الهيئــــة الوطنيــــة
للأمـــن السيبـــراني

National Cybersecurity Authority

Guide to Telework Cybersecurity Controls Implementation

(GTCC-1:2023)

Sharing Indicator: white
Document Classification: Public

Disclaimer: This Guide has been developed by the National Cybersecurity Authority to enable organizations to implement the Telework Cybersecurity Control (TCC). The National Cybersecurity Authority must not be responsible for relying on this document only. It emphasizes the need to take into account the requirements of the organization and its environment. The National Cybersecurity Authority confirms that this document is only a guide that can be used as an illustrative model and does not necessarily mean that this is the only method of implementing TCC, provided that other methods do not conflict with the requirements of the National Cybersecurity Authority. This document contains some illustrative deliverables related to the TCC implementation. The assessor or auditor has the right to request other evidences as deemed necessary to ensure that all TCC 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 TCC-1: 2021 (referred to in this document as “Controls”), to enable national organizations to implement the requirements to comply with the TCC. 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 entities.

Objectives

The main objective of this guide is to enable national entities to fulfill compliance requirements for the TCC implementation, strengthen their cybersecurity, and reduce cybersecurity risks that may arise from internal and external cyber threats.

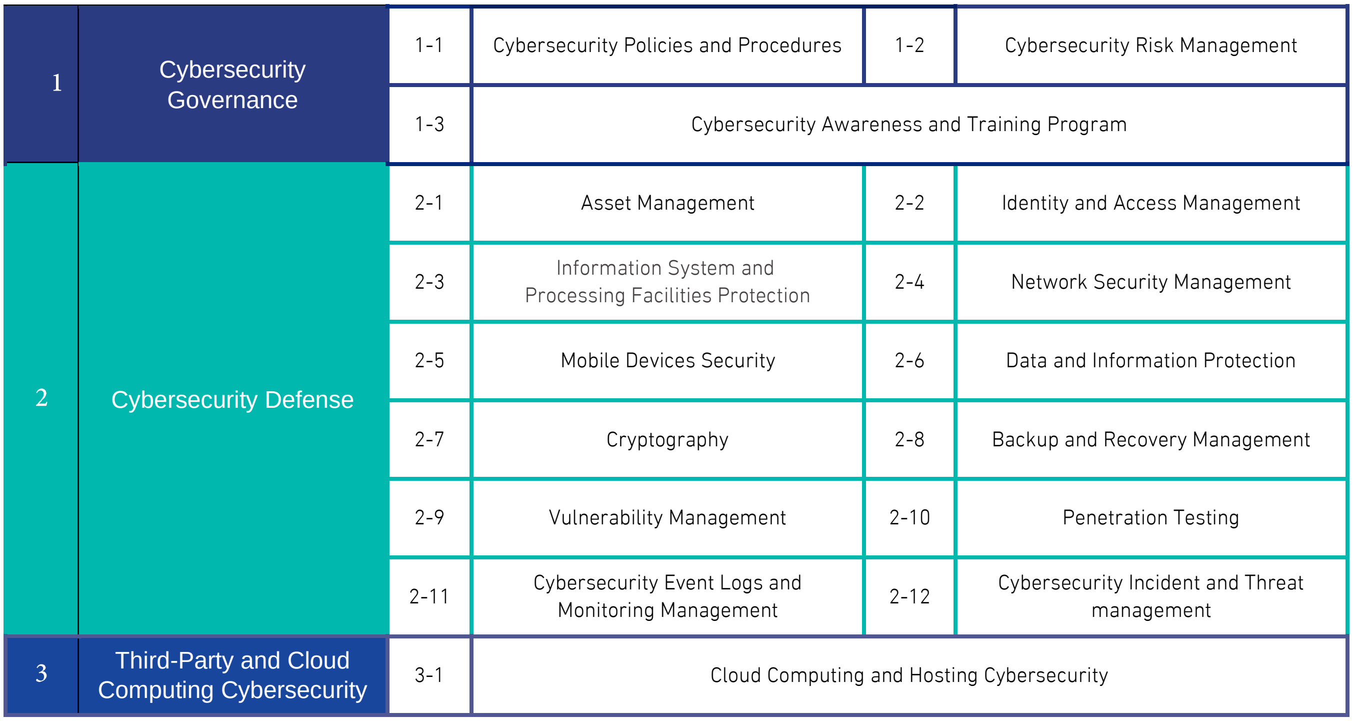
Scope of Work

This guide's scope of work is the same as the TCC-1:2022's:

- 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”.
- The NCA strongly encourages all other organizations in the Kingdom to leverage this guide, to take advantage of these controls, and to implement best practices to improve and enhance their cybersecurity.

TCC Domains and Subdomains

Figure 1 below show the main domain and subdomains of TCC

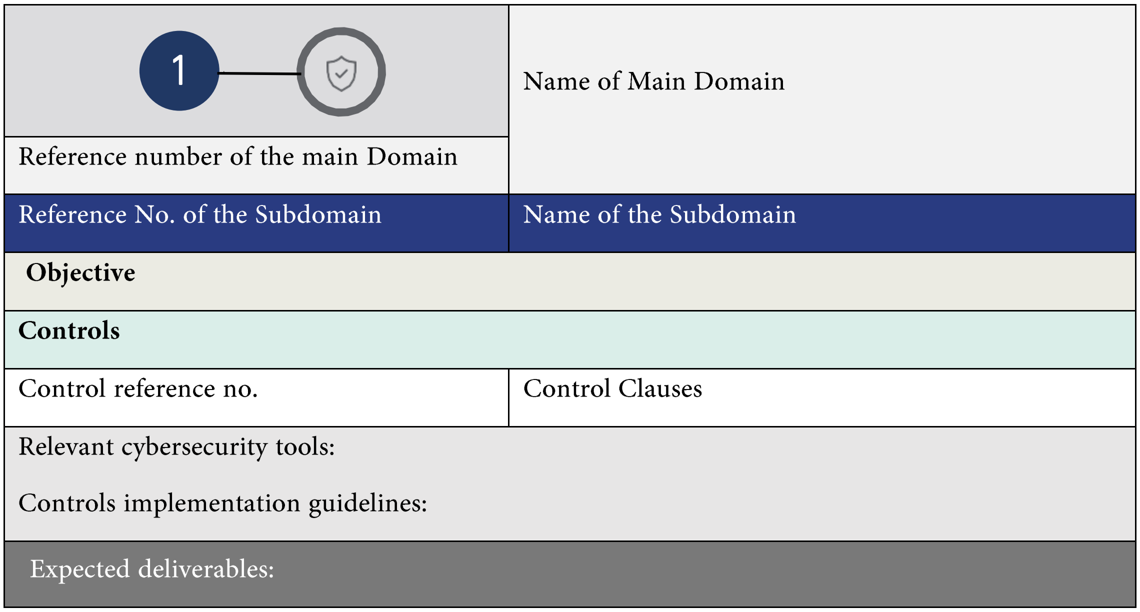


1	Cybersecurity Governance	1-1	Cybersecurity Policies and Procedures	1-2	Cybersecurity Risk Management
		1-3	Cybersecurity Awareness and Training Program		
2	Cybersecurity Defense	2-1	Asset Management	2-2	Identity and Access Management
		2-3	Information System and Processing Facilities Protection	2-4	Network Security Management
		2-5	Mobile Devices Security	2-6	Data and Information Protection
		2-7	Cryptography	2-8	Backup and Recovery Management
		2-9	Vulnerability Management	2-10	Penetration Testing
		2-11	Cybersecurity Event Logs and Monitoring Management	2-12	Cybersecurity Incident and Threat management
3	Third-Party and Cloud Computing Cybersecurity	3-1	Cloud Computing and Hosting Cybersecurity		

