الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Guide to Organizations' Social Media Accounts Cybersecurity Controls Implementation

(GOSMACC– 1 : 2023)

TLP: white
Document Classification: Public

Disclaimer: This Guide has been developed by the National Cybersecurity Authority to assist organizations in implementing Cloud Cybersecurity Controls (CCC–1:2022) for Cloud Service Providers (CSPs). 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 Cloud Cybersecurity Controls, as long as alternative methods align with the National Cybersecurity Authority. This document contains some illustrative deliverables related to the implementation of Cloud Cybersecurity Controls. The assessor or auditor has the right to request other evidences as deemed necessary to ensure that proper implementation of all Cloud Cybersecurity Controls.

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 OSMACC-1: 2021 (referred to in this document as "Controls"), to enable national entities to implement the requirements to comply with the OSMACC. 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 OSMACC 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 OSMACC-1:2021's:

- These controls apply to government organizations in the Kingdom of Saudi Arabia, including ministries, authorities, establishments and others, and organizations and companies related to them. It also applies to private sector organizations that own, operate or host sensitive national infrastructure. All of them are referred to in this document as (The Organization).
- The NCA strongly encourages all other organizations in the Kingdom to leverage these controls to implement best practices to improve and enhance their cybersecurity.

OSMACC Domains and Subdomains

Figure 1 below show the main domain and subdomains of OSMACC

1	Cybersecurity Governance	1-1	Cybersecurity Policies and Procedures	1-2	Cybersecurity Risk Management
		1-3	Cybersecurity in Human Resources	1-4	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	Mobile Devices Security
		2-5	Data and Information Protection	2-6	Cybersecurity Event Logs and Monitoring Management
		2-7	Cybersecurity Incident and Threat Management		
3	Third-Party and Cloud Computing Cybersecurity	3-1	Third-Party Cybersecurity		

Figure 3: OSMACC Main Domains and Subdomains

Structure of the Guideline

Figure 2 below show the structure of OSMACC

	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: OSMACC Structure

OSMACC Implementation General Guideline

General Guidelines
• Inventory all social media accounts on all social media platforms used by the organization and review them regularly. • Identify the technical assets, applications, and systems related to social media accounts on all platforms used by the organization. • Identify and document the OSMACC requirements, along with associated roles and responsibilities, and having them authorized by the authorizing official, reviewing them periodically. • Review the ECC guidelines and implement OSMACC for entities. • Develop a plan to implement OSMACC across all platforms, and monitor it continuously.

OSMACC Implementation Guideline

1 (Cybersecurity Governance)

1-1	Cybersecurity Policies and Procedures	
Objective	To ensure that cybersecurity requirements are documented, communicated and compiled with by the organization as per related laws and regulations, and organizational requirements.	
Controls		
1-1-1	Referring to control 1-3-1 in the ECC, cybersecurity policies and procedures must include the following:	
	1-1-1-1	Defining and documenting the cybersecurity requirements for organizations' social media accounts as part of the organization's cybersecurity policies.
	Related Cybersecurity Tools: • Template for Cybersecurity Documentation Development Procedure **Controls implementation guidelines:** • Define and document the cybersecurity requirements for the social media accounts as part of organizations' cybersecurity policies. • Ensure the document is disseminated to all personnel within the organization and relevant external parties through approved communication channels, as per the scope defined in the policy (e.g., distributing policies and procedures via the organization's internal portal or sending them through email).	
	Expected Deliverables: • Document containing cybersecurity requirements for social media accounts requirements approved by the authorizing official. • Ensuring compliance with the document in addition to disseminating it to employees and relevant parties.	
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	Assessing cybersecurity risks for organization's social media accounts, once per year at least.
	Related Cybersecurity Tools: • Template for Cybersecurity Risk Management Policy • Template for Cybersecurity Risk Management Procedure • Template for Cybersecurity Risk Register **Controls implementation guidelines:** • Conduct a Risk Assessment to all organization's social media accounts at least once a year or less. To discover, identify, and mitigate potential risks related to social media accounts. • Conduct review against the identified risks for all the social media accounts of the organization at least once per year or less.	
	Expected Deliverables: • Risk Assessment report of all the organization's social media accounts as per the cybersecurity requirements of the organization, and review it periodically based on the specified date.	
	1-2-1-2	Assessing cybersecurity risks during planning and before permitting use of organization's social media accounts.
	Related Cybersecurity Tools: • Template for Cybersecurity Risk Management Policy • Template for Cybersecurity Risk Management Procedure • Template for Cybersecurity Risk Register **Controls implementation guidelines:** • Conduct Cybersecurity Risk Assessment during planning and before permitting use of organization's social media accounts.	
	Expected Deliverables: • Risk Assessment report of all the organization's social media accounts as per the cybersecurity requirements, prior of initial use of the accounts.	
	1-2-1-3	Including cybersecurity risks related to organization's social media accounts in the organization's cybersecurity risk register, and monitoring it at least once a year.
	Related Cybersecurity Tools: • Template for Cybersecurity Risk Management Policy • Template for Cybersecurity Risk Management Procedure • Template for Cybersecurity Risk Register **Controls implementation guidelines:**	

