الهيئة الوطنية للأمن السيبراني

National Cybersecurity Authority

Guide to Data Cybersecurity Controls (DCC) Implementation

(GDCC-1:2023)

TLP: white
Document Classification: Public

Disclaimer: This Guide has been developed by the National Cybersecurity Authority to enable organizations to implement the DCC. The National Cybersecurity Authority disclaims responsibility for relying solely on this document and emphasizes the importance of considering the organization's specific requirements and environment. The National Cybersecurity Authority clarifies that this guide serves as an illustrative model and does not necessarily mean that this is the only method of implementing the DCC, as long as alternative methods align with the National Cybersecurity Authority. This document contains some illustrative deliverables related to the implementation of the DCC. The assessor or auditor has the right to request other evidences as deemed necessary to ensure that all DCC are implemented.

In the Name of Allah,

The Most Gracious,

The Most Merciful

Traffic Light Protocol (TLP):

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

Red – Personal, Confidential and for 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 Restriction

Table of Contents

List of Figures

Introduction

The National Cybersecurity Authority (referred to in this document as "NCA") developed a guide for implementing the cybersecurity controls stipulated in the DCC-1: 2022 (referred to in this document as "Controls"), to enable national orgnizations to implement the requirements to comply with the DCC. This guide was developed based on the information and experiences that NCA collected and analyzed since the publication of the Controls, and was aligned with cybersecurity best practices to facilitate the implementation of the Controls across national orgnizations.

Objectives

The main objective of this guide is to enable national orgnizations to fulfill compliance requirements for implementing cybersecurity controls for data (DCC) within the organization. This aims to strengthen the cybersecurity level within the entity, reducing cybersecurity risk arising from both internal and external cyber threats.

Scope of Work

This guide's scope of work is the same as the (DCC-1:2022):

- These controls are applicable to government organizations in the Kingdom of Saudi Arabia (including ministries, authorities, establishments, and others) and their companies and entities, as well as private sector organizations owning, operating, or hosting Critical National Infrastructures (CNIs), which are all referred to herein as "The organization", in addition to consultancy services companies that work on high-sensitivity strategic projects.
- 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 Domains and Subdomains

Figure 1 below show the main domain and subdomains of DCC

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 3: DCC Main Domains and Subdomains

Structure of the Guideline

Figure 2 below shows the structure of DCC

	Name of Main Domain
Reference number of the main Domain	
Reference No. of the Subdomain	Name of the Subdomain
Objective	
Controls	
Control reference no.	Control Clauses
Relevant cybersecurity tools: Controls implementation guidelines:	
Expected deliverables:	

Figure 2: DCC Structure

DCC Implementation Guidelines

General guidelines
• Identifying the organization's data and its owners, classifying them according to relevant legislative and regulatory requirements, and conducting regular reviews. • Identify technical assets and systems that generate, process, or store the organization's data, and conducting regular reviews. • Identify and document the data cybersecurity requirements for the organization, along with associated roles and responsibilities, and obtaining approval from the authorizing official, followed by regular reviews. • Review the ECC guidelines and implement controls related to the DCC. • Develop a Data Cybersecurity Control (DCC) plan and continuously monitor its implementation.

Guidelines for Implementing Data Cybersecurity Controls

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	
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.
	Related Cybersecurity tools: • Template for Cybersecurity Auditing Procedure • Template for Cybersecurity Reviewing and Auditing Policy • Template for Cybersecurity Auditing Plan Log **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review the implementation of all Data Cybersecurity requirements in the organization as per the data classification level. • Review must be conducted at least annually across all data classification levels. • Review must be conducted at least annually for the implementation of Data Cybersecurity Controls across all data classification levels. • An approved audit plan based on the specified period of time should be documented and approved to ensure that cybersecurity controls are effectively implemented and operate in accordance with the organizational policies and procedures, as well as related national and international laws, regulations and agreements.

	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Annual review report for all data classification levels at least once a year.
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.
	Related Cybersecurity tools: • Template for Cybersecurity Reviewing and Auditing Policy **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Identify the independent parties outside the organization's cybersecurity function, such as internal audit management or third party auditors, to review and audit the implementation of Data Cybersecurity Controls in the organization. • Review must be conducted at least every 2 years or less for Public or Confidential data classification level and at least annually or less for Secret or Top Secret data classification level. • Implement Data Cybersecurity Controls by independent parties separate from the cybersecurity management within the organization, according to the specified timeframe for each level. • An approved audit plan based on the specified period of time should be documented to ensure that the cybersecurity controls are effectively implemented and operate in line with the organizational policies and procedures of the authority, the relevant national legal and regulatory requirements, and international requirements.
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Independent auditor's report that were carried out on all data cybersecurity requirements in the organization.
1-2	**Cybersecurity in Human Resources**