Figure 3: TCC Main Domains and Subdomains

Structure of the Guideline

Figure 2 below show the structure of TCC



1	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: TCC Structure

TCC Implementation General Guidelines

-	General Guidelines
	Control implementation guidelines: ● List all services and systems that are accessed remotely, and review them periodically. ● List all Privileged Accounts that have the ability to manage and access telework systems, and review them periodically. ● Identify and document the entity's cybersecurity requirements for telework and the roles and responsibilities related to them, and have them approved by the authority holder and reviewed periodically. ● Review the guideline for implementing basic cybersecurity controls (ECC), and implement controls related to cybersecurity controls for telework. ● Develop a plan to implement cybersecurity controls for telework, and follow it continuously.

TCC Implementation Guidelines

1 (Cybersecurity Governance)

<table>
<tr><th>1-1</th><th colspan="2">Cybersecurity Policies and Procedures</th></tr>
<tr><td>Objective</td><td colspan="2">To ensure that cybersecurity requirements are documented, communicated and complied with by the organization as per related laws and regulations, and organizational requirements.</td></tr>
<tr><td colspan="3">Controls</td></tr>
<tr><td rowspan="3">1-1-1</td><td colspan="2">Referring to control 1-3-1 in the ECC, cybersecurity policies and procedures must cover, at a minimum, the following:</td></tr>
<tr><td>1-1-1-1</td><td>Defining and documenting the telework cybersecurity requirements and controls as part of the organization’s cybersecurity policies.</td></tr>
<tr><td colspan="2">**Related Cybersecurity Tools:**
● Procedure for Development of Cybersecurity Documents Template
Controls implementation guidelines:
● Develop and document cybersecurity policies for telework, which may include, but is not limited to:
○ Assess cybersecurity risks of telework systems, at least once a year.
○ Assess cybersecurity risks when planning and before allowing telework for any service or system.
○ Include cybersecurity risks related to telework systems, services, and systems allowed to work remotely, in the entity’s cybersecurity risk register, and follow up on it at least once a year.
○ Secure usage and protection of devices designated for telework.
○ Secure handling of login ID’s and passwords.
○ Protecting data that is saved on devices used for telework and handling it according to its classification and the entity’s procedures and policies.
○ Secure handling of applications and solutions used for telework, such as virtual meetings, collaboration and file sharing.
○ Secure handling of home networks and ensuring their protection settings.</td></tr>
</table>

	○ Avoid working remotely using unreliable public devices or networks or while in public places. ○ Avoid unauthorized physical access, loss, theft and vandalism of technical assets and telework systems. ○ Communicate directly with the department concerned with cybersecurity in the entity if a cybersecurity threat is suspected. ○ Training workers on the technical skills necessary to ensure the application of cybersecurity requirements and practices when dealing with telework systems. ● Ensure that the entity's requirements are supported by executive management. This is through the approval of the head of the entity or their representative.	
	Expected Deliverables: ● A document demonstrating the cybersecurity requirements for telework approved by the entity in line with basic cybersecurity controls. (For example: electronic copy or official hard copy). ● Official approval by the head of the entity or his representative on the requirements (For example: via the entity's official e-mail, or by paper or electronic signature).	
1-2	**Cybersecurity Risk Management**	
Objective	To ensure managing cybersecurity risks in a methodological approach in order to protect the organization's information and technology assets as per organizational policies and procedures, and related laws and regulations.	
Controls		
1-2-1	In addition to the controls within subdomain 1-5 in the ECC, requirements for cybersecurity risk management should include at least the following:	
	1-2-1-1	Assessment of the cybersecurity risks for telework systems, once per year at least.
	Related Cybersecurity Tools: ● Cybersecurity risk management policy. ● Cybersecurity risk management procedure.	

- Cybersecurity risk register.

Controls implementation guidelines:

- Conduct a cybersecurity risk assessment on telework systems in order to identify all potential threats that could affect the integrity of those systems or expose the information they process to any cyber risks or potential vulnerabilities, taking into account the nature of those systems.
- Assess the cybersecurity risks of each system periodically, at least once a year.
- Create reports on the cybersecurity risk assessment processes for each system, provided that the following is documented:
  - Cyber risks and potential vulnerabilities.
  - The probability of the risk occurring.
  - Impact ratio.
  - Risk level.
  - Responsible for the potential risk.
  - Description of the risk treatment plan.
  - Affected assets.
- Work on developing a plan to address the list of cybersecurity risks for each system.

Expected Deliverables:

- Periodic cybersecurity risk assessment reports on the entity’s telework systems.
- Treatment plans for cybersecurity risks for all telework systems.
- Follow up on treatment plans and verify their implementation.

1-2-1-2	Assessment of cybersecurity risks during planning and before permitting telework for any service or system.

Related Cybersecurity Tools:

- Cybersecurity risk management policy.
- Cybersecurity risk management procedure.
- Cybersecurity risk register.

Controls implementation guidelines:

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.

- Include cybersecurity requirements within the entity’s IT change management” cycle.
- Implement cybersecurity risk assessment procedures when planning and before allowing telework for any service or system.
- Work on addressing all cybersecurity risks identified according to the cybersecurity risk management methodology.
- Work on developing a treatment plan for the list of cybersecurity risks for each system, while following up the treatment plan periodically.

Expected Deliverables:

- A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder).
- A report detailing the identification, assessment, and remediation of cybersecurity risks related to planning and prior allowing telework for any service or system.
- Cybersecurity risk register for teleworking includes (during planning, upon implementation and before use).

1-2-1-3	Including the cybersecurity risks related to telework systems and its related services and systems in the entity's cybersecurity risk register, and monitoring it at least once a year.

Related Cybersecurity Tools:

- Cybersecurity risk management policy.
- Cybersecurity risk management procedure.
- Cybersecurity risk register.