	• Define and document the cybersecurity risks for the organization's social media accounts. • Verify that the cybersecurity risk associated with the social media are included in the organization's cybersecurity risk register. • Review and monitor the social media risks at least every year or less.
	Expected Deliverables: • Inclusion of social media accounts' risks in the cybersecurity risk register. • Review report of cybersecurity risks associated with the requirements for the organization's social media accounts.
1-3	**Cybersecurity in Human Resources**
Objective	To ensure that cybersecurity risks and requirements related to personnel (employees and contractors) are managed efficiently prior to employment, during employment and after termination/separation as per organizational policies and procedures, and related laws and regulations.
Controls	
1-3-1	In addition to the subcontrols within control 1-9-4 in the ECC, the cybersecurity requirements for personnel responsible for managing the organization's social media accounts should include at least the following:
	1-3-1-1 Cybersecurity awareness about social media accounts.
	Related Cybersecurity Tools: • Plan for Cybersecurity Awareness Program • Template for Acceptable Use Policy • Template for Cybersecurity Human Resources **Controls implementation guidelines:** • Develop and document a social media cybersecurity awareness program, which must include topics such as use of social media, do's and don'ts of social media, managing access to the social media accounts, privacy issues on social media, types of cybercrimes social media accounts are prone to, organization's brand value on social media etc. • All personnel responsible for managing the social media accounts must be undergoing the cybersecurity awareness program for social media accounts. • Conduct the social media cybersecurity awareness program for employees and individuals responsible for managing social media accounts on a periodic basis and maintain record of training.
	Expected Deliverables:

	• Documented and approved customized awareness program for organization's social media. • Records of periodically conducted awareness sessions/training.	
	1-3-1-2	Implementation of and compliance with the cybersecurity requirements as per the organizational cybersecurity policies and procedures for the organization's social media accounts.
	Related Cybersecurity Tools: • Template for Cybersecurity Human Resources Policy • Template for Cybersecurity Policies Compliance • Template for Confidentiality Agreement **Controls implementation guidelines:** • Implement the cybersecurity requirements for the social media accounts as part of organizations' cybersecurity policies. • Verify the compliance to cybersecurity requirements for the social media accounts in a periodic basis, as defined in the organization's policies and procedures. • Ensure that all personnel have read and signed the Acceptable Use Policy.	
	Expected Deliverables: • Compliance report of cybersecurity requirements for the organization's social media accounts. • Sample of implementation of cybersecurity requirements for the social media accounts. • Sample of Acceptable Use Policy forms signed by the organization's personnel.	
1-4	**Cybersecurity Awareness and Training Program**	
Objective	To ensure that personnel are aware of their cybersecurity responsibilities and have the essential cybersecurity awareness. It is also to ensure that personnel are provided with the required cybersecurity training, skills and credentials needed to accomplish their cybersecurity responsibilities and to protect the organization's information and technology assets.	
Controls		
1-4-1	In addition to the subcontrols 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 the organization's social media accounts and the secure use to minimize these risks and threats, including the following:	
	1-4-1-1	Secure use and protection of devices dedicated to the organization's social media accounts and ensuring that they do not contain classified data or used for personal purposes.
	Related Cybersecurity Tools:	

