity Management (BCM)			
4.Third-Party and Cloud Computing Cybersecurity	3-1	Third-Party Cybersecurity	Cloud Computing and Hosting Cybersecurity	
5.ICS Cybersecurity	Industrial Control Systems (ICS) Protection			

Figure 5: ECC and DCC Subdomains

Appendix (B): Terms and Definitions

Table (2) below highlights some of the terms and their definitions which were used in this document.

Terminology	Definition
Data Leakage Prevention Technologies (DLP)	Technologies used to protect sensitive data from unauthorized disclosure, and to prevent its circulation outside the organization in any form of such data, and its location; Whether stored on volumes (At-rest), or on the user devices or servers (In-Use), or in movement via the network (In-transit).
Mobile Device Management (MDM) System	A technical system used to manage, monitor, and protect mobile devices of employees by applying cybersecurity policies.
Rights Management Technologies	Technologies used to protect sensitive data from unauthorized disclosure, and to limit processing it as per the privileges assigned to the authorized users.
Consulting Services	Services provided by a professional advisory team where consultants review and analyze client business data and documents, which may contain sensitive and confidential data, and offer advice, benchmarks, and use their expertise to recommend best practice or help businesses based on their individual requirements. This does not include professional cybersecurity services. Examples: ● Digital Transformation Consultancy. ● Strategy and regulation analysis and development.

Terminology	Definition
Professional Cybersecurity Services	Cybersecurity services that are provided by an NCA-certified/licensed provider based on a clear cybersecurity assessment or response scope. Example: ● Cybersecurity Vulnerability Assessment. ● Cybersecurity Incident Response. ● Cybersecurity Risk Assessment.
Managed Services	Professional services that are provided on subscription basis by an NCA certified/licensed provider to offload some professional IT and cybersecurity operations. This includes products, solutions, software, and hardware. Example: ● Managed Cybersecurity Operations Center (SOC). ● Managed IT services.

Table 2: Terms and Definitions

Appendix (C): List of the Abbreviations

Table (3) below highlights some of the abbreviations and their meanings which were used in this document.

Abbreviations	Full Term
BYOD	Bring Your Own Device
ECC	Essential Cybersecurity Controls
MDM	Mobile Device Management
NCS	National Cryptographic Standard
TLP	Traffic Light Protocol

Table 3: List of Abbreviations

Appendix (D): The Relationship with Data Lifecycle

Table (4) below highlights the relationship between the Data Cybersecurity Control and the stages of data lifecycle.

Controls		Data lifecycle				
Main control	Sub control	Create	Store	Share	Use	Dispose
1-1-1	-----	✓	✓	✓	✓	✓
1-1-2	-----	✓	✓	✓	✓	✓
1-2-1	1-2-1-1	✓	✓	✓	✓	✓
	1-2-1-2	✓	✓	✓	✓	
1-3-1	1-3-1-1	✓	✓	✓	✓	✓
	1-3-1-2		✓	✓	✓	
	1-3-1-3		✓	✓	✓	
	1-3-1-4		✓	✓	✓	
	1-3-1-5					✓
	1-3-1-6		✓	✓	✓	
	1-3-1-7		✓	✓	✓	✓
2-1-1	2-1-1-1			✓	✓	
	2-1-1-2			✓	✓	
2-1-2	-----			✓	✓	
2-1-3	-----			✓	✓	
2-2-1	2-2-1-1	✓	✓	✓	✓	
	2-2-1-2	✓	✓	✓	✓	
	2-2-1-3	✓	✓	✓	✓	
	2-2-1-4	✓	✓	✓	✓	
2-3-1	2-3-1-1	✓	✓	✓	✓	✓
	2-3-1-2	✓	✓	✓	✓	✓
2-4-1	2-4-1-1	✓	✓	✓	✓	
	2-4-1-2	✓	✓	✓	✓	✓
	2-4-1-3		✓	✓	✓	
	2-4-1-4	✓	✓	✓	✓	✓
2-5-1	2-5-1-1	✓	✓	✓	✓	
	2-5-1-2	✓	✓	✓	✓	
2-6-1	2-6-1-1					✓
	2-6-1-2					✓
	2-6-1-3					✓
	2-6-1-4					✓
	2-6-1-5					✓
2-7-1	-----			✓	✓	
2-7-2	-----			✓	✓	
2-7-3	2-7-3-1		✓	✓	✓	
	2-7-3-2			✓	✓	

Controls		Data lifecycle				
Main control	Sub control	Create	Store	Share	Use	Dispose
	2-7-3-3			✓	✓	
	2-7-3-4			✓	✓	
	2-7-3-5					✓
2-7-4	-----			✓	✓	
3-1-1	3-1-1-1		✓	✓	✓	
	3-1-1-2	✓	✓	✓	✓	✓
	3-1-1-3			✓	✓	
	3-1-1-4	✓	✓	✓	✓	
	3-1-1-5	✓	✓	✓	✓	
	3-1-1-6	✓	✓	✓	✓	
3-2-1	3-2-1-1		✓	✓	✓	
	3-2-1-2	✓	✓	✓	✓	✓
	3-2-1-3			✓	✓	
	3-2-1-4	✓	✓	✓	✓	
	3-2-1-5	✓	✓	✓	✓	
	3-2-1-6	✓	✓	✓	✓	
	3-2-1-7	✓	✓	✓	✓	

Table 4: The relationship Data Lifecycle



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