Controls implementation guidelines:

- Work on creating a cybersecurity risk register for telework systems, services and systems that are allowed to work remotely, or include the risks related to them clearly within the entity’s general cybersecurity risk register, so that it contains the following:
    - Cyber risks and potential vulnerabilities.
    - The probability of the risk occurring.
    - Impact ratio.
    - Risk level.

	○ Responsible for the potential risk. ○ Description of the risk treatment plan. ○ Affected assets. ● Include the cybersecurity risks of telework systems, services and systems allowed for telework that were identified and evaluated during the evaluation process, and assign them to stakeholders. ● Follow up the cybersecurity risk register for telework systems, services and systems allowed to work remotely periodically, at least once a year, so that treatment plans are followed up, their implementation is verified, any new risks are added, and changes are documented in the register.	
	Expected Deliverables: ● Cybersecurity risk register for telework and services and systems permitted to work remotely. ● Changes log of the cybersecurity risk register for telework systems, services, and authorized telework. ● Follow up on treatment plans and verify their implementation. ● Periodically review cybersecurity risks related to telework systems.	
1-3	**Cybersecurity Awareness and Training Program**	
Objective	To ensure that the entity's employees are aware of their cybersecurity responsibilities and have the essential cybersecurity awareness. It is also to ensure that entity's employees 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 sub-controls within control 1-10-3 in the ECC, the cybersecurity awareness program must cover the awareness about the potential cyber risks and threats related to telework, including the following:	
	1-3-1-1	Secure use of telework devices and how to protect them.
	Related Cybersecurity Tools: ● Cybersecurity awareness program. **Controls implementation guidelines:**	

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.
- Provide cybersecurity awareness programs that cover the secure usage of telework devices and how to protect them.

Expected Deliverables:

- A document that identifies and documents the requirements of this policy (such as a policy and/or procedure approved by the authority holder).
- Document of providing awareness content of the secure use of telework devices and how to protect them.
- Proof of providing awareness content on the safe use of telework devices and how to protect them.

1-3-1-2	Secure handling of identities and passwords.

Related Cybersecurity Tools:

- Cybersecurity awareness program.

Controls implementation guidelines:

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.
- Provide cybersecurity awareness programs that cover secure handling of identities and password.

Expected Deliverables:

- A document that identifies and documents the requirements of this policy (such as a policy and/or procedure approved by the authority holder).
- Action plan to implement the cybersecurity awareness program that covers the secure handling of identities and password.

	● Proof of providing awareness content of the secure handling of identities and password.	
	1-3-1-3	Protection of the stored data on the telework devices, and to be handled based on its classification.
	Related Cybersecurity Tools: ● Cybersecurity awareness program. **Controls implementation guidelines:** ● Work to define the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Provide awareness programs in cybersecurity that cover the protection of data that is saved on devices used for telework and dealing with them according to their classification and the entity's procedures and policies.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● An action plan to implement a cybersecurity awareness program that covers the protection of data that is saved on devices used for telework and dealing with it according to its classification and the entity's procedures and policies. ● Proof of providing awareness content to protect the data that is saved on devices used for telework and dealing with it according to its classification and the entity's procedures and policies.	
	1-3-1-4	Secure handling of applications and solutions used for telework such as: virtual conferencing and collaboration, and file sharing solutions.
	Related Cybersecurity Tools: ● Cybersecurity awareness program.	

	Controls implementation guidelines: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Provide cybersecurity awareness programs that cover the secure handling of applications and solutions used for telework such as: virtual conferencing and collaboration, and file sharing solutions.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Action plan to implement the cybersecurity awareness program that cover the secure handling of applications and solutions used for telework such as: virtual conferencing and collaboration, and file sharing solutions. ● Proof of providing awareness content to avoid working remotely using unreliable public devices or networks or while in public places.	
	1-3-1-5	Secure handling of home networks, making sure it is configured in a secure way.
	Related Cybersecurity Tools: ● Cybersecurity awareness program. **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Provide cybersecurity awareness programs that cover the secure handling of home networks, making sure it is configured in a secure way.	
	Expected Deliverables: • A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder).	

<table>
<tr><td rowspan="6"></td><td colspan="2">• Action plan to implement the cybersecurity awareness program that cover secure handling of home networks, making sure it is configured in a secure way.
• Proof of providing awareness content to avoid working remotely using unreliable public devices or networks or while in public places.</td></tr>
<tr><td>1-3-1-6</td><td>Avoidance of teleworking using unreliable public devices or networks or while in public places.</td></tr>
<tr><td colspan="2">**Related Cybersecurity Tools:**
● Cybersecurity awareness program.
Controls implementation guidelines:
● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.
● Provide cybersecurity awareness programs that cover the secure handling of home networks, making sure it is configured in a secure way.</td></tr>
<tr><td colspan="2">**Expected Deliverables:**
● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder).
● Action plan to implement the cybersecurity awareness program that cover the avoidance of teleworking using unreliable public devices or networks or while in public places.
● Proof of providing awareness content to avoid working remotely using unreliable public devices or networks or while in public places.</td></tr>
<tr><td>1-3-1-7</td><td>Unauthorized physical access, loss, theft, and sabotage of technical assets and telework systems.</td></tr>
<tr><td colspan="2">**Related Cybersecurity Tools:**
● Cybersecurity awareness program.
Controls implementation guidelines:</td></tr>
</table>

	● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Provide cybersecurity awareness programs that cover the unauthorized physical access, loss, theft, and sabotage of technical assets and telework systems.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Action plan to implement the cybersecurity awareness program that cover the unauthorized physical access, loss, theft, and damage of technical assets and telework systems. ● Proof of providing awareness content on unauthorized physical access, loss, theft and damage of technical assets and teleworking systems.	
	1-3-1-8	To Communicate directly with the cybersecurity department If a cybersecurity threat is suspected.
	Related Cybersecurity Tools: ● Cybersecurity awareness program. **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Provide cybersecurity awareness programs that cover how to communicate directly with the cybersecurity department If a cyber threat is suspected.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Action plan to implement the cybersecurity awareness program on how to communicate directly with the cybersecurity department if a cyber threat is suspected. ● Proof of providing awareness content and communicating directly with the department concerned with cybersecurity in if a cyber threat is suspected.	

1-3-2	In addition to the sub-controls within control 1-10-4 in the ECC, employees must be trained with the required technical skills to ensure the implementation of the cybersecurity requirements when handling telework systems.
	Related Cybersecurity Tools: ● Cybersecurity awareness program. **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Develop and implement training program for employees working in cybersecurity team or other team members wherever required, to ensure implementation of cybersecurity requirements with required technical skills for teleworking systems. ● Periodic awareness programs to be conducted to ensure safe handling of the cyber security incidents and implementation/services requirements.
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Documented training program and its periodic implementation for handling cyber security services and support for teleworking requirements. ● Training certificates for workers on the technical skills necessary to ensure the application of cybersecurity requirements and practices when dealing with telework systems.