		• Plan for Cybersecurity Awareness Program **Controls implementation guidelines:** • Develop and document a social media cybersecurity awareness program, which must include topics such as secure use of devices used for organization's social media accounts, review security configuration and hardening for social media devices, data protection of social media devices, prohibition of use of classified data or personal data of the employee on social media device. • All the personnel in the organization must be undergoing the cybersecurity awareness program for social media accounts. • Conduct the social media cybersecurity awareness program on a periodic basis and maintain record of training.
		Expected Deliverables: • Documented and approved customized awareness program for social media which includes secure use and protection of social media devices. • Sample of the awareness materials/contents provided to the organization's personnel.
	1-4-1-2	Secure handling of identities, passwords and security questions.
		Related Cybersecurity Tools: • Plan for Cybersecurity Awareness Program **Controls implementation guidelines:** • Develop and document a social media cybersecurity awareness program, which must include topics such as identity management of social media accounts, strong password policies, secure handling of identity credentials, setting up security questionnaire, multi-factor authentication on social media accounts. • All the personnel in the organization must be undergoing the cybersecurity awareness program for social media. • Conduct the social media cybersecurity awareness program on a periodic basis and maintain record of training.
		Expected Deliverables: • Documented and approved customized awareness program for social media which includes secure handling of identity and access of social media accounts. • Sample of the awareness materials/contents provided to the organization's personnel.
	1-4-1-3	Organization's social media accounts restoration plan and dealing with cybersecurity incidents.
		Related Cybersecurity Tools: • Plan for Cybersecurity Awareness Program

Controls implementation guidelines:

- Develop and document a social media cybersecurity awareness program, which must include topics such as incident and threat management for social media accounts, identification of incident, reporting of suspicious activity on social media account, restoration plan for social media account recovery.
- All the personnel in the organization must be undergoing the cybersecurity awareness program for social media.
- Conduct the social media cybersecurity awareness program on a periodic basis and maintain record of training.
- Establishing and documenting a plan for social media account recovery:
  - Contact information for the Cybersecurity Incident Response Team (IRT).
  - Timely notification to the Incident Response Team.
  - Documenting the incident after account recovery.

Expected Deliverables:

- Documented and approved customized awareness program for social media which includes social media account incident management and restoration plan.
- Sample of the awareness materials/contents provided to the organization's personnel.
- Documented plan to recover the organization's social media accounts.

1-4-1-4	Secure handling of applications and solutions used for the organization's social media accounts.

Related Cybersecurity Tools:

- Plan for Cybersecurity Awareness Program

Controls implementation guidelines:

- Develop and document a social media cybersecurity awareness program, which must include topics such as social media applications and solutions, security configuration hardening of applications and solutions, monitoring and logging of social media applications.
- All the personnel in the organization must be undergoing the cybersecurity awareness program for social media.
- Conduct the social media cybersecurity awareness program on a periodic basis and maintain record of training.

Expected Deliverables:

- Documented and approved customized awareness program for social media which includes secure handling of social media applications and solutions.
- Sample of the awareness materials/contents provided to the organization's personnel.

1-4-1-5	Not to use the organization's social media accounts for personal purposes such as browsing.

	Related Cybersecurity Tools: • Plan for Cybersecurity Awareness Program **Controls implementation guidelines:** • Develop and document a social media cybersecurity awareness program, which must include topics such as usage of organization's social media accounts, social media etiquettes for the account operations for the organization, prohibition of use of social media account for personal usage. • All the personnel in the organization must be undergoing the cybersecurity awareness program for social media. • Conduct the social media cybersecurity awareness program on a periodic basis and maintain record of training.	
	Expected Deliverables: • Documented and approved customized awareness program for social media which includes prohibition of usage of organization's social media account for personal usage. • Sample of the awareness materials/contents provided to the organization's personnel.	
	1-4-1-6	Avoiding accessing the organization's social media accounts using untrusted public devices or networks.
	Related Cybersecurity Tools: • Plan for Cybersecurity Awareness Program **Controls implementation guidelines:** • Develop and document a social media cybersecurity awareness program, which must include topics such as access to the social media accounts, avoiding public devices/networks or those which are not defined by organization's policies, risks associated with accessing social media accounts on untrusted public devices or networks. • All the personnel in the organization must be undergoing the cybersecurity awareness program for social media. • Conduct the social media cybersecurity awareness program on a periodic basis and maintain record of training.	
	Expected Deliverables: • Documented and approved customized awareness program for social media which includes prohibition of accessing organization's social media accounts using untrusted public devices or networks. • Sample of the awareness materials/contents provided to the organization's personnel.	
	1-4-1-7	Communicating directly with the cybersecurity department if a cybersecurity threat is suspected.
	Related Cybersecurity Tools: • Plan for Cybersecurity Awareness Program **Controls implementation guidelines:**	

	• Develop and document a social media cybersecurity awareness program, which must include topics such as incident response to social media cybersecurity threat, how to contact directly to cybersecurity department in case of a threat. • All the personnel in the organization must be undergoing the cybersecurity awareness program for social media. • Conduct the social media cybersecurity awareness program on a periodic basis and maintain record of training.
	Expected Deliverables: • Documented and approved customized awareness program for social media which includes communicating directly with cybersecurity department for suspected cybersecurity threat to social media accounts. • Sample of the awareness materials/contents provided to the organization's personnel.
1-4-2	In addition to the sub controls within control 1-10-4 in the ECC, personnel responsible for managing the organization's social media accounts must be trained on the required technical skills, plans and procedures necessary to ensure the implementation of the cybersecurity requirements and practices when using the organization's social media accounts.
	Related Cybersecurity Tools: • Plan for Cybersecurity Awareness Program **Controls implementation guidelines:** • Develop and document a training curriculum for the personnel to be trained for proper handling and management of social media accounts which must include required skills to manage the accounts, organization's social media standard controls as a part of procedures to follow for the cybersecurity requirements, implementation, operation and monitoring of social media accounts' activities for threat management. • Personnel responsible for managing the social media accounts in the organization must be undergoing the cybersecurity training for required skills and procedures. • Conduct the social media training program on a periodic basis and maintain record of training.
	Expected Deliverables: • Documented and approved customized training program for authorized personnel who are responsible for managing the organization's social media accounts. • Sample records of training conducted for or attended by personnel responsible for managing the social media accounts.

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 managing information and technology assets must include at least the following:	
	2-1-1-1	Identifying and inventorying organization's social media accounts, and information and technology assets related to them, and updating them at least once, every year.
	Related Cybersecurity Tools: • Template for Asset Management Policy • Template for Asset Management Standard including Classification Guidelines **Controls implementation guidelines:** • Identify and document the list of social media accounts, along with the associated information and technology assets related to them, across all the platforms that are used by the organization. • Maintain and periodically review the inventory of social media assets at least once a year or less.	
	Expected Deliverables: • Documented and approved inventory of all the social media accounts with related assets. • Periodic review report of inventory of social media assets of the organization.	
2-2	**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 tasks.	
Controls		
2-2-1	In addition to the subcontrols within control 2-2-3 in the ECC, cybersecurity requirements for identity and access management related to organization's social media accounts must include at least the following:	
	2-2-1-1	Using social media accounts designated for organizations, not individuals

	Related Cybersecurity Tools: • Template for Identity and Access Management Policy **Controls implementation guidelines:** • Identify organization's social media accounts across all social media platforms, excluding accounts belonging to individuals with official titles (e.g., Excellencies and Honors). • Ensuring the secure usage and management of these accounts.	
	Expected Deliverables: • Sample of social media accounts used in the organization to verify that it is designated only for organizations and not individuals. And it should be noted that individuals referred to within the organization may either be responsible for managing the organizations social media accounts or may be regular users for these accounts, such as employees, clients, and affiliates of the organization. In both cases, they are required to adhere to the organization's policy, regarding the use of social media accounts.	
	2-2-1-2	Registering using official information (official specific social media email and official mobile number), and do not use personal information.
	Related Cybersecurity Tools: • Template for Identity and Access Management Policy **Controls implementation guidelines:** • Verify that the social media accounts of the organization are registered only using official email and official mobile number that are designated only for social media accounts. Further, confirm that personal information of any personnel is not used to create organization's social media account.	
	Expected Deliverables: • Sample of the official information used for registration of social media account.	
	2-2-1-3	Verifying organization's social media accounts whenever possible and maintaining a consistent identity across all organization's social media accounts used; to facilitate knowledge of official accounts, and to discover fraud or unofficial accounts.
	Related Cybersecurity Tools: • Template for Identity and Access Management Policy **Controls implementation guidelines:** • Verify that the social media accounts of the organization are verified/authorized by the social media platform. Further, verify that the social media accounts have consistent identity across all organization's social media accounts used.	
	Expected Deliverables:	

	• Sample of organization's social media accounts that have been verified/authorized by the social media platform.
2-2-1-4	Using a secure and specific password for each organization's social media account, changing the password regularly, and not to repeat use of passwords.
	Related Cybersecurity Tools: • Template for Identity and Access Management Policy • Template for Identity and Access Management Standards, encompassing password management **Controls implementation guidelines:** • Verify that each social media account is registered using a secure password that is different than the passwords used for the other social media accounts. Further, verify and implement the periodic change of social media accounts' passwords regularly and without using previously used passwords.
	Expected Deliverables: • Documented social media accounts controls specifying that cybersecurity requirements for password management of social media accounts. • Periodic reports that details changes in the passwords of social media accounts.
2-2-1-5	Using multi-factor authentication for organization's social media accounts logins.
	Related Cybersecurity Tools: • Template for Identity and Access Management Policy **Controls implementation guidelines:** • Verify that the organizations' social media accounts are using multi-factor authentication for logging in to the accounts. This must be done using the credentials and devices of the organization for added security.
	Expected Deliverables: • Sample of using multi-factor authentication while logging in to the social media accounts.
2-2-1-6	Activating and updating security questions and documenting them in a safe place.
	Related Cybersecurity Tools: • Template for Identity and Access Management Policy **Controls implementation guidelines:** • Verify that the organizations' social media accounts are using security questions for security purposes. Further, review and verify that the security questions are updated periodically and documented securely with restricted access to only the authorized personnel.

	Expected Deliverables: • Documented social media accounts controls requiring the setup and update of security questions for the organizations' social media accounts. • Documented security questions in a secured and restricted file with access only to authorized personnel.
2-2-1-7	Managing organization's social media accounts access rights based on business need, considering the sensitivity of the accounts, the level of access rights and the type of devices and systems used.
	Related Cybersecurity Tools: • Template for Identity and Access Management Policy **Controls implementation guidelines:** • Verify that the access rights to organizations' social media accounts are based on the business needs of the organization, the sensitivity of accounts, and the type of devices and systems used.
	Expected Deliverables: • Documented social media accounts controls restricting the access rights of social media accounts based on the business needs within the organization considering the sensitivity of the accounts, the level of access rights, and the type of devices and systems used. • Documented procedure of granting access to social media accounts (provisioning workflow). • Sample of approved and implemented access right requests.
2-2-1-8	Restricting access rights of service providers of social media management, social media monitoring or brand protection.
	Related Cybersecurity Tools: • Template for Identity and Access Management Policy **Controls implementation guidelines:** • Identify, document, and verify the access rights of social media account management service providers, monitoring social media platforms, or safeguarding the organization's identity from fraud.
	Expected Deliverables: • Documented social media controls restricting the access rights of social media accounts to the service providers. • Sample of access rights granted to service providers.
2-2-1-9	Restricting access to organization's social media accounts to specific devices.
	Related Cybersecurity Tools: • Template for Identity and Access Management Policy

	Controls implementation guidelines: • Verify that the access rights to organizations' social media accounts are restricted to specific devices. • Use social media accounts management platforms and services.
	Expected Deliverables: • Documented social media accounts controls restricting the access rights of social media accounts to specific devices. • Sample of social media accounts configurations to restrict the access from specific device. • Sample of social media account management platforms and services configurations that allow specifying the devices permitted to access the organization's social media accounts.
2-2-2	With reference to ECC subcontrol 2-2-3-5, user identities and access rights used for organization's social media accounts must be reviewed at least once every year.
	Related Cybersecurity Tools: • Template for Identity and Access Management Policy **Controls implementation guidelines:** • Inventory and document the user identities and access rights used for organization's social media accounts. • Maintain and periodically review all the user identities and access rights at least every year or less.
	Expected Deliverables: • Review report of user identities and access rights of organization's social media accounts.
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 subcontrols in ECC control 2-3-3, cybersecurity requirements for protecting organization's social media accounts and technology assets related to them must include at least the following:
	2-3-1-1 — Applying updates and security patches for social media applications at least once a month.
	Related Cybersecurity tools: • Template for Patch and Update Management Standard • Template for Patch and Update Management Packages Policy **Controls implementation guidelines:**

	• Identify the applications handling the social media accounts. • Review the patching guidance with respect to the social media applications utilized and document the patching procedures to be followed in line with the guidance. • Periodic security patching and updates must be conducted at least every month or less for applications handling social media accounts.	
	Expected Deliverables: • Documented procedures for security patches and updates for social media applications. • Periodic report for security patches and updates implemented on social media accounts applications.	
	2-3-1-2	Reviewing configurations and hardening of organization's social media accounts and technology assets related to them at least once a year.
	Related Cybersecurity tools: • Template for Configuration and Hardening Policy • Template for Secure Configuration and Hardening Standard • Template for Social Media Security Standard **Controls implementation guidelines:** • Identify the applications that are used by the organization that handles social media accounts. • Review the guidelines and procedures for protection and hardening related to social media account application and adhere to them when implementing protection and hardening on the applications. • Periodic security configuration and hardening must be conducted at least annually or earlier for applications handling social media accounts.	
	Expected Deliverables: • Documented security hardening procedures for applications handling social media accounts. • Secure configurations and hardening review report that have been conducted periodically.	
	2-3-1-3	Reviewing and hardening default configurations, such as default passwords, pre-login, and lockout, for organization's social media accounts and technology assets related to them.
	Controls implementation guidelines: • Identify the technology assets and systems handling social media accounts.	

	• Document and approve security configuration and hardening policy for all technology assets. • Review the default configurations which includes, but not limited to, default passwords, pre-login, account lockout, guests accounts, service accounts, backgrounds, default administrators, legacy protocols, open ports in the system. • Verify and ensure that the security configurations must not be set as default for the technology assets.	
	Expected Deliverables: • Documented policies and procedures for hardening default settings. • Sample of default configurations for social media accounts. • Default configuration review report for social media accounts.	
	2-3-1-4	Restricting activation of features and services in social media accounts on need basis and carrying out risk assessment if there is a need to activate it.
	Controls implementation guidelines: • Identify the applications handling the social media accounts. • Document and approve security configuration and hardening policy for all technology assets. • Review the features and services within the social media account and perform a risk assessment before activating these features. Further, verify that only those services are activated which are required based on the risk assessment conducted.	
	Expected Deliverables: • Documented risk assessment of social media accounts and their features before activation.	
2-4	**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		
2-4-1	In addition to the subcontrols within control 2-6-3 in the ECC, cybersecurity requirements for mobile device security related to organization's social media accounts must include at least the following:	
	2-4-1-1	Centrally manage mobile devices for organization's social media accounts using a Mobile Device Management system (MDM).
	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 list of mobile devices in the organization that are used for handling organization's social media accounts. • 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 social media accounts.	
	Expected Deliverables: • Documented list of all the mobile devices in the organization used for handling organization's social media accounts. • Sample of Mobile Device Management (MDM) system's configurations.	
	2-4-1-2	Applying updates and security patches on mobile devices, at least once every month.
	Related Cybersecurity Tools: • Template for User Devices, Mobile Devices, and Personal Devices Security Policy **Controls implementation guidelines:** • Identify the list of mobile devices in the organization that are used for handling organization's social media accounts. • Review guidelines and procedures for updates and patches related to mobile devices handling social media accounts, and adhere to them when applying security and hardening measures on mobile devices. • Periodic security patching and updates must be conducted at least every month or earlier for mobile devices handling social media accounts.	
	Expected Deliverables: • Documented security patching procedures for social media applications. • Patching review report for periodic security patching.	
2-5	**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		
2-5-1	In addition to the subcontrols in ECC control 2-7-3, cybersecurity requirements for protecting and handling data and information for organization's social media accounts must include at least the following:	

	2-5-1-1	Technology assets for management of organization's social media accounts must not contain classified data, per relevant regulations.
	Related Cybersecurity Tools: • Template for Cybersecurity Data Policy • Template for Cybersecurity Data Standard **Controls implementation guidelines:** • Review and verify that only relevant classification of data is present in the technology assets used for handling organization's social media accounts and no confidential data of the organization is present in these assets, in accordance with the organizational policies and procedures, as well as related national laws, regulations and agreements. •	
	Expected Deliverables: • Review report of data classification contained in the assets used for handling organization's social media accounts..	
2-6	**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		
2-6-1	In addition to the subcontrols in ECC control 2-12-3, cybersecurity requirements for event logs and monitoring management for organization's social media accounts and technology assets related to them must include at least the following:	
	2-6-1-1	Activating all notifications and cybersecurity alerts for organization's social media accounts and cybersecurity events logs on related technology assets.
	Related Cybersecurity Tools: • Template for Cybersecurity Event Logs and Monitoring Management Policy • Template for Cybersecurity Event Logs and Monitoring Management Standard **Controls implementation guidelines:** • Identify the technical assets and systems handling social media accounts. • Implement the activation of all notifications and alerts for cybersecurity events related to the logging of events for the organization's social media accounts.	
	Expected Deliverables:	

	• Sample of cybersecurity notifications and alerts activated for events on the assets used for handling organization's social media accounts.
2-6-1-2	Following organization's social media accounts and monitoring them to ensure that they do not post any unauthorized content, or login any unauthorized access.
	Related Cybersecurity Tools: • Template for Cybersecurity Event Logs and Monitoring Management Policy **Controls implementation guidelines:** • Identify, document, and approve procedures for monitoring social media accounts to ensure no unauthorized content is published or unauthorized access occurs. • Review the content of the organization's social media accounts by monitoring their accounts and observing their content and activities. • Verify that the content posted on social media accounts is authorized. • Regularly review the procedures for monitoring social media accounts.
	Expected Deliverables: • Documented procedures for monitoring social media accounts. • Review content that is posted on the organization's social media accounts.
2-6-1-3	Monitoring social media networks to ensure the organization is not being impersonated.
	Related Cybersecurity Tools: • Template for Cybersecurity Event Logs and Monitoring Management Policy **Controls implementation guidelines:** • Monitoring the social media account networks within the organization to ensure that all accounts and channels are authorized, and that no account is impersonating the identity of the organization and posting on its behalf. In the event of identity theft, appropriate action should be taken regarding the impersonated account, and the reporting mechanism for social media accounts should be implemented.
	Expected Deliverables: • Review of social media network for impersonation of organization's social media plan. • Sample of the service used for brand protection. • Documented procedure for handling identity impersonation of the organization, including specifying the necessary actions to be taken. • Plan for reporting in case of social media account impersonation. • Define and document non-discloure clauses for the organization's social media accounts.

	2-6-1-4	Automated monitoring for any change in the accounts pattern, indicators of compromise, or the publication of any unauthorized content or impersonation of the organization.
	Related Cybersecurity Tools: • Template for Cybersecurity Event Logs and Monitoring Management Policy **Controls implementation guidelines:** • Review and verify the social media accounts of the organization for any change in account patterns, indicators of compromise or the publication of any unauthorized content or impersonation, through automated monitoring of the network.	
	Expected Deliverables: • Automated monitoring of organizations' social media accounts for any anomaly in behaviour.	
2-7	**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		
2-7-1	In addition to the subcontrols within control 2-13-3 in ECC, cybersecurity requirements for incident and threat management in the organization must include at least the following:	
	2-7-1-1	Developing a plan to recover the organization's social media accounts and to deal with cyber incidents.
	Related Cybersecurity Tools: • Template for Cybersecurity Incident Management and Threat Policy • Template for Cybersecurity Incident Management and Threat Standard • Guideline for Cybersecurity Incident Response • Templates for Cybersecurity Incident Response Detailed Plan. **Controls implementation guidelines:** • Define and document the recovery plan for the organization's social media accounts for which the control of the account is lost by the organization due to any cybersecurity incident or otherwise. • Ensure the following in the social media account recovery plan: - Contact information for the Cybersecurity Incident Response Team (IRT). - Timely notification to the Incident Response Team. - Documenting the incident after account recovery	

	Expected Deliverables: • Documented recovery plan for organization's social media accounts.

3 (Third-Party Cybersecurity)

3-1	Third-Party Cybersecurity	
Objective	To ensure the protection of assets against the cybersecurity risks related to third-parties including outsourcing and managed services as per organizational policies and procedures, and related laws and regulations	
Controls		
3-1-1	A need assessment for the use of social media management, automated monitoring or brand protection services along with associcated cybersecurity risks must be conducted.	
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:** • In case there is a need to use social media account management services, automated monitoring of social media accounts, or protection against impersonation, a study and assessment of the necessity for such actions must be conducted, considering the associated cybersecurity risks. The results should be documented and approved by the authorized party.	
	Expected Deliverables: • Documented report to assess the needs of the organization before resorting to external parties' services for managing social media accounts, automated monitoring, or brand protection services. • Documented report for the risk assessment that conducted before resorting to external parties' services for managing social media, automated monitoring or brand protection services. • Documented report to assess the needs of the organization using social media management, automated monitoring or brand protection services.	
3-1-2	In addition to the subcontrols within control 4-1-2 in ECC, cybersecurity requirements for use of social media management, automated monitoring or brand protection services in the organization must include at least the following:	
	3-1-2-1	Non-disclosure clauses and secure removal of organization's data by the third-party upon service termination
	Related Cybersecurity tools: • Template for Cybersecurity Policy Related to Third-Parties **Controls implementation guidelines:** • Review the service level agreement between the organization and third-parties who are responsible of managing social media accounts, automated monitoring or brand protection services firm.	

- Verify that the non-disclosure clauses and secure removal of organization's data are documented in the agreement. Further, verify that the services firm must also provide evidence of secure removal of data to the organization.

Expected Deliverables:

- Documented service level agreement with third-parties who are responsible of managing social media accounts, automated monitoring or brand protection services firm that includes clauses of non-disclosure and secure data removal upon service termination.

3-1-2-2	Communication procedures to report vulnerabilities and cyber incidents.

Related Cybersecurity tools:

- Template for Cybersecurity Policy Related to Third-Parties

Controls implementation guidelines:

- Review the service level agreement between the organization and third-parties who are responsible of managing social media accounts, automated monitoring or brand protection services firm.
- Verify and document the procedures to be followed by the services firm with respect to the incident management of cyber incidents and reporting of vulnerabilities to the organization in a timely manner, in the contract or the service level agreements.

Expected Deliverables:

- Documented procedures for cyber incidents and reporting of vulnerability to the organization, in the contract or service level agreement.

3-1-2-3	Requirements for the third-party to comply with cybersecurity requirements and policies to protect organizations' social media accounts, and related laws and regulation.

Related Cybersecurity tools:

- Template for Cybersecurity Policy Related to Third-Parties

Controls implementation guidelines:

- Review the service level agreement between the organization and third-parties who are responsible of managing social media accounts, automated monitoring or brand protection services firm.
- Verify and document the requirements for the services firm to comply with the cybersecurity requirements and policies to protect organizations' social media accounts in line with the organizational policies and procedures of the authority and the relevant national legal and regulatory requirements, in the service level agreement.

Expected Deliverables:

	• Documented procedures for compliance with the cybersecurity requirements and policies of the organization, and the relevant national legal and regulatory requirements in the service level agreement.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority