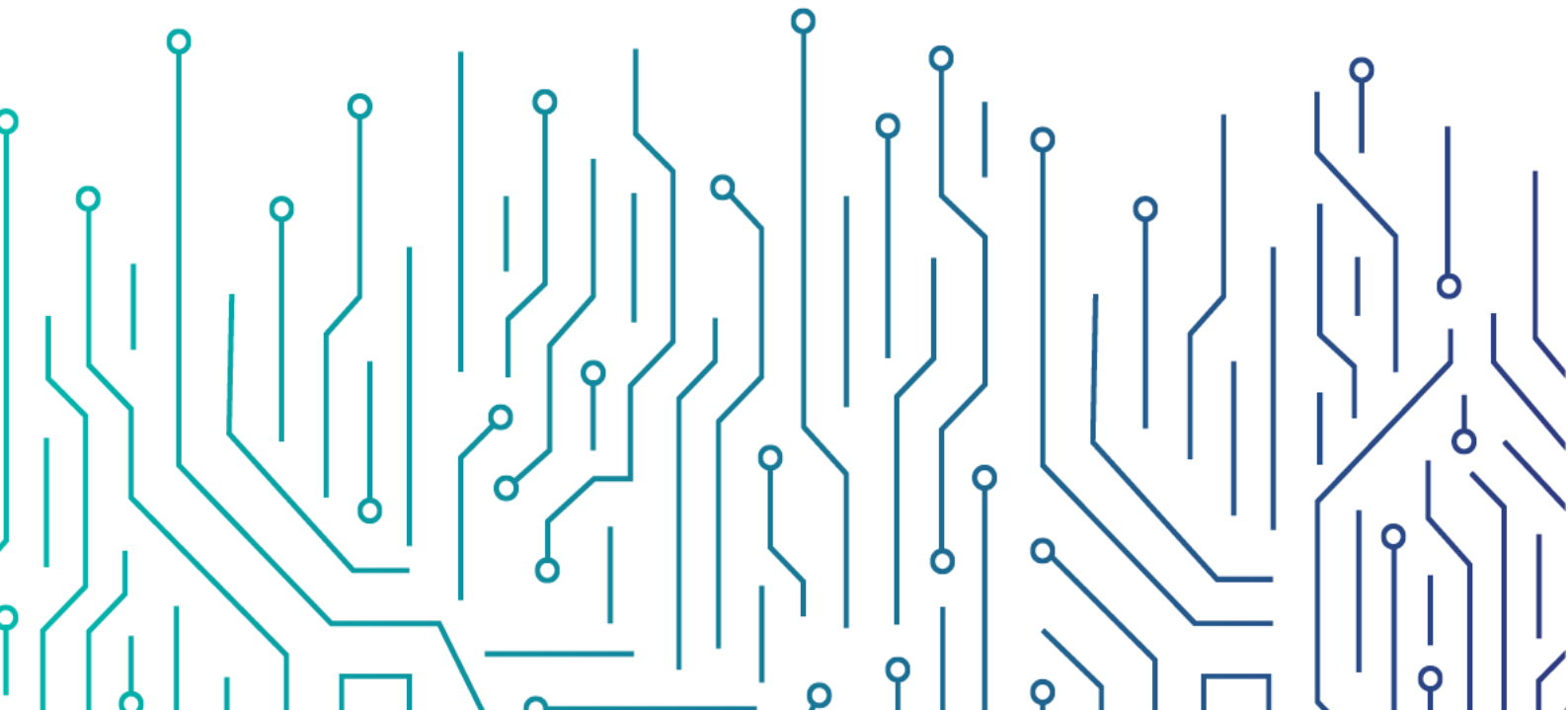
الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Data Cybersecurity Controls (DCC -1:2021)

Sharing Indicator: White

Document Classification: Public

Draft Version



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.

Table of Contents

List of Tables

List of Figures and Illustrations

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, increasing their level of transparency and responsibility, and encouraging the diversification of the economy and the use of data-based services. National data are one of the most important assets contributing to the success of the strategic goals of that Vision and are 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 or external relations, or critical infrastructures.

The NCA's mandate as per the Royal Decree number 6801, dated 11/2/1439H, makes it the national and specialized reference for matters related to cybersecurity in the kingdom. 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. They 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 for its own cybersecurity responsibilities as confirmed by Royal Decree number 57231, dated 10/11/1439H, which states that "all government organization must improve their cybersecurity level to protect their networks, systems and data, and comply with NCA's policies, framework, standards, controls and guidelines".