2 (Cybersecurity Defense)

2-1	Asset Management	
Objective	To ensure that the organization has an accurate and detailed inventory of information and technology assets in order to support the organization's cybersecurity and operational requirements to maintain the confidentiality, integrity and availability of information and technology assets.	
Controls		
2-1-1	In addition to the controls within subdomain 2-1 in the ECC, cybersecurity requirements for asset management related to telework systems should include at least the following:	
	2-1-1-1	Identifying and maintaining an annually-updated inventory of information and technology assets of the telework systems.
	Related Cybersecurity Tools: ● Asset management policy ● Asset classification standards template **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Develop an inventory of information and technical assets for telework systems in an electronic format, specifying the inventory date, several methods can be applied to store and use an inventory and inventory of assets, including but not limited to: ○ Configuration Management Database (CMDB). ○ Asset management programs. ○ A specialized tool for asset management. ○ Spreadsheets. ○ Database ● Identify all the information and technical assets (hardware & software) used in teleworking system and document them.	

	● Ensure that the inventory is centralized between the department concerned with cybersecurity and information technology and other concerned departments, and that it is updated and ensured its accuracy at least once a year.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Detailed telework asset inventory. ● Periodic plan for asset inventory update with latest information and approved.	
2-2	**Identity and Access Management**	
Objective	To ensure 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		
2-2-1	In addition to the sub-controls within control 2-2-3 in the ECC, cybersecurity requirements for identity and access management related to telework systems shall include at least the following:	
	2-2-1-1	Managing telework access rights based on need, considering the sensitivity of the systems, the level of access rights and the type of devices used by employees for telework.
	Related Cybersecurity Tools: ● Identity and access management policy **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Develop telework access management procedures by the organization, taking into account the following: ○ System sensitivity. ○ Level of access.	

	○ Type of devices used by employees to work remotely. ○ Validity period. ● Implement the required technological controls to provide and manage identities and access rights of telework assets.	
	Expected Deliverables ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● A list of all permissions and accesses used for telework. ● Requests for granting permissions and access to users to enable telework, along with the necessary approvals. ● Audit reports on the activities of authorized accounts.	
	2-2-1-2	Restricting remote access for the same user from multiple computers at the same time (Concurrent Logins).
	Related Cybersecurity Tools: ● Identity and access management policy **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Implement secure session management by setting a maximum number of session allowed by one user. ● When there is a need for an exception to this requirement, procedures are determined to obtain the necessary approval from the relevant department and the department concerned with cybersecurity.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder).	

- A screenshot of the remote access restriction for the same user from multiple computers at the same time, including the maximum number of sessions the user is allowed.
- Procedures adopted for exceptions to this requirement.
- A formal approval for any exception.

2-2-1-3	Using secure standards to manage identities and passwords used in the telework systems.

Related Cybersecurity Tools:

- Identity and access management policy
- Identity and access management standards

Controls implementation guidelines:

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.
- Develop password standard taking into consideration best practices, including but not limited to:
    - A The minimum number of password symbols for important and sensitive privileges is 10 and for the rest of the privileges is 8.
    - Password expiration period is at least 30 days for important and high privileged permissions, and at least 90 days for the remaining permissions.
    - Password complexity.
    - Password and account Lockout.
    - Password activation.
    - Password history log.
    - Number of attempts allowed is 3.
    - Passwords used during the last 12 times must not be repeated.
    - Passwords should not be used based on the personal data of the user with privileges, such as date of birth.
    - The password must be complex and include at least 4 of the following characters:
        - Upper case letters
        - Lower case letters
        - Numbers (1234)

	■ Special symbols (#%*@) ● Activate two-factor authentication for telework systems in addition to the user name and password, which may be, for example: ○ One Time Password in a text message sent to the mobile number registered to the end user. ○ One Time Password is displayed in a hard token program or device for multi factor authentication. ○ Use biometrics to verify identities (example: fingerprint). ● Use Virtual Private Network (VPN) to encrypt traffic between user and systems.
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Proof of using secure standards to manage identities and passwords used in the telework systems for example but not limited, a screenshot of password configuration policy and screenshot of MFA implementation.
2-2-2	With reference to the ECC sub-control 2-2-3-5, user's identities and access rights used for teleworking must be reviewed at least once every year.
	Related Cybersecurity Tools: ● Identity and access management policy **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Review the login identities and access permissions used for telework by conducting a periodic evaluation (according to a documented and approved review plan, and based on a specific time period of at least once a year). ● Review all login identities and access permissions used for telework in all aspects, including but not limited to: ○ The principle of minimum permissions and privileges

	○ The principle of separation of duties, and the principle of the need for knowledge and use in cooperation with relevant departments (such as the department concerned with information technology “IT”). ○ The validity period granted. ○ The status of the person entitled to the granted privileges , for example but not limited to: if he is still present in the administration, or has been transferred to another team, or has resigned from the entity, or the user’s work does not require access to telework and take the necessary measures according to the status of the person granted the authority to work. ● Document all reviews and changes made to the login identities and access permissions used for telework in the entity, including, but not limited to: ○ Periodic reviews of granted privileges ○ Changes that occurred from the last version. ○ Changes required on the granted privileges
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Results of reviewing login identities and access permissions for sensitive systems in the entity. ● Documented periodic plan to review the identities of telework users and their access rights. ● Proof of periodic identity and access review requirements, for example: an official, approved document demonstrating the periodic review of identities and access permissions for telework users.
2-3	**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	
2-3-1	In addition to the sub controls in the ECC control 2-3-3, cybersecurity requirements for protecting telework systems and information processing facilities must include at least the following:

	2-3-1-1	Applying updates and security patches for telework systems at least once every month.

Related Cybersecurity Tools:

- Patch Management Policy.
- Configuration and Hardening Standard.
- Patch Management Standard.

Controls implementation guidelines:

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.

- Define procedures for patch management on systems, devices and applications, which include:
  - The scope of systems where patches are implemented must be defined to include:
    - Workstations.
    - Operating Systems.
    - Network Devices.
    - Databases.
    - Applications.
  - Time period required to implement patches must be at least once every month.
  - Patches procedures must be included in change management methodology or change management must be included into patch management policy.
  - Change management approval must be included as part of patch approval form for all systems, devices and applications, including but not limited to: requesting approvals via e-mail, paper, or through an internal system.
  - Patches must be implemented to the defined scope after obtaining the necessary approval.
  - Continuously review the application of update packages and patches to ensure that all necessary updates have been applied to all devices, systems and applications for remote work.

Expected Deliverables:

- A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder).