<table>
<tr><td>Objective</td><td colspan="2">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.</td></tr>
<tr><td colspan="3">Controls</td></tr>
<tr><td>1-2-1</td><td colspan="2">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:</td></tr>
<tr><td></td><td>1-2-1-1</td><td>Screening and vetting candidates in jobs related to data handling.</td></tr>
<tr><td></td><td colspan="2">Related Cybersecurity tools:
Template for Cybersecurity Human Resources Policy
Controls implementation guidelines:
Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials.
Identify the suitable candidates for secret and top secret data handling jobs based on the skillset and CV screening.
Review their skillset using various methodologies including interviews, skill based test, both oral as well as written. Also, develop a background verification process for the selected candidates either by an internal or third party vendor team.
Develop, document and approve an action plan for granting new access to the candidates according to the roles and permissions required.
Develop a periodic review process to delete unused and unjustified roles and permissions.</td></tr>
<tr><td></td><td colspan="2">Expected Deliverables:
Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials).
A recruitment and onboarding process which includes screening and vetting as per the skillset of the candidate.
Selection of background verification vendor or internal team.
Periodically verified and approved list of users with their permissions (e.g. Privacy/Data Protection Officer).
Review of HR Cybersecurity policy in line with data cybersecurity policies.</td></tr>
</table>

	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.
	Related Cybersecurity tools: • Template for Cybersecurity Human Resources Policy • Template for Cybersecurity Policies Compliance • Template for Confidentiality Agreement **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Identify the personnel who should be working on the confidential, secret or top secret data, based on the classification. • Review the employment agreement of the personnel and develop and document a clause with the help of legal department, pledging to not use generative artificial intelligence systems, social media, or communication applications to create, store or share the organization's data, with the exception of generative artificial intelligence systems, and secure communication applications approved by relevant authorities.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Signed agreement by the personnel on the use of generative artificial intelligence systems, social media, and communication applications.	
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		
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:	
	1-3-1-1	Risks of data leakage and unauthorized access to data during its lifecycle.

	Related Cybersecurity tools: • Cybersecurity Awareness Program Plan **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • All the personnel in the organization should be undergoing the cybersecurity awareness program for data protection and data classification, with designated awareness sessions for new personnel before granting access to organization's data. • Develop and document a data protection cybersecurity awareness program, which should include topics such as introduction to data leakage, what counts as a data leakage such as using unapproved generative artificial intelligence systems,, risks associated with data leakage, and action plan to be followed if a leakage happens or unauthorized access to data during its lifecycle. • Conduct the data protection cybersecurity awareness program on a periodic basis and maintain record of training.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented and approved customized awareness program for data protection which includes risks of data leakage and unauthorized access to data during its lifecycle. • Sample of the related awareness program components (awareness emails, awareness sessions, awareness test campaigns, etc.)	
	1-3-1-2	Secure handling of classified data while traveling and outside the workplace.
	Related Cybersecurity tools: • Cybersecurity Awareness Program Plan **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • All the personnel in the organization should be undergoing the cybersecurity awareness program for data protection.	

- Develop and document a data protection cybersecurity awareness program, which should include topics such as data introduction to data classification, data classification policy, secure handling of classified data while outside the workplace and travel.
- Conduct the data protection cybersecurity awareness program on a periodic basis and maintain record of training.

Expected Deliverables:

- Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials).
- Documented and approved customized awareness program for data protection which includes secure handling of classified data while traveling and outside the workplace.
- Sample of the awareness program components (educational email messages, awareness sessions, phishing awareness campaigns, etc.).

1-3-1-3	Secure handling of data during meetings (virtual and in-person).

Related Cybersecurity tools:

- Cybersecurity Awareness Program Plan

Controls implementation guidelines:

- Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials.
- All the personnel in the organization should be undergoing the cybersecurity awareness program for data protection.
- Develop and document a data protection cybersecurity awareness program, which should include topics such as protocols for virtual and in person meeting, meeting etiquettes, exchange of data with wider audience, proper disposal of information post recording the data during meetings.
- Conduct the data protection cybersecurity awareness program on a periodic basis and maintain record of training.

Expected Deliverables:

- Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials).
- Documented and approved customized awareness program for data protection which includes secure handling of data during meetings.
- Sample of the awareness program components (educational email messages, awareness sessions, phishing awareness campaigns, etc.).

	1-3-1-4	Secure handling when using printers, scanners and copiers.
	Related Cybersecurity tools: • Cybersecurity Awareness Program Plan **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • All the personnel in the organization should be undergoing the cybersecurity awareness program for data protection. • Develop and document a data protection cybersecurity awareness program, which should include topics such as restricted printer use from unauthorized access, remote configurations for printers and scanners, attentive to the printed data and proper disposal if data is no longer required. • Conduct the data protection cybersecurity awareness program on a periodic basis and maintain record of training.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented and approved customized awareness program for data protection which includes secure use of printers, scanners and copy machines. • Sample of the awareness program components (educational email messages, awareness sessions, phishing awareness campaigns, etc.).	
	1-3-1-5	Procedures for secure data disposal.
	Related Cybersecurity tools: • Cybersecurity Awareness Program Plan **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • All the personnel in the organization should be undergoing the cybersecurity awareness program for data protection. • Develop and document a data protection cybersecurity awareness program, which should include topics such as introduction to secure data disposal, data disposal policy, data disposal process, shredding and information about data disposal vendor, if any.	

