



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Organizations' Social Media Accounts

Cybersecurity Controls

(OSMACC -1:2021)

Sharing Notice: **White**
Document Classification: **Open**

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

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 and Confidential to the Recipient only**

The recipient is not allowed to share red-classified materials with any person, from within or outside the organization, beyond the scope specified for receipt.

 **Amber – Limited Sharing**

The recipient of amber-classified materials may share the information contained therein with concerned personnel only in the same organization, and with those competent to take procedures with regard to the information.

 **Green – Sharing within the Same Community**

Green-classified materials may be shared with others within the same organization or in other organization that have relations with your organization or are operating in the same sector. However, such materials may not be shared or exchanged through public channels.


 **White – No Restrictions**

Table of Contents

Executive Summary	8
Introduction	9
Objectives	10
Scope of Work and Applicability	10
Scope of Work	10
Statement of Applicability	10
Implementation and Compliance	11
Update and Review	11
OSMACC Domains and Structure	12
Main Domains and Subdomains of OSMACC	12
Structure	13
OSMACC	14
Appendices	20
Appendix (A): The relationship with the Essential Cybersecurity Control	20

List of Tables

Table (1): OSMACC Structure	13
-----------------------------	----

List of the Figures & Illustrations

Figure (1): OSMACC Main Domains and Subdomains	12
Figure (2): OSMACC Controls Coding Scheme	13
Figure (3): OSMACC Controls Structure	13
Figure (4): Guide to Colors of Subdomains in Figure 5	20
Figure (5): ECC and OSMACC Subdomains	21

Executive Summary

Social networks are one of the enablers for rapid and effective communication with the beneficiaries, which contributes to a speedy response and improving and facilitating the experience of the beneficiaries. With the increase in the use of social networks officially by organizations inside the Kingdom to communicate with the beneficiaries, the risk of theft crimes of official social media accounts, misuse of them or impersonation has increased, which necessitates setting cybersecurity requirements to reduce these risks.

To contribute to reducing these risks and enhancing the protection of organizations' social media accounts, with the aim of reaching a safe and reliable Saudi cyber space that enables growth and prosperity; The National Cybersecurity Authority has developed the Organizations' Social Media Accounts Cybersecurity Controls (OSMACC - 1: 2021) to set the minimum cybersecurity requirements to enable organizations to use social networks in a safe manner. This document explains the details of the Organizations' Social Media Accounts Cybersecurity Controls, their goals, scope of work, and compliance approach and monitoring.

Organizations must implement all necessary measures to ensure continuous compliance with these controls, in order to comply with item 3 of article 10, in the mandate of the National Cybersecurity Authority.

Introduction

The National Cybersecurity Authority (referred to in this document as “The Authority”) has developed the Organizations' Social Media Accounts Cybersecurity Controls (OSMACC - 1: 2021) after conducting a study of cybersecurity best practices and analyzing previous cyber incidents and attacks. This comes within the mandate and tasks of The Authority according to its mandate as per the Royal Decree No. (6801) dated 11/2/1439 AH, “Establishing policies, governance mechanisms, frameworks, standards, controls and guidelines related to cybersecurity, circulating them to the relevant organization, following up on compliance with them, and updating them.”

Social networks are one of the enablers for rapid and effective communication with the beneficiaries, which contributes to a speedy response and improving and facilitating the experience of the beneficiaries. With the increase in the use of social networks officially by organizations inside the Kingdom to communicate with the beneficiaries, the risk of theft crimes of official social media accounts or misuse of them has increased. In addition, the risk of impersonation of official organizations in social networks.

To contribute to reducing these risks and enhancing the protection of organizations' social media accounts, with the aim of reaching a safe and reliable Saudi cyber space that enables growth and prosperity; The National Cybersecurity Authority has developed the Organizations' Social Media Accounts Cybersecurity Controls (OSMACC - 1: 2021) to set the minimum cybersecurity requirements to enable Organizations' to use social networks in a safe manner.

In preparing the Organizations' Social Media Accounts Cybersecurity Controls, The Authority has been keen to align its components with the components of the Essential Cybersecurity Controls that are a basic requirement for the OSMACC. Adherence to OSMACC can only be achieved by achieving continuous compliance with the Essential Cybersecurity Controls in the first place, as they are linked to relevant national and international legislative and regulatory requirements.

The Organizations' Social Media Accounts Cybersecurity Controls consist of the following:

- 3 Main Domains
- 12 Subdomains
- 15 Main Controls
- 38 Subcontrols

Objectives

The Organizations' Social Media Accounts Cybersecurity Controls aim to:

- Contribute to raising the level of cybersecurity at the national level.
- Enabling organizations to use social networks in a safe manner.
- Readiness to respond effectively to cyber incidents that may have negative impacts.

Scope of Work and Applicability

Scope of Work

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.

Statement of Applicability

These controls have been prepared so that they are compatible with the cybersecurity requirements for all organizations and sectors in the Kingdom of Saudi Arabia taking into account the diversity and nature of work, and The Organization that uses social networks must adhere to all the controls applicable to it.

Implementation and Compliance

In order to comply with item 3 of article 10, in the mandate of the National Cybersecurity Authority, organizations must implement all necessary measures to ensure continuous compliance with these controls, which cannot be achieved without achieving continuous compliance with the Essential Cybersecurity Controls (ECC – 1: 2018) where applicable.

The Authority evaluates organizations' compliance with the OSMACC through multiple means such as self-assessments by the organizations, and/or on-site audits, in accordance with the mechanisms deemed appropriate by the Authority.

Update and Review

The Authority will periodically review and update the OSMACC as per the cybersecurity requirements and the related industry updates. The Authority will communicate and publish the updated version of OSMACC for implementation and compliance.

OSMACC Domains and Structure

Main Domains and Subdomains of OSMACC

Figure (1) below shows the main domains and subdomains of the Organizations' Social Media Accounts Cybersecurity Controls. Appendix (A) shows the relationship with the Essential Cybersecurity Controls.

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 1: OSMACC Main Domains and Subdomains

Structure

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



Figure (2): OSMACC Controls Coding Scheme

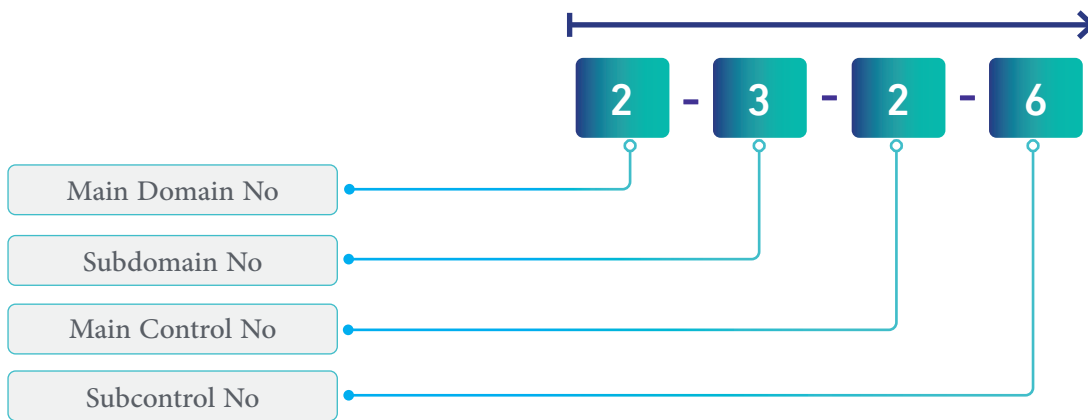


Figure 3: OSMACC Controls Structure

Table (1) shows the structure of OSMACC.

	Name of Main Domain
Reference number of the Main Domain	
Reference number of the Subdomain	Name of Subdomain
Objective	
Controls	
Reference number of the control	Control clauses

Table1 : OSMACC Structure

Organizations' Social Media Accounts Cybersecurity Controls (OSMACC)

1 Cybersecurity Governance

1-1	Cybersecurity Policies and Procedures
Objective	To ensure that cybersecurity requirements are documented, communicated and complied 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: <ul style="list-style-type: none"> 1-1-1-1 Defining and documenting the cybersecurity requirements for organizations' social media accounts as part of the organization's cybersecurity policies.
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: <ul style="list-style-type: none"> 1-2-1-1 Assessing cybersecurity risks for organization's social media accounts, once per year at least. 1-2-1-2 Assessing cybersecurity risks during planning and before permitting use of organization's social media 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.
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	<p>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:</p> <p style="margin-left: 40px;">1-3-1-1 Cybersecurity awareness about social media accounts.</p> <p style="margin-left: 40px;">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.</p>
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	<p>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:</p> <p style="margin-left: 40px;">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.</p> <p style="margin-left: 40px;">1-4-1-2 Secure handling of identities, passwords and security questions.</p> <p style="margin-left: 40px;">1-4-1-3 Organization's social media accounts restoration plan and dealing with cybersecurity incidents.</p> <p style="margin-left: 40px;">1-4-1-4 Secure handling of applications and solutions used for the organization's social media accounts.</p> <p style="margin-left: 40px;">1-4-1-5 Not to use the organization's social media accounts for personal purposes such as browsing.</p> <p style="margin-left: 40px;">1-4-1-6 Avoiding accessing the organization's social media accounts using untrusted public devices or networks.</p> <p style="margin-left: 40px;">1-4-1-7 Communicating directly with the cybersecurity department if a cybersecurity threat is suspected.</p>
1-4-2	In addition to the subcontrols 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.

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	<p>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:</p> <p style="margin-left: 20px;">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.</p>
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 assigned tasks.
Controls	
2-2-1	<p>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 shall include at least the following:</p> <p style="margin-left: 20px;">2-2-1-1 Using social media accounts designated for organizations, not individuals.</p> <p style="margin-left: 20px;">2-2-1-2 Registering using official information (official specific social media email and official mobile number), and do not use personal information.</p> <p style="margin-left: 20px;">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.</p> <p style="margin-left: 20px;">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.</p> <p style="margin-left: 20px;">2-2-1-5 Using multi-factor authentication for organization's social media accounts logins.</p> <p style="margin-left: 20px;">2-2-1-6 Activating and updating security questions and documenting them in a safe place.</p>

	<p>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.</p> <p>2-2-1-8 Restricting access rights of service providers of social media management, social media monitoring or brand protection.</p> <p>2-2-1-9 Restricting access to organization's social media accounts to specific devices.</p>
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.
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	<p>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:</p> <p>2-3-1-1 Applying updates and security patches for social media applications at least once a month.</p> <p>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.</p> <p>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.</p> <p>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.</p>
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	<p>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:</p> <p>2-4-1-1 Centrally manage mobile devices for organization's social media accounts using a Mobile Device Management system (MDM).</p> <p>2-4-1-2 Applying updates and security patches on mobile devices, at least once every month.</p>

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.
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. 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. 2-6-1-3 Monitoring social media networks to ensure the organization is not being impersonated. 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.
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.

3 Third Party and Cloud Computing Cybersecurity

3-1	Third-Party Cybersecurity
Objective	To ensure the protection of assets against the cybersecurity risks related to third-parties including outsourcing and managed services as per organizational policies and procedures, and related laws and regulations.
Controls	
3-1-1	A need assessment for the use of social media management, automated monitoring or brand protection services along with associated cybersecurity risks must be conducted.
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: <ul style="list-style-type: none"> 3-1-2-1 Non-disclosure clauses and secure removal of organization's data by the third-party upon service termination. 3-1-2-2 Communication procedures to report vulnerabilities and cyber incidents. 3-1-2-3 Requirments for the third-party to comply with cybersecurity require-ments and policies to protect organizations' social media accounts, and related laws and regulation.

Appendices

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

The Organizations' Social Media Accounts Cybersecurity Controls is an extension to the Essential Cybersecurity Controls (ECC- 1: 2018) as shown in figures (4) and (5), through the following:

- (12) subdomains, to which cybersecurity controls have been added for organizations' social media accounts
- (17) subdomains, to which no additional cybersecurity controls have been added for organizations' social media accounts

	Subdomains where cybersecurity controls have been added for organizations' social media accounts
	Subdomains where no additional cybersecurity controls have been added for organizations' social media accounts

Figure 4: Guide to Colors of Subdomains in Figure 5

1- Cybersecurity Governance	Cybersecurity Strategy		Cybersecurity Management	
	1-1	Cybersecurity Policies and Procedures	Cybersecurity Roles and Responsibilities	
	1-2	Cybersecurity Risk Management	Cybersecurity in Information Technology Projects	
	Cybersecurity Regulatory Compliance		Cybersecurity Periodical Assessment and Audit	
	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	Email Protection	
	Networks Security Management		2-4	Mobile Devices Security
	2-5	Data and Information Protection	Cryptography	
	Backup and Recovery Management		Vulnerabilities Management	
	Penetration Testing		2-6	Cybersecurity Event Logs and Monitoring Management
	2-7	Cybersecurity Incident and Threat Management	Physical Security	
	Web Application Security			
	3- Cybersecurity Resilience		Cybersecurity Resilience aspects of Business Continuity Management (BCM)	
4- Third-Party and Cloud Computing Cybersecurity	3-1	Third-Party Cybersecurity	Cloud Computing and Hosting Cybersecurity	
5 - ICS Cybersecurity	Industrial Control Systems (ICS) Protection			

Figure 5: ECC and OSMACC Subdomains



الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