	● Approved procedures indicate that change management approval is required for patches. ● Reports that the scope of patches covers all devices and applications of telework systems. ● Reports that the patches are performed according to the period specified in the procedures (including but not limited to: a screenshot or direct example that displays the date and scope for several samples of patches approved by e-mail, internal system or paper that are performed in advance to include devices, systems and applications periodically).	
	2-3-1-2	Reviewing telework systems' configurations and hardening at least once every year.
	Related Cybersecurity Tools: ● Patch Management Policy. ● Configuration and Hardening Standard **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Define technical standard to Review telework systems' configurations and hardening from trusted sources for example but not limited, the vendor of telework system. ● Define a procedure for reviewing configuration and hardening of telework system. ● Review the configuration and hardening of telework system based on approved standard at least once a year, this include but not limited: access management, encryption and secure system setting.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Telework configuration and hardening standard approved by the organization (e.g., electronic copy or official hard copy).	

- Reports that telework systems configuration and hardening are reviewed at least every year.

2-3-1-3	Reviewing and changing default configurations, and ensuring the removal of hard-coded, backdoor and/or default passwords.

Related Cybersecurity Tools:

- Patch Management Policy.
- Configuration and Hardening Standard

Controls implementation guidelines:

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.
- Ensure that there are no hard-coded, backdoor or default passwords on telework systems based on approved standard and document the results.

Expected Deliverables:

- A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder).
- Reports of reviewing and changing default configurations, and ensuring the removal of hard-coded, backdoor and/or default passwords.

2-3-1-4	Securing Session Management which includes the session authenticity, lockout, and timeout.

Controls implementation guidelines:

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.
- Implement secure session management process that includes :
  - Authentication.
  - Authorization.
  - Access.
  - Control.

  - Lockout.
  - Timeout.
- Define session duration by ensuring no impact on availability of the services and information while teleworking.
- Document and approve the session lockout and session timeout duration in telework systems from stakeholders.

Expected Deliverables:

- A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder).
- Documented and approved telework policy on having defined session management process, and duration for session lock out and session time out.
- Screenshot of session management that include:
  - Session authentication.
  - Session lockout.
  - Session timeout.

2-3-1-5	Restricting the activation of the features and services of the telework systems based on needs, provided that potential cyber risks are analyzed in case there is a need to activate them.

Controls implementation guidelines:

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.
- Documenting and specifying restrictions in telework systems, after clarifying and accepting the risks, to ensure safe activation over the Internet to activate technical features and services based on the user's need, while specifying the duration of activation.
- Develop and document workflow for appropriate approval of a user request for specific feature/services required for a particular business operations and specify the duration of activation.
- Perform analysis of potential cyber risk before approving and activating specific user request for certain technical features or services in telework systems.

Expected Deliverables:

- A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder).

	● An approved procedures document to restrict the activation of features and services in telework systems as needed. ● Reports analyzing potential cyber risks before activation.	
2-4	**Network Security Management**	
Objective	To ensure the protection of organization's network from cyber risks.	
Controls		
2-4-1	In addition to the sub controls in the ECC control 2-5-3, cybersecurity requirements of telework systems' network security management must include at least the following	
	2-4-1-1	Restrictions on network services, protocols and ports used to access remotely, specifically to internal systems and to only be opened based on need.
	Related Cybersecurity Tools: ● Network security policy ● Network security standard **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Implement the requirements of restrictions on network services, protocols and ports used to access remotely by using appropriate and advanced technologies including but not limited to restriction by firewall systems. ● Establishment of approval procedures to update the Firewall Rules to ensure that no update or change is made without the approval of the representative.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Sample showing the implementation of requirements related to network services, protocols, and ports restrictions, including but not limited to: ○ Template showing the implementation of network services, protocols, and ports restrictions requirements (e.g., screenshot showing evidence of subscription and use of modern and advanced technologies to apply restrictions network services, protocols, and ports through firewall system)	

- Sample showing approval procedures form to update the Firewall. In addition, a sample showing what has been updated on the Firewall Rules.

2-4-1-2	Reviewing firewall rules and configurations, at least once every year.

Related Cybersecurity Tools:

- Network security policy
- Network security standard

Controls implementation guidelines:

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.
- Work on reviewing firewall settings, lists and rules related to telework systems; At least once a year, for example but not limited to:
  - Review unused/activated lists within the last 90 days to be deleted and disabled.
  - Update settings according to recent resource versions.
  - Arrange lists according to effectiveness and performance.
  - Review and analyze VPN lists
- Documenting the audit results to include, but not be limited to:
  - Changes after review.
  - Review date.
  - Accreditation

Expected Deliverables:

- A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder).
- Review report of firewall settings for sensitive systems in the entity (evaluation table).
- Documented process to periodic review of firewall rules & configurations.

2-4-1-3	Protecting against Distributed Denial of Service Attack (DDoS) attacks to limit risks arising from these attacks.

Related Cybersecurity Tools:

- Network security policy
- Network security standard
- Protection against Distributed Denial of Service (DDOS) attacks Standard template

Controls implementation guidelines:

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.
- Provide protection systems from Distributed Denial of Service Attacks (DDoS) on telework systems to reduce the risks resulting from network disruption attacks and update them on an ongoing basis.
- Adjust firewall settings to protect against Distributed Denial of Service Attacks (DDoS).
- Apply the principle of multiple availability (High Availability) to the entity's telework systems, including, but not limited to: firewall systems, web proxy systems.
- Work on concluding an agreement with the service provider or Internet service provider to implement mechanisms and ensure protection against network disruption attacks (Distributed Denial of Service Attack "DDoS").

Expected Deliverables:

- A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder).
- Systems and techniques for protecting against network disruption attacks on telework systems.
- A list of settings and controls for protection against network disruption attacks (Distributed Denial of Service Attack "DDoS").

2-4-1-4	Protecting against Advanced Persistent Threats (APT) at the network layer.