	• Conduct the data protection cybersecurity awareness program on a periodic basis and maintain record of training.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented and approved customized awareness program for data protection which includes secure data disposal. • Sample of the awareness program components (educational email messages, awareness sessions, phishing awareness campaigns, etc.).	
	1-3-1-6	Risks of sharing documents and information through non-secure channels.
	Related Cybersecurity tools: • Cybersecurity Awareness Program Plan **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • All the personnel in the organization should be undergoing the cybersecurity awareness program for data protection. • Develop and document a data protection cybersecurity awareness program, which should include topics such as proper channels to share documents in the organization, risk associated with data leakage such as using generative artificial intelligence systems, and penalties associated with sharing documents through non-secure channels. • Conduct the data protection cybersecurity awareness program on a periodic basis and maintain record of training.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented and approved customized awareness program for data protection which includes risk of sharing documents through non-secure channels. • Sample of the awareness program components (educational email messages, awareness sessions, phishing awareness campaigns, etc.).	
	1-3-1-7	Cybersecurity risks related to the use of external storage media.
	Related Cybersecurity tools:	

	• Cybersecurity Awareness Program Plan **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • All the personnel in the organization should be undergoing the cybersecurity awareness program for data protection. • Develop and document a data protection cybersecurity awareness program, which should include topics such as storage media policy, usage of external storage media units in the organization, risk associated with data leakage from storage device, approval process for using external storage media, if required. • Conduct the data protection cybersecurity awareness program on a periodic basis and maintain record of training.
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented and approved customized awareness program for data protection which includes risk related to the use of external storage media. • Sample of the awareness program components (educational email messages, awareness sessions, phishing awareness campaigns, etc.).

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		
2-1-1	In addition to the subcontrols in ECC control 2-2-3, the cybersecurity requirements for identity and access management must cover at least the following:	
	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.
	Related Cybersecurity tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Identify the list of personnel in the organization who have access to Secret and Top Secret data, and ensure that they have Saudi nationalities. • List of privileged accesses to secret and top secret data should be approved, maintained and reviewed by the authorized person.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented and approved Privileged Access Management Policy. • Approved list of privileges for Secret and Top Secret data from the authorized person.	

	• Review of CS roles & Responsibilities policy in line with data cybersecurity policies.	
	2-1-1-2	Prohibiting the sharing of approved lists of privileges with unauthorized persons.
	Related Cybersecurity tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Inventory the approved list of privileges and work on preventing the sharing of these lists with unauthorized individuals. • Review the access provisioning process for the approved list of privileges and verify that proper approval mechanism is in place. • Periodic review of privileged access permissions to confidential, secret and top secret data should be performed.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented and approved Identity and Access Management Policy. • Maintained list of users having approved privileged accesses.	
2-1-2	Managing identities and access rights to view data using Privileged Access Management systems.	
	Related Cybersecurity tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Access to confidential, secret and top secret data should be managed using a Privileged Access Management system.	

	• Define and implement a privileged access management system, as per the requirements of the organization, to manage identities who have access rights to view data. • Verify that proper access management solution is in place for access to privileged access rights.
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Logs tracking identities with access rights to Restricted, Secret, Top secret data. • Periodically prepared review and evaluation reports. • Implementation plan for Privileged Access Management system. • Conduct regular tests on Privileged Access Management system to ensure its effectiveness. • Documents illustrating how to use asset management techniques to manage privileged accesses. • Documents illustrating maintenance and monitoring procedures for access management technologies.
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.
	Related Cybersecurity tools: • Template for Identity and Access Management Standards, encompassing password management • Template for Identity and Access Management Policy **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Develop and document procedures and an action plan for periodic review of users' privileged access rights in case of personnel roles changes. • Review should be conducted at least annually for Public or Confidential data classification level and at least every three months or less for Secret or Top Secret data classification level.
	Expected Deliverables:

	• Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Action plan for periodic review of users' identities and access rights. • Sample reports of the periodic review of users' identities and access rights that have been conducted.

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		
2-2-1	In addition to the subcontrols in ECC control 2-3-3, cybersecurity requirements for Information System and Processing Facilities Protection must include at least the following:	
	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.
	Related Cybersecurity tools: • Template for Patch and Update Management Policy • Template for Patch and Update Management Standard **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Identify the systems and services handling data across all classification. • Review the patching guidance with respect to the systems and services utilized and document the patching procedures to be followed in line with the guidance. • Periodic security patching and updates should be conducted at least every month or earlier for systems and services handling Public or Confidential data and immediately for systems and services handling Secret or Top Secret data.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented security patching procedures for systems and services handling data.	

	• Patching review report for periodic security patching.	
	2-2-1-2	Reviewing the secure configuration and hardening of systems used to handle data as specified for each data classification level.
	Related Cybersecurity tools: • Template for Patch and Update Management Policy • Template for Configuration and Hardening Policy • Template for Configuration and Hardening Standard **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Identify the systems handling data across all classification. • Review the security configuration guidance with respect to the systems utilized and document the hardening procedures to be followed in line with the guidance. • Periodic security configuration and hardening should be conducted at least annually or earlier for systems handling Public or Confidential data and at least every 6 months or earlier for systems and services handling Secret or Top Secret data.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Approved standard for reviewing security configuration and hardening for data processing systems (e.g., approved hard copy or electronic version). • Reports indicating that security configuration and hardening for systems used for data handling are reviewed according to the timeframe for each level.	
	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.
	Related Cybersecurity tools: • Template for Patch and Update Management Policy **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials.	

	• Identify the technology assets and systems handling data across all classification. • Review the default configurations which includes, but not limited to, default passwords, guests accounts, service accounts, backgrounds, default administrators, legacy protocols, open ports in the system. • Verify and ensure that the security configurations should not be set as default for the technology assets.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Default configuration review report for technology assets.	
	2-2-1-4	Disabling the Print Screen or Screen Capture features on the devices that create or process documents.
	Controls implementation guidelines: • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Identify the devices that process Secret and Top Secret data of the organization. • Review and verify the Print Screen or Screen Capture features on the devices and ensure that they are disabled in the system.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Review report that verifies that devices' print screen feature is disabled on devices that handles Secret and Top secret documents. • Sample of the system security configurations.	

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	

<table>
<tr><td rowspan="5">2-3-1</td><td colspan="2">In addition to the subcontrols in ECC control 2-6-3, cybersecurity requirements for mobile devices must cover at least the following:</td></tr>
<tr><td>2-3-1-1</td><td>Centrally managing the organization's owned mobile devices using Mobile Device Management (MDM) system and activating the remote wipe feature.</td></tr>
<tr><td colspan="2">Related Cybersecurity Tools:
Template for User Devices, Mobile Devices, and Personal Devices Security Policy
Template for Mobile Devices Security Standard
Controls implementation guidelines:
Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials.
Identify the list of mobile devices in the organization that store, use and process organization's data.
Define and implement a Mobile Device Management (MDM) system, as per the requirements of the organization, to manage the mobile devices who have access to data.
Review that the MDM system should have remote swipe functionality enabled in all the devices.</td></tr>
<tr><td colspan="2">Expected Deliverables:
Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials).
Documented list of all the mobile devices in the organization handling the data.
Implementation plan for Mobile Device Management (MDM) system.
Screenshot of Mobile Device Management (MDM) system in use.
Sample of related Mobile Device Management (MDM) configurations.</td></tr>
<tr><td>2-3-1-2</td><td>Centrally managing BYOD devices using Mobile Device Management (MDM) system and activating the remote wipe feature.</td></tr>
<tr><td colspan="2">Related Cybersecurity Tools:
Template for User Devices, Mobile Devices, and Personal Devices Security Policy
Controls implementation guidelines:
Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials.</td></tr>
</table>

	• Identify the list of personnel's mobile devices outside the organization that store, use and process organization's data. • Define and implement a Mobile Device Management (MDM) system, as per the requirements of the organization, to manage the mobile devices who have access to organization's public and confidential data. • Review that the MDM system must have remote swipe/delete functionality enabled in all the BYOD devices. • Verify that BYOD devices should not have access to any secret or top secret data of the organization. • Ensure that BYOD devices are not used for any secret or top secret data.
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented list of all the personnel's mobile devices outside the organization handling the organization's data. • Implementation plan for Mobile Device Management (MDM) system for BYOD devices.

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		
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:	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Data Protection Policy • Template for Cybersecurity Data Protection Standard **Controls implementation guidelines:**	

	• Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review and select the software or system, used to create, store, print and display data in the organization, that has the capability to label data using watermark as per the data classification and unique traceable number throughout the document's lifecycle. • Implement the above said features for all the secret and top secret data documents while creating, storing, printing or displaying the document. • Identify and define the data classification policy to include the watermark labelling and unique traceable features for the organization's documents.
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Implementation plan for Watermark and unique traceable number feature in document software or system. • Documented and approved data cybersecurity policy which includes the documentation features for secret and top secret data. • Sample of a document labelled with watermark.
	2-4-1-2 — Using Data Leakage Prevention technologies and Rights Management technologies.
	Related Cybersecurity Tools: • Template for Cybersecurity Data Protection Policy • Template for Cybersecurity Data Protection Standard **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Define and document Data Leakage Prevention (DLP) and Rights Management standards. • Identify and implement the Data Leakage Prevention (DLP) and Rights Management systems as per the requirements for confidential, secret and top secret data. • Review the Data Leakage Prevention techniques that should include, but not limited to, rule for incident identification, message filtering mechanism, data leak prevention for

	endpoints, network, cloud and/or storage, content filtering capabilities, incident response and remediation. • Review the Rights Management techniques that should include, but not limited to, automated provisioning, privileged activity monitoring, login auditing, password management utilities, LDAP entry management, two factor authentication.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented Data Leakage Prevention standard. • Implementation plan for Data Leakage Prevention (DLP) system. • Implementation plan for Rights Management system. • Screenshot of Data Leakage Prevention (DLP) and Rights Management systems in use. • Sample of Data Leakage Prevention (DLP) and Rights Management systems' configurations.	
	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.
	Related Cybersecurity Tools: • Template for Cybersecurity Data Protection Policy **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Identify and maintain record of all the environments other than production environment. • Review and verify that migration of restricted, secret and top secret data in the production environment is not allowed in the non-production environments. However, in case of business requirements, appropriate checks and controls should be applied, which includes, but not limited to, data masking/data scrambling, data purging, data anonymization, appropriate business and technical approvals of requirements, information security assessment.	

	• Develop and document cybersecurity controls that include data migration risk assessment, protection of data during migration through protection techniques (e.g. data masking, data scrambling, etc.) • Develop and document procedures about migration of production data in non-production environments.
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented procedures and controls about migration of production data into other environments.
	2-4-1-4 Using brand protection service to protect the organization's identity from impersonation.
	Related Cybersecurity Tools: • Template for Data Loss Prevention Standard **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Identify and maintain record of all the identities in the organization brand online that might be prone to impersonation. • Review the available vendors that provide brand protection services and analyse the suitability of the service based on the requirements of the organization. • Review and implement the brand protection service for the organization's identities.
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented list of identities in the organization that are prone to impersonation. • Implementation plan of vendor brand protection service. • Sample of brand protection reports and alerts.

2-5	**Cryptography**

Objective	To ensure the proper and effcient use of cryptography to protect information assets as per organizational policies and procedures, and related laws and regulations.	
Controls		
2-5-1	In addition to the subcontrols in ECC control 2-8-3, cybersecurity requirements for cryptography must cover at least the following:	
	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).
	Related Cybersecurity Tools: • Template for Encryption Standard • Template for Encryption Policy • Template for Encryption Key Management Standard **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Identify and document all the cryptographic algorithms for both data at rest and data in transit state of the secret and top secret data of the organization. • Review and verify the cryptographic algorithms used in the organization for the abovementioned data are aligned with the requirements of the "advanced level" in NCA National Cryptographic Standards (NCS-1:2020).	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented cryptographic technologies used for secret and top secret data of the organization. • Sample of encryption system's configurations.	
	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).
	Related Cybersecurity Tools:	

	• Template for Encryption Policy • Template for Encryption Key Management Standard **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Identify and document all the cryptographic algorithms for both data at rest and data in transit state of the confidential data of the organization. • Review and verify the cryptographic algorithms used in the organization for the abovementioned data are aligned with the requirements of the "moderate level" in NCA National Cryptographic Standards (NCS-1:2020).
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented cryptographic technologies used for confidential data of the organization.

2-6	**Secure Data Disposal**	
Objective	To ensure a secure data disposal as per organizational policies and procedures, and related laws and regulations.	
Controls		
2-6-1	Cybersecurity requirements for secure data disposal must cover at least the following:	
	2-6-1-1	Identification of technologies, tools and procedures for the implementation of secure data disposal according to the data classification level.
	Related Cybersecurity tools: • Template for Physical Security Cybersecurity Policy • Template for Physical Security Standards **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials.	

- Identify the list of on premises and mobile storage physical assets such as external hard drives, tape drives, optical storage devices, flash storage etc. in use for storage of confidential, secret and top secret data of the organization.
- Define and document the data disposal plan for the above mentioned storage devices in a secured manner.
- Review the data disposal techniques used for secure data disposal which should include, but not limited to, data wiping using third party software, overwriting, reformatting; data destruction using physical destruction of storage asset using vendor services.

Expected Deliverables:

- Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials).
- Documented list of storage assets handling confidential, secret or top secret data.
- Documented data disposal plan for storage equipments.

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.

Related Cybersecurity tools:

- Template for Physical Security Standards

Controls implementation guidelines:

- Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials.
- Implement secure destruction of storage media when they are no longer in need for use.
- Define and document the data disposal plan for the above mentioned storage devices in a secured manner.
- Review and implement the device destruction techniques used in the process for device disposal that ensure permanent destruction beyond recovery. Further, in case of third party service to be utilized, review, verify and approve as per the requirements of the organization.

	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented list of on premises and mobile storage physical assets in use for storage of confidential, secret and top secret data of the organization. • Documented data disposal procedure for storage media. • Implementation plan of third party service for data device disposal, if required. • Sample of disposal records/reports.	
	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.
	Related Cybersecurity tools: • Template for Physical Security Standards **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Define and document the data erasure plan for the above mentioned data in a secured manner. • Review and implement the data wiping techniques used in the process for data wiping that ensure permanent wiping of data beyond recovery, without any damage to the usability of the device. Further, in case of third party software or service to be utilized, review, verify and approve as per the requirements of the organization.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented list of storage assets handling restricted, secret or top secret data. • Documented data erasure plan for storage equipments. • Implementation plan data erasure, including actions of third party software or service for data wiping, if required.	
	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.

	Related Cybersecurity tools: • Template for Physical Security Standards **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review the implementation plan secure data disposal operations in the organization for the storage media handling confidential, secret or top secret data. • Verify that for all the storage media, appropriate implementation plan steps are followed as per the requirement of either data erasure or media disposal. Further, verify that all the proper approvals and sign offs are provided prior to the hand off and conorganizationation of data disposal is provided.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Implementation plan data erasure, including actions of third party software or service for data wiping, if required. • Document trail of proper data disposal steps is maintained.	
	2-6-1-5	Keeping a record of all secure data disposal and erasure operations that have been conducted.
	Controls implementation guidelines: • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review the data disposal action plan in place and conorganization that it should include the monitoring and logging of data and devices in the organization. It should also maintain the status of all the in scope data storage assets and log any changes to the status as per the defined rules by the organization. • Review and implement any third party software or service to be utilized to monitor and log the data storage assets' operations.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials).	