Data have become a key element and have a prominent role to play in the economic and development process. Interest in data is essential for effective decision-making support and contribution to the kingdom of Saudi Arabia vision 2030. And taking into consideration the growing reliance of regulators on technical means to set up, store, and share data, meant that cyber threats and risks on data are increasing, requiring that cybersecurity requirements to be set to reduce these threats and risks.

In order to reach a safe 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: 2021) to set the minimum cybersecurity requirements to enable organizations to protect their data during the entire life cycle of data. This document highlights the details of cybersecurity controls for the data, their objectives, scope of work, and the mechanism of compliance and follow-up. The organizations should take into consideration the requirements of the Critical Systems Cybersecurity Controls (CSCC-1: 2019) in the case of dealing with data that is classified at a top secret and secret levels. The organizations also 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 date 10/11/1439H.

Introduction

The National Cybersecurity Authority (referred to in this document, as "NCA") has developed the Data Cybersecurity Controls (DCC-1: 2021) after conducting a comprehensive study of multiple national and international Cybersecurity frameworks and standards, studying related national decisions, laws and regulatory requirements, reviewing and leveraging cybersecurity best practices, analyzing previous cybersecurity incidents and attacks at the national level.

Thus, based on the regulatory mandates issued by the National Data Management Office (NDMO), data are classified into four classifications based on their sensitivity and protection needs, which are: public, confidential, secret, and top secret. DCC requirements will help organizations to avoid the ever-increasing cybersecurity threats and minimize the negative impacts in order to protect the vital interests, national security, critical infrastructures, high priority sectors and governmental services and practices.

During the development of these controls, NCA considered the alignment between DCC and ECC (which is a prerequisite for compliance with DCC). The organizations must continuously comply with both in order to be fully comply (whenever applicable) with the relevant national, international and legislative, regulatory requirements.

The Data Cybersecurity Controls consist of the following

- 3 Main Domains.
- 11 Subdomains.
- 17 Main Controls
- 33 Subcontrols

Objectives

The main objectives of these controls are to:

- Raise the level of cybersecurity in order to protect national data.
- Support organizations' cybersecurity during the data lifecycle in order to protect their data and information assets from cybersecurity threats and risks.
- Raise the 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).

The NCA strongly encourages all other organizations in the Kingdom to leverage these controls to implement best practices to improve and enhance their cybersecurity.

DCC Statement of Applicability

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

Implementation and Compliance

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, periodic reports of the compliance tool or on-site audits.

Update and Review

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

DCC Domains and Structure

Main domains and subdomains of DCC

The following figure shows the main domains and subdomains of the Data Cybersecurity Controls,

Appendix (A) clarifies the relationship with the Essential Cybersecurity Controls (ECC).

1.Cybersecurity Governance	1-1	Cybersecurity Periodical 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 Processing Facilities Protection
	2-3	Mobile Devices Security	2-4	Data and Information protection
	2-5	Cryptography	2-6	Physical Security
	2-7	Cybersecurity for printers, scanners and copy machines		
3.Third-Party and Cloud Computing Cybersecurity	3-1	Third-Party Cybersecurity		

Figure (2): DCC domains and subdomains

Structure

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

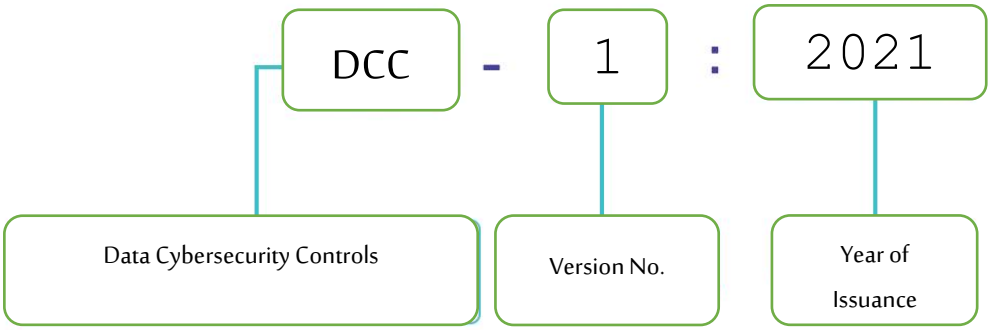


Figure (2): Controls Coding Scheme

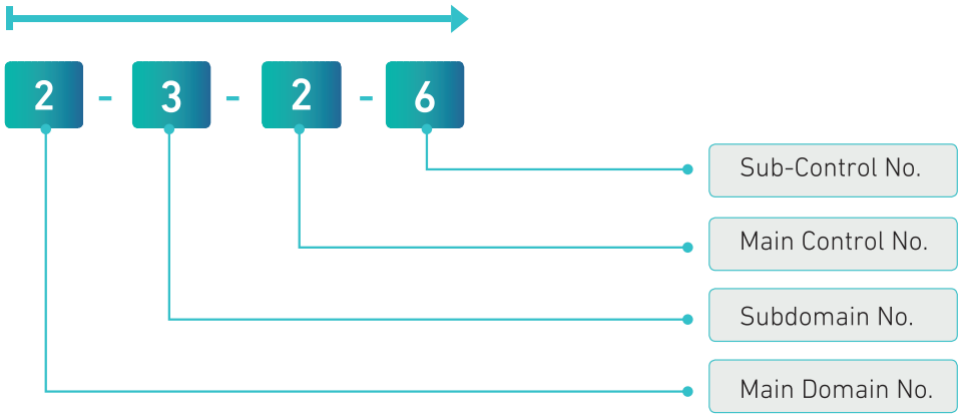


Figure (3): DCC Structure

Table (1) below shows the methodological structure of DCC

Table (1): DCC Structure

1  Reference number of the Main Domain	Name of Main Domain
Reference No. of the Subdomain	Name of Subdomain
Objective	
Controls	Public confidential Secret Top Secret
Control Reference Number	Control Clauses

Data Cybersecurity Controls

Details of the Data Cybersecurity Controls (DCC)

1. Cybersecurity Governance						
1-1	Cybersecurity Periodical 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			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 every 3 years		At least annually	
1-1-2	With reference to ECC control 1-8-1, cybersecurity review and audit must be conducted by independent parties outside the organization's cybersecurity function periodically as specified for each data classification level.		At least every 5 years		Every 3 years	
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			Classification Level			
1-2-1	In addition to the subcontrols in the ECC control 1-9-3, personnel's cybersecurity requirements 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 or vetting candidates of functions related to/ dealing with the data.			✓	✓
	1-2-12	A signed agreement by personnel pledging to not use social media and communication applications to create, store or share the organization's data, with the exception of secure communication applications approved by the relevant authorities.		✓	✓	✓

1-3	Cybersecurity Awareness and Training Program					
objective	To ensure that personnel are aware of their cybersecurity responsibilities and have the essential 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			Classification Level			
1-3-1	In addition to the subcontrols in ECC controls 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 physical).	✓	✓	✓	✓
	1-3-1-4	Secure handling when using printers, scanners and copiers.	✓	✓	✓	✓
	1-3-1-5	Secure data destruction procedures.	✓	✓	✓	✓
	1-3-1-6	Risks of sharing documents and information through unauthorized channels.	✓	✓	✓	✓
	1-3-1-7	Risks related to the use of mobile storage units.	✓	✓	✓	✓

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			Classification Level			
2-1-1	In addition to the subcontrols in ECC control 2-2-3, the cybersecurity requirements for identity and access management must include at least the following:		Public	confidential	Secret	Top Secret
	2-1-1-1	Strict restriction on accessing, viewing and sharing of data based on lists of privileges approved by the authorized person (the head of the organization or his/her delegate).			✓	✓
	2-1-1-2	Prohibiting the sharing of lists of approved privileges with unauthorized persons.		✓	✓	✓
2-1-2	Managing access identities and privileges to view data using Privileged Access Management systems			✓	✓	✓
2-1-3	With reference to ECC subcontrol 2-2-3-5, periodic review of users' identities and access rights that are used to access data.		At least annually		At least every 6 months	
2-2	Information System and Processing Facilities Protection					
objective	To ensure the protection of information systems and information processing facilities (including workstations and infrastructures) against cyber risks.					
Controls			Classification Level			
2-1-1	In addition to the subcontrols in ECC control 2-3-3, the cybersecurity requirements for Information System and Processing Facilities Protection must include at least the following:		Public	confidential	Secret	Top Secret
	2-2-1-1	Installing security patches and updates to systems and services used to handle data.	At least every 6 months		At least every 3 months	
	2-2-1-2	Reviewing the secure configuration and hardening of systems used to handle data.	At least annually		At least every 6 months	
	2-2-1-3	Reviewing and securing the default configuration (e.g., default passwords and backgrounds) of the technology assets and systems used to handle the data.	✓	✓	✓	✓
	2-2-1-4	Disabling the Print Screen or Screen Capture features for 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			Classification Level			
2-3-1	In addition to the subcontrols in ECC control 2-6-3, cybersecurity requirements for mobile devices must include at least the following:		Public	confidential	Secret	Top Secret
	2-3-1-1	Use of centralized Mobile Device Management – MDM for organization's mobile devices; and enabling the system to remotely wipe/delete mobile devices.	✓	✓	✓	✓
	2-3-1-2	Managing BYOD devices through the MDM system; and enabling the system to remotely wipe/delete mobile devices.	✓	✓	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			Classification Level			
2-4-1	In addition to the subcontrols in ECC control 2-7-3, cybersecurity requirements for data and information protection must include at least the following:		Public	confidential	Secret	Top Secret
	2-4-1-1	Use of Watermark feature to label the whole document when creating, storing, printing, or displaying the document on the screen, and making sure each copy of the document has a traceable number.			✓	✓
	2-4-1-2	Use of Data Leakage Prevention techniques.		✓	✓	✓
	2-4-1-3	Prohibiting the use of data in any environment other than the production environment, except after applying strict controls to protect that data, such as: data masking or data scrambling techniques.		✓	✓	✓
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			Classification Level			
2-5-1	In addition to the subcontrols in ECC control 2-8-3, cybersecurity requirements for cryptography must include at least the following:		Public	confidential	Secret	Top Secret
	2-5-1-1	Use of technical mechanisms and secure cryptographic algorithms for strong encryption when creating, storing, transmitting, 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	Use of technical mechanisms and secure cryptographic algorithms for strong encryption when creating, storing, transmitting, and for overall network communication medium; as per the requirements of the "moderate level" in the National Cryptographic Standards (NCS-1:2020).		✓		
2-6	Physical Security					
objective	To ensure the protection of the organization's information and technology assets from unauthorized physical access, loss, theft and damage.					
Controls			Classification Level			
			Public	confidential	Secret	Top Secret
2-6-1	With reference to ECC subcontrol 2-14-3-4, cybersecurity requirements for secure disposal and re-use of physical assets that hold classified information (including documents and storage media) must include at least the following:					
	2-6-1-1	Fully wiping the data stored on storage equipment in a secure manner.		✓	✓	✓
	2-6-1-2	Fully disposing the on premise and mobile storage equipment after completely finishing using it.			✓	✓
	2-6-1-3	Keeping a log for completed wipe and disposals operations.		✓	✓	✓
	2-6-1-4	Use of paper cross-shredding devices.			✓	✓
	2-6-1-5	Enabling and protecting CCTV logs which are used to monitor centralized printers, scanners and copy machines areas.			✓	✓
2-7	Cybersecurity for Printers, Scanners and Copy Machines					
objective	To ensure a secure hanling of data when using Printers, Scanners and Copy Machines.					
Controls			Classification Level			
			Public	confidential	Secret	Top Secret
2-7-1	Cybersecurity requirements for printers, scanners and copy machines must be defined, documented and approved.			✓	✓	✓
2-7-2	The cybersecurity requirements for printers, scanners and copy machines must be implemented.			✓	✓	✓
2-7-3	The cybersecurity requirements for printers, scanners and copy machines must include at least the following:					
	2-7-3-1	Disabling the temporary storage feature.		✓	✓	✓
	2-7-3-2	Enabling and requiring authentication for using centralized printers, scanners and copy machines.		✓	✓	✓
	2-7-3-3	Securely retaining (for a period not less than 18 months) logs of using printers, scanners and copy machines			✓	✓

2-7-4	The Implementation of the cybersecurity requirements for printers, scanners and copy machines must be reviewed periodically.	At least annually	At least every 3 months

3. 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 and managed services as per organizational policies and procedures, and related laws and regulations.					
Controls			Classification Level			
3-1-1	In addition to the controls in ECC domain 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 for outsourcing and managed services employees who have access to the data.			✓	✓
	3-1-1-2	Outsourcing and managed services must be through national providers and entities; as per related laws and regulations.			✓	✓
	3-1-1-3	Contractual commitment by third parties to securely and fully dispose the organization's data at the end of the contract or in case of contract termination, providing evidences of such disposal to the organization.		✓	✓	✓

ملاحق

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

Data Cybersecurity Controls (DCC-1:2021) is an extension to Essential Cybersecurity Controls (ECC- 1: 2018) as illustrated in figures (4) & (5) below :

- (10) subdomains, to which cybersecurity controls have been added for data cybersecurity controls.
- (19) subdomains, to which no additional 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.

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	Cybersecurity Periodical Assessment 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 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		2-6	Physical Security
	Web Application Security		2-7	Cybersecurity for printers and 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 disclo sure, 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.

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
DDoS	Distributed Denial of Service Attack
ECC	Essential Cybersecurity Controls
MDM	Mobile Device Management

Table (3): List of Abbreviations