Related Cybersecurity Tools:

- Network security policy
- Network security standard
- Advanced Persistent Threats (APT) Standard Template

	Controls implementation guidelines: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Working to provide protection systems against advanced persistent threats at the network level for telework systems (Network APT) and updating them continuously, for example but not limited to: ○ Provide advanced protection systems to detect and prevent intrusions, such as: Intrusion Prevention/Detection Systems (IDS/IPS, HIDS/HIPS) on all parts of the network and updating them continuously. ○ Update continuous monitoring procedures at the network level to protect against threats.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● A list of all systems available to protect against advanced persistent threats to teleworking systems. ● Documented procedures for continuous monitoring, as well as applying and using advanced persistent threat protection tools.	
2-5	**Mobile Device 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		
2-5-1	In addition to the sub-controls within control 2-6-3 in the ECC, cybersecurity requirements for mobile device security related to telework systems shall include at least the following:	
	2-5-1-1	Central management of mobile devices and BYODs using a Mobile Device Management system (MDM).
	Related Cybersecurity Tools: ● Workstations, Mobile Devices and BYOD Security Policy Template	

	● Mobile Devices Security Standard Template **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Ensure that mobile devices and BYOD devices are managed centrally using the Mobile Device Management system to maintain confidentiality, integrity, and availability of organization's information.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Documented procedures for implementing the mobile device management system on all BYOD devices using MDM provided by the entity. ● Sample of MDM implementation.	
	2-5-1-2	Applying updates and security patches on mobile devices, at least once every month.
	Related Cybersecurity Tools: ● Workstations, Mobile Devices and BYOD Security Policy Template ● Mobile Devices Security Standard Template **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Ensure that the approval of the change management in the entity is part of the approvals required to implement security updates and patches for mobile device security for telework in the entity. ● Define a documented, periodic plan to implement mobile security updates and patches and mobile device management (MDM) solutions for telework at least once a month. ● Follow up on the implementation of mobile security patch and update packages for telework continuously through the use of patch and update management tools and technologies.	

	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Documented process to apply technical updates & security patches on mobile devices. ● Reports showing the patches performed according to the period specified in the procedures.	
2-6	**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		
2-6-1	In addition to the sub controls in the ECC control 2-7-3, cybersecurity requirements for protecting and handling data and information must include at least the following:	
	2-6-1-1	Identifying classified data, according to the relevant regulations, that can be used, accessed or dealt with through telework systems.
	Related Cybersecurity Tools: ● Data Loss Prevention Standard Template **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Identify data in storage and data in transit in private telework systems in accordance with the entity's data policies and Data Cybersecurity Controls (DCC) issued by the National Cybersecurity Authority. ● Determine the classification of data at each stage according to data cybersecurity controls (DCC).	

	● Ensure that all data that may be used, accessed or handled through teleworking systems is classified based on relevant regulatory and legislative requirements. ● Determine mechanisms and methods for dealing with data based on its classification.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Documented and approved process for the data types their classification in telework systems. ● A guide to applying technical systems in cybersecurity to classify data within telework system.	
	2-6-1-2	Protecting classified data, which was identified in control 2-6-1-1, using controls such as: not allowing the use of a specific type of classified data, or by the use of technology (e.g. Data leakage Prevention), such controls and technologies can be determined by analyzing the cyber risks of the organization.
	Related Cybersecurity Tools: ● Data Loss Prevention Standard Template **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Identify and classify telework systems data based on relevant regulatory and legislative requirements. ● Conduct a cybersecurity risk analysis on the classified data (which was included in the outputs of control No. 2-6-1-1) in order to identify all potential threats that could affect the integrity of that data or expose it to any cyber risks or potential vulnerabilities. Taking into account the nature of this data. ● Based on the results of cyber risk analysis reports, work is done to identify controls or techniques that contribute to preventing the use of a type of classified data or preventing data leakage in the entity.	

	• Review, approve and implement controls necessary to prevent data loss, using data leakage prevention tools and others, which are determined based on identified use cases and risk factors. • Data blocking use cases can be controlled at different levels, but are not limited to: email, sending documents with an external party, transferring data via physical devices such as: (USB, hard disk, etc.), and sharing data via hard drives. Network, transmission via Bluetooth connection, unwanted access to internal database server for telework users, use of remote sharing applications.	
	Expected Deliverables: • A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). • An approved document with a guide to implementing controls for data protection (preventing data leakage). • A guide to implementing cybersecurity controls and techniques to prevent access, use, and transfer of restricted information to an internal or external user.	
2-7	**Cryptography**	
Objective	In addition to the sub-controls within control 2-8-3 in the ECC, cybersecurity requirements for cryptography related to telework systems shall include at least the following:	
Controls		
2-7-1	In addition to the sub-controls within control 2-8-3 in the ECC, cybersecurity requirements for cryptography related to telework systems shall include at least the following:	
	2-7-1-1	The use of updated and secure methods and algorithms for encryption over the entire network connection used for telework, according to the Advanced level within the National Cryptography Standards (NCS 1:2020).
	Related Cybersecurity Tools: • Encryption policy • Encryption standard • Encryption key management standards **Controls implementation guidelines:**	

	● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Identify secure algorithms, keys, and encryption devices by adhering to correct application standards and updating them by reviewing them annually and ensuring that they are in line with the encryption standards issued by the Cybersecurity Authority. ● Use of advanced level encryption methods and algorithms based on the National Encryption Standards (NCS 1:2020) across the entire network used for telework. ● Review the effectiveness of techniques used for secure management of algorithms, keys and cryptographic devices ● Strong algorithms and encryption tools to be used wherever possible, such as but not limited to: telework device password encryption, data files encryption while transferring outside organization, encryption of secret information stored in telework systems.
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Cybersecurity procedures that cover the secure management of the entity's algorithms, keys, and encryption devices (for example: an electronic copy or an official hard copy). ● A document defining the cycle of reviewing the effectiveness of the techniques used; for the secure management of algorithms, keys and encryption devices during their life cycle operations at the organization. ● A list of protocols and technologies used to encrypt the entire network connection used for telework.
2-8	**Backup and Recovery Management**
Objective	To ensure the protection of organization's data and information including information systems and software configurations from cyber risks as per organizational policies and procedures, and related laws and regulations.

Controls		
2-8-1	In addition to the subcontrols in the ECC control 2-9-3, cybersecurity requirements for backup and recovery management must include at least the following:	
	2-8-1-1	Performing backup within planned intervals, according to the organization's risk assessment.
	Related Cybersecurity Tools: ● Backups policy template ● Backups standard template **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● In line with the organization risk assessment policy, define the plan for periodic planned backup of data and settings of telework systems. ● Review the backup performance within planned internals ● Ensure to have business continuity via backup plans of telework systems.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● A documented and approved plan for making backup copies of telework systems. ● A guide to implementing the technical controls required to perform planned backups of teleworking systems and ensure business continuity.	
2-8-2	With reference to the ECC subcontrol 2-9-3-3, a periodical test must be conducted at least once every six months in order to determine the efficiency of recovering telework systems backups.	
	Related Cybersecurity Tools: ● Backups policy template ● Backups standard template **Controls implementation guidelines:**	

	● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Based on defined backup periodicity and business continuity plan, define and approve the periodic testing of telework backup systems at least once every six months. ● Ensure the effectiveness of the recovery procedures by conducting a test to restore backups periodically to ensure the ability to restore data and telework systems according to the period specified in the procedures and according to the period that has been identified for the completion of restoring backups.	
	Expected Deliverables: ● A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). ● Document a business plan and procedures for implementing cybersecurity requirements for backup management. ● Test reports that examine the effectiveness of backups for telework systems, so that it clarifies the difference between the expected duration and the test duration for restoring all backups.	
2-9	**Vulnerabilities Management**	
Objective	To ensure timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploiting these vulnerabilities to launch cyber attacks against the organization.	
Controls		
2-9-1	In addition to the subcontrols in the ECC control 2-10-3, cybersecurity requirements for technical vulnerabilities management of telework systems must include at least the following:	
	2-9-1-1	Assessing vulnerabilities on technical components of telework systems, and to be classified based on criticality at least once every three months.
	Related Cybersecurity Tools: ● Vulnerability management policy ● Vulnerability management standard ● Vulnerability assessment procedure	

	• Vulnerability register **Controls implementation guidelines:** • Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. • Installing and linking techniques and tools for examining and discovering vulnerabilities in information and technical assets of the telework systems in the organization. • Develop a periodic plan (at least once every three months) and procedures for examining and discovering vulnerability in the information and technical assets of the telework systems in the organization.	
	Expected Deliverables: • A document that identifies and documents the requirements of this control (such as a policy and/or procedure approved by the authority holder). • Approved vulnerabilities management procedures and a periodic plan (at least once every three months) to scan and discover vulnerabilities in telework systems. • Periodic reports to examine and discover vulnerability in telework systems.	
	2-9-1-2	Remediating vulnerabilities for telework systems, at least once every three months.
	Related Cybersecurity Tools: • Vulnerability management policy • Vulnerability management standard • Vulnerability assessment procedure • Vulnerability register **Controls implementation guidelines:** • Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.	

	• Sharing reports of the vulnerabilities inspected and discovered in the information and technical assets of teleworking system of the organization with the concerned departments, which include, but are not limited to: ○ Department concerned with managing applications ○ Department of Management of user devices ○ Infrastructure Department ○ Department concerned with database management ○ Network management • Ensure that the shared vulnerability reports of teleworking system contain: ○ A description of the vulnerabilities. ○ Relevant asset's name which vulnerabilities were scanned and discovered in. ○ Classification of vulnerabilities. • Work with the concerned departments to define a timeline and a plan to address the vulnerabilities, taking into account the classification of the vulnerabilities and the classification of the assets concerned • Develop a mechanism to ensure that gaps are addressed according to the plan.
	Expected Deliverables: • Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. • Vulnerability management procedures. • Procedures for managing security fixes and updates patches for telework systems. • Reports of vulnerabilities for telework systems (before and after treatment).
2-10	**Penetration Testing**
Objective	To assess and evaluate the efficiency of the organization's cybersecurity defense capabilities through simulated cyber-attacks to discover unknown weaknesses within the technical infrastructure that may lead to a cyber breach.
Controls	
2-10-1	In addition to the sub-controls within control 2-11-3 in the ECC, cybersecurity requirements for penetration testing related to telework systems shall include at least the following:

	2-10-1-1	Scope of penetration tests must cover all of the telework systems' technical components.
	Related Cybersecurity Tools: ● Penetration testing policy template ● Penetration testing standard template **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Identify all technical components that support telework services. ● Define the appropriate pre-requisites and stakeholder approvals required before performing penetration testing in telework systems and its technical components. ● Document the penetration testing scope, and level allowed for penetration testers by the organization to ensure no impact on business operations.	
	Expected Deliverables: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Documented scope for the penetration testing of all telework systems and technical components.	
2-10-2	With reference to the ECC subcontrol 2-11-3-2, penetration tests must be conducted on telework systems at least once every year.	
	Related Cybersecurity Tools: ● Penetration testing policy template ● Penetration testing standard template **Controls implementation guidelines:**	

	● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Based on the penetration scope, document the pre-requisites and required stakeholder approvals before performing penetration testing on telework system and technical components. ● Get plan approval to conduct penetration testing, and inform relevant stakeholders prior to testing to ensure there is no impact on operational processes. ● Ensure planned penetration testing is conducted at least once a year on teleworking systems and technical components. ● Prepare penetration testing report for audit, compliance and remediation purpose. ● Prepare a plan to address the gaps discovered in telework systems and follow up on it periodically.	
	Expected Deliverables: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Documented and approved plan to conduct periodic penetration testing of telework systems and technical components at least once every year. ● Detailed Penetration testing report of telework systems.	
2-11	**Cybersecurity Events Logs and Monitoring Management**	
Objective	To ensure timely collection, analysis and monitoring of cybersecurity events for early detection of potential cyber-attacks in order to prevent or minimize the negative impacts on the organization's operations.	
Controls		
2-11-1	In addition to the subcontrols in the ECC control 2-12-3, cybersecurity requirements for event logs and monitoring management for telework systems must include at least the following:	
	2-11-1-1	Activating cybersecurity events logs on all technical components of telework systems.

Related Cybersecurity Tools:

- Cybersecurity Event Logs and Monitoring Management Policy Template
- Cybersecurity Event Logs and Monitoring Management Standard Template

Controls implementation guidelines:

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.
- Based on the cyber security policies of the organization and ECC controls, a scope is defined for event logs and monitoring management of telework systems and its technical components.
- Activate and review logging of all cyber security events of telework environment.

Expected Deliverables:

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.
- Screenshot or a direct example showing the activation of logs through SIEM.

2-11-1-2	Monitoring and analyzing user behavior (UBA).

Related Cybersecurity Tools:

- Cybersecurity Event Logs and Monitoring Management Policy Template
- Cybersecurity Event Logs and Monitoring Management Standard Template

Controls implementation guidelines:

- Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder.
- Provide specialized systems to monitor and analyze user behaviour.
- Work with the relevant departments in the entity to determine acceptable user behaviour on telework systems in order to identify suspicious behaviour.

	● Develop security procedures (Incident response playbook) to be taken for cases that have been studied and identified with the relevant departments for suspicious behaviour cases.	
	Expected Deliverables: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● A list of systems and settings to monitor user behaviour to ensure continuous analysis. ● A list of all the cases that have been studied and analysed. ● Incident response playbook.	
	2-11-1-3	Monitoring telework systems events around the clock.
	Related Cybersecurity Tools: ● Cybersecurity Event Logs and Monitoring Management Policy Template ● Cybersecurity Event Logs and Monitoring Management Standard Template **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Monitor all cybersecurity events for telework systems around the clock (24/7/365/365) through specialized teams.	
	Expected Deliverables: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Monitor event logs of technical assets and teleworking systems around the clock, including but not limited to: a table showing the allocated times around the clock for the specialized team.	

		● A contract demonstrating the followed monitoring template incase the security operations center or monitoring was provided by a service provider.
	2-11-1-4	Updating and implementing cybersecurity monitoring procedures around the clock, to include monitoring remote access operations, especially remote access from outside the Kingdom of Saudi Arabia, after checking their authenticity.
		Related Cybersecurity Tools: ● Cybersecurity Event Logs and Monitoring Management Policy Template ● Cybersecurity Event Logs and Monitoring Management Standard Template **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Review and verify cybersecurity monitoring procedures, update them and implement controls to monitor them around the clock. ● Monitoring and analysis of event logs may include but not limited to: remote access operations within or from outside KSA after checking their authenticity, application event logs, system event logs, storage event logs, antivirus event logs, incident logs and others. ● Work to save all activities and records of remote login operations and ensure that they are sent to the operations and monitoring center to ensure that they are constantly monitored by specialized teams by linking login logs with monitoring systems, for example: the (SEIM) system.
		Expected Deliverables: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Cybersecurity monitoring procedures document to include monitoring remote access operations, especially remote access operations from outside the Kingdom, and verifying their authenticity. ● A guide demonstrating the monitoring of remote login events around the clock through the organization’s security operations center.

2-11-2	With reference to the ECC sub-control 2-12-3-5, retention period of cybersecurity's telework systems event logs must be 12 months minimum, in accordance with relevant legislative and regulatory requirements.	
	Controls implementation guidelines: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Identify and develop a mechanism to store all cybersecurity event logs for teleworking systems and technical components for a retention period of at least 12 months or more, in accordance with relevant legislative and regulatory requirements. ● Identify, document, and approve security controls for archiving or deleting stored records in accordance with the designated organization's retention and cybersecurity policy for telework systems.	
	Expected Deliverables: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● A screenshot or direct proof from the SIEM system showing record logs period for at least 12 months. ● A sample of stored logs extracted from the SIEM system where records have been kept for at least 12 months.	
2-12	**Cybersecurity Incident and Threat Management**	
Objective	To ensure timely identification, detection, effective management and handling of cybersecurity incidents and threats to prevent or minimize negative impacts on organization's operation taking into consideration the Royal Decree number 37140, dated 14/8/1438H.	
Controls		
2-12-1	In addition to the sub-controls within control 2-13-3 in the ECC, cybersecurity requirements for incident and threat management related to telework systems shall include at least the following:	
	2-12-1-1	Updating cyber security incidents response plans and contact information within the organization in a way that is compatible with the telework situation

		and to ensure the ability to communicate and the preparedness of the incident response teams.
	Related Cybersecurity Tools: ● Cybersecurity Incident and Threat Management Policy Template ● Cybersecurity Incident and Threat Management Standards Template ● Detailed plans templates for responding to cybersecurity incidents **Controls implementation guidelines:** ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Based on organization's cyber security incident and threat management policies, define and update response plans and relevant information for telework systems. ● Prepare and plan to run appropriate programs to communicate cyber incidents and threat management policies, to prevent mislead actions by telework users. ● Notify users about how to raise cyber incidents in case of suspected activity or actual event and to show preparedness of the organization's incident response team.	
	Expected Deliverables: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Updated response plans for telework systems. ● Documented and approved plan to run campaigns to communicate cyber incident and threat management policies. ● Sample cyber incidents report raised by telework users.	
	2-12-1-2	Periodically obtaining and dealing with threat intelligence information related to telework systems.
	Related Cybersecurity Tools: ● Cybersecurity Incident and Threat Management Policy Template ● Cybersecurity Incident and Threat Management Standards Template	

	● Detailed plans templates for responding to cybersecurity incidents **Controls implementation guidelines:** ● Work to define the requirements of this control and document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Work to partner with the platforms responsible for sending proactive information (Threat Intelligence) via email or other technical platforms, and these platforms include: ○ Saudi Computer Emergency Response Team (CERT). ○ Haseen's information sharing platform. ○ Newsletter of the communication and information technology authority. ○ Bulletins or announcements provided by companies specialized in cybersecurity. ○ Bulletins or announcements provided by security and technical service providers that were previously contracted by the entity. ● Work to deal with alerts sent by these platforms through: ○ Send it to the relevant team to deal with it (for example, but not limited to: the Information Technology Department, the Security Operations Center, the Department for Updates and Repairs). ○ Determine a period of time for dealing with these alerts according to the level of severity. ○ Continuous follow-up to ensure that the alerts sent to the relevant team have been dealt with securely (for example, but not limited to: ensuring that the update for the vulnerabilities sent has been applied).
	Expected Deliverables: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● A screenshot or direct evidence showing the entity's subscription to one of the platforms.

	● A screenshot or live evidence of an example of alerts on telework systems that were previously dealt with according to the necessary procedures.	
	2-12-1-3	Addressing and implementing the recommendations and alerts for cyber security incidents and threats issued by the Sector regulator or by the National Cybersecurity Authority (NCA).
	Related Cybersecurity Tools: ● Cybersecurity Incident and Threat Management Policy Template ● Cybersecurity Incident and Threat Management Standards Template ● Detailed plans templates for responding to cybersecurity incidents **Controls implementation guidelines:** ● Work to define the requirements of this control and document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Develop a mechanism to continuously receive information from proactive information platforms and information issued by the National Authority. ● Develop, adopt and implement a mechanism to address incoming recommendations for cyber alerts/incidents/threats. ● Communicate identified cyber risks/threats/incidents with the Cyber Security team and Risk Committee to ensure proactive decision making to minimize impact on operational processes.	
	Expected Deliverables: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● An approved document to address recommendations related to incidents and threats by the sector supervisor or the National Cybersecurity Authority. ● A document for the process of reporting cyber incidents/threats to the organization's cyber security team and dealing with them.	

3 (Third-Party and Cloud Computing Cybersecurity)

3-1	Cloud Computing and Hosting Cybersecurity	
Objective	To ensure the proper and efficient remediation of cyber risks and the implementation of cybersecurity requirements related to hosting and cloud computing as per organizational policies and procedures, and related laws and regulations. It is also to ensure the protection of the organization's information and technology assets hosted on the cloud or processed/ managed by third-parties.	
Controls		
3-1-1	In addition to the sub-controls in the ECC control 4-2-3, cybersecurity requirements related to the use of hosting and cloud computing services must include at least the following:	
	3-1-1-1	The location of the hosted telework systems must be inside the Kingdom of Saudi Arabia
	Related Cybersecurity Tools: ● Cloud Computing and Hosting Cybersecurity Policy Template **Controls implementation guidelines:** ● Work to define the requirements of this control and document them in the cybersecurity requirements document, and have them approved by the authority holder. ● Ensure that the organization's telework systems, or any part of its technical components, are hosted in a reliable and secure place within the Kingdom of Saudi Arabia.	
	Expected Deliverables: ● Work on defining the requirements for this control, document them in the cybersecurity requirements document, and have them approved by the authority holder. ● An official document proving that the organization's telework systems, or any part of its technical components, are hosted in a reliable and secure place within the Kingdom of Saudi Arabia.	

الهيئـــة الوطنيـــة
للأمـــن السيبـــراني
National Cybersecurity Authority