	• Maintained list of all the data storage assets in the organization with their status and other relevant parameters. • Implementation plan of monitoring of data disposal, including actions of third party service for data storage assets' operations, if required. • Sample of disposal and erasure records/reports.
2-6-2	The implementation of the secure data disposal requirements must be reviewed as specified for each data classification level.
	Related Cybersecurity tools: • Template for Physical Security Cybersecurity Policy **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review the process of secure data disposal techniques with respect to the implementation plan and data disposal policy. • Periodic review of data disposal process for storage devices must be conducted at least annually or less for Public or Confidential data classification level and at least every 6 months or less for Secret or Top Secret data classification level, to ensure that the requirements are effectively implemented.
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Review report of secure data disposal process.

2-7	Cybersecurity for Printers and Scanners and Copy Machines
Objective	To ensure secure handling of data when using Printers, Scanners and Copy Machines.
Controls	
2-7-1	Cybersecurity requirements for printers, scanners and copy machines must be defined, documented and approved.
	Controls implementation guidelines:

	• Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review the cybersecurity requirements for printers, scanners and copy machines handling confidential, secret and top secret data of the organization. • Define, document and approve the security configuration and hardening policy for the organization to ensure appropriate use of organization's printers, scanners and copy machines by authorized personnel.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials).	
2-7-2	Cybersecurity requirements for printers, scanners and copy machines must be implemented.	
	Controls implementation guidelines: • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review the cybersecurity requirements for printers, scanners and copy machines handling confidential, secret and top secret data of the organization. • Implement the security configuration and hardening policy for the organization to ensure appropriate use of organization's printers, scanners and copy machines by authorized personnel. This should include, but not limited to, placement of the devices, configuration of the devices, access management to the devices, patching, logging and monitoring, disabling default configurations among other requirements.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Implemented cybersecurity requirements for printers, scanners, and copy machines within the organization.	
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.

	Controls implementation guidelines: • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review and implement the printers, scanners and copy machine devices' settings for temporary storage and ensure that the feature is disabled for devices handling confidential, secret and top secret data of the organization.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Implementation of disabling temporary storage feature in printers, scanners and copy machines of the organization.	
	2-7-3-2	Enabling authentication on centralized printers, scanners and copy machines and requiring it before usage.
	Controls implementation guidelines: • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review and implement the printers, scanners and copy machine devices' authentication settings and ensure that it is enabled for all the authorized personnel accessing the confidential, secret and top secret data of the organization.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Implementation of enabling authentication for centralized printers, scanners and copy machines.	
	2-7-3-3	Securely retaining (for a period not less than 12 months) logs of printers, scanners and copy machines usage.
	Controls implementation guidelines: • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review and implement the printers, scanners and copy machine devices' logging settings and ensure that it is logs are retained for devices handling secret and top secret data of the organization for a period not less than 12 months. • The electronic log should contain records of what has been printed, scanned, copied. Additionally, Hashing can be used to create a digital signature for documents or files and to verify their integrity by determining if they were altered or modified.	
	Expected Deliverables:	

	• Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Implementation of retention of logs for printers, scanners and copy machines.	
	2-7-3-4	Enabling and protecting CCTV logs which are used to monitor centralized printers, scanners and copy machines areas.
	Controls implementation guidelines: • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review and implement the CCTV setup in the organization to ensure that monitoring of assets related to secret and top secret data such as centralized printers, scanners and copy machines. • Verify that the logging of CCTV of the above mentioned setup is enabled and stored as per the data disposal policy. • Review that the access to the CCTV logs is restricted only to authorized personnel. • Periodic review of access to CCTV logs should be performed to ensure that only authorized personnel have access to them.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Implementing logging of CCTV cameras monitoring centralized printers, scanners and copy machines. • Review of access to CCTV logs to authorized personnel only.	
	2-7-3-5	Using cross-shredding devices, to securely dispose documents when no longer needed.
	Controls implementation guidelines: • Identify the requirements of this control and document them in a cybersecurity requirements document for secure data disposal in all its forms, both soft and hard copies, followed by approval from the authorizing officials. • Ensure that physical copies of secret and top secret data are shredded, if not in use. This should be implemented by placing cross-shredding devices in the organization premises. • Review the data retention policy for shredding of physical copies in case of end of retention period of data.	

	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Providing shredding devices in the organization's buildings for proper disposal of paper documents.
2-7-4	Implementation of cybersecurity requirements for printers, scanners and copy machines must be reviewed as specified for each data classification level.
	Controls implementation guidelines: • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Periodic review of printers, scanners and copy machine devices' cybersecurity requirements should be carried out on at least annually for devices handling public and confidential data and at least every 3 months for devices handling secret and top secret data.
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Implementation of periodic reviews for printers, scanners and copy machines.

3 Third-Party Cybersecurity 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		
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:	
	3-1-1-1	Screening or vetting third-party employees who have access to the data.
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review their skillset using various methodologies including RFPs, candidate CV, accreditation among others. Also, develop a background verification process for the selected outsourced employees either by an internal or third party vendor team. • Develop, document and approve an action plan for granting new access to the candidates according to the roles and permissions required. • Develop a periodic review process to delete unused and unjustified roles and permissions.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • A recruitment and onboarding process which includes screening and vetting as per the skillset of the third-party employees. • Selection of background verification vendor or internal team. • Periodically verified and approved list of users with their permissions. • Review of HR Cybersecurity policy in line with data cybersecurity policies.	

	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.
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review the service level agreement between the organization and the third parties with respect to the confidential, secret and top secret data handling of the organization. • Verify that the end of service clause in the agreement defines and documents proper data disposal of organization's data as per the data disposal policy. Further, verify that the third parties should also provide evidence of data disposal to the organization.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented procedures for third parties in data disposal policy of the organization for confidential, secret and top secret data. • Review of service level agreement for proper data disposal in the end of service.	
	3-1-1-3	Documenting all data sharing operations within third-parties, including data sharing justification.
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review the service level agreement between the organization and the third parties with respect to the confidential, secret and top secret data sharing operations of the organization within the third-parties.	

	• Define and implement the clause related to data sharing in the agreement., which should include, but not limited to, description of data shared, restrictions of data usage, required data protection safeguards and justification related to sharing of data. • Verify and document the organization's data flow to the third parties only after appropriate data sharing justification is provided.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented procedure for data sharing operations with the third-parties. • Review of service level agreement for proper process for data sharing operations with the third-parties.	
	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.
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review the service level agreement between the organization and the third parties with respect to the cross border data transfer of the organization's confidential, secret and top secret data outside the kingdom. • Verify and define the data protection standards and laws followed by hosting organization outside the kingdom, to safeguard the organization's data. Further, obtain the written approval from the Authorizing Official to transfer the data outside the kingdom, in accordance with the related laws and regulations. • Verify the other required regulatory requirement such as data subject consent requirements, impact assessment for cross border data transfer outside the kingdom.	
	Expected Deliverables:	

	• Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented procedure for cross border data transfer of the organization outside the kingdom. • Review of service level agreement for proper process for cross border data transfer with the third-parties.	
	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.
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • Review the service level agreement between the organization and the third parties with respect to the incident that may affect confidential, secret and top secret data. • Verify and define the process to notify the organization in case of a cybersecurity incident which might have led to an exposure to the organization's data. Further, also define specific SLA timelines that third-parties have to follow for prompt notification to the organization.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented procedure for cybersecurity incident notification related to the data of the organization. • Review of service level agreement for proper process for cybersecurity incident notification with the third-parties.	
	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.
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:**	

<table>
<tr><td></td><td>

Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials.
Verify and define the process to reclassify the data to the least level to make sure that only required data is sent across to the third -party and any unintended data for them must not be sent. This can be achieved by various data hiding techniques, such as, but not limited to, data masking, data anonymization, data scrambling, data filtering.

Expected Deliverables:

Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials).
Documented procedure for data hiding on outgoing data sent by the organization.

</td></tr>
<tr><td>3-1-2</td><td>
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:
<table>
<tr><td>3-1-2-1</td><td>Screening or vetting consultancy services employees who have access to the data.</td></tr>
</table>
Related Cybersecurity tools:

Template for Cybersecurity Policy Related to Third-Parties

Controls implementation guidelines:

Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials.
Enforce consultancy services companies that are working on strategic projects to provide screening or vetting data for employees wokring on thsse projects, and consultancy services companies should coaporate with the organization in this matter.
Review and assess the candidates' skills and competencies using various methodologies including interviews, and oral and written test. Furthermore, consider the candidate' screening or vetting results that are selected either by an internal or third party vendor team.
Review their skillset using various methodologies including RFPs, candidate CV, accreditation among others. Also, develop a background verification process for the selected outsourced employees either by an internal or third party vendor team.
Develop, document and approve an action plan for granting new access to the candidates according to the roles and permissions required.
Develop a periodic review process to delete unused and unjustified roles and permissions.

</td></tr>
</table>

	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Document outlining the provision of employee data by consulting services company required to conduct security screenings for personnel working on strategic projects within the organization. • Document outlining the completion of the security screening process for employees of consulting services companies by the organization. • A recruitment and onboarding process which includes screening and vetting as per the skillset of the consultancy services employees. • Selection of background verification vendor or internal team. • Verified and approved list of users with their permissions. • Review of HR Cybersecurity policy in line with data cybersecurity policies.	
	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.
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • The organization should work on obtaining assurances from consulting services companies and their employees working on strategic projects regarding non-disclosure of information and their ability to securely delete the organization's data upon the termination of the contractual relationship. Additionally, they should refrain from disclosing any information before obtaining written consent from the organization. Consulting services companies are required to cooperate with the organization in implementing this procedure. • Review the service level agreement between the organization and the consultancy services organization with respect to the confidential, secret and top secret data handling of the organization. • Verify that the end of service clause in the agreement defines and documents proper data disposal of organization's data as per the data disposal policy. Further, verify that the	

	consultancy services organization should also provide evidence of data disposal to the organization.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Document outlining the inclusion of clauses regarding confidentiality, non-disclosure of data, and secure data deletion to ensure consulting services companies and their employees do not disclose the organization's information (Hard or soft copy). • Documented procedures for consultancy services organization in data disposal policy of the organization for confidential, secret and top secret data. • Review of service level agreement for proper data disposal in the end of service.	
	3-1-2-3	Documenting all data sharing operations within consultancy services, including data sharing justification.
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • The organization should document the process of sharing data with consulting services companies involved in strategic projects based on the principle of Need-to-Know. • Consulting services companies involved in strategic projects should ensure the documentation of data sharing with authorized employees based on the principle of Need-to-Know. • Review the service level agreement between the organization and the consultancy services with respect to the confidential, secret and top secret data sharing operations of the organization within the third-parties. • Define and implement the clause related to data sharing in the agreement., which should include, but not limited to, description of data shared, restrictions of data usage, required data protection safeguards and justification related to sharing of data. • Verify and document the organization's data flow to the consultancy services only after appropriate data sharing justification is provided.	
	Expected Deliverables:	

	• Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented procedure for data sharing operations with the consultancy services. • Review of service level agreement for proper process for data sharing operations with the consultancy services.	
	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.
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • The organization must mandate consulting services companies working on strategic projects to inform them in the event of a cybersecurity incident affecting the shared data, and to cooperate with the organization in implementing this procedure. • Review the service level agreement between the organization and the consultancy services with respect to the incident that may affect confidential, secret and top secret cross border data. • Verify and define the process to notify the organization in case of a cybersecurity incident which might have led to an exposure to the organization's data. Further, also define specific SLA timelines that consultancy services have to follow for prompt notification to the organization.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented procedure for cybersecurity incident notification related to the data of the organization. • Review of service level agreement for proper process for cybersecurity incident notification with the consultancy services.	
	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.
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties	

Controls implementation guidelines:

- Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials.
- The organization must mandate consulting services companies working on strategic projects to use data within the scope defined by the organization, and to cooperate with the organization in implementing this procedure.
- Verify and define the process to reclassify the data to the least level to make sure that only required data is sent across to the consultancy services and any unintended data for them must not be sent. This can be achieved by various data hiding techniques, such as, but not limited to, data masking, data anonymization, data scrambling, data filtering.

Expected Deliverables:

- Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials).
- Documented procedure for reclassifying data to the lowest level that achieves the objective before sharing it (e.g. data masking, data anonymization, data scrambling, data filtering).

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.

Related Cybersecurity tools:

- Template for Cybersecurity Policy Related to Third-Parties

Controls implementation guidelines:

- Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials.
- The organization must mandate consulting services companies working on strategic projects involving secret and top secret data not to use open and non-designated rooms for consultancy services employees, and not to use devices not owned by the organization. It is also the responsibility of the consulting services companies to cooperate with the organization in implementing this procedure.
- Review the service level agreement between the organization and the consultancy services with respect to the dedicated closed room and devices that utilize secret and top secret organization data.
- Verify and define a dedicated closed room where the consultancy services employees can dedicatedly provide service to the organization. Further, provide organization's devices for them to share and process data.

	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented procedure for handling closed room workspace and data handling devices for consultancy services employees. • Evidence illustrating that the consulting services companies are compliant with not using non-designated rooms for consultancy services employees. • Review of service level agreement for using dedicated workspace and devices for the consultancy services employees.	
	3-1-2-7	Activating access control system to allow only authorized access to the closed room.
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • The organization must mandate consulting services companies working on strategic projects involving secret and top secret data to use access control systems for entry and exit from designated rooms for authorized consultancy services employees, according to their permissions. Consulting services companies should cooperate with the organization in implementing this procedure. • Review the service level agreement between the organization and the consultancy services with respect to the access control to the closed room for handling secret and top secret organization data. • Verify and define a dedicated closed room as an access controlled space where only authorized consultancy services employees can have access to the organization's data and data storage devices.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented procedure for activating access control system to the closed room workspace for consultancy services employees. • Review of service level agreement for using dedicated access controlled workspace for the consultancy services employees.	

	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.
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:** • Identify the requirements of this control and document them in a cybersecurity requirements document, followed by approval from the authorizing officials. • The organization must mandate consulting services companies working on strategic projects involving secret and top secret data to prohibit the entry of devices not owned by the organization and to prevent taking out storage media and devices from the closed rooms designated for consultancy services employees. • Review the service level agreement between the organization and the consultancy services with respect to the storage media and device used to handle secret and top secret organization data. • Verify and define the procedures which prevent carrying the storage devices and media dealing with organization's data outside the closed room. Further, verify that no other storage media must be allowed to enter the closed room. This should be implemented using security checks at the entry and exit from the closed room.	
	Expected Deliverables: • Document detailing the identification and documentation of the requirements of this control (e.g. a policy and/or procedure approved by the authorizing officials). • Documented procedure for restrictions on storage devices during the entry and exit of closed room workspace for consultancy services employees. • Review of service level agreement for proper usage of organization's storage media by consultancy services employees.	


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority