

Security guidelines for using social media

July 2024

Page 1	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
-----------	-------------------------	-----------	---	---



Issuance and Distribution:

Issuing Authority	Email	Issue Date
General Directorate of Policies and Governance Ministry of Transport, Communications and Information Technology	Governance@mtcit.gov.om	2024

Document Log:

Version	Date	Issuing Authority	Notes
0.1	2016	Information Technology Authority	
0.2	2024	Ministry of Transport, Communications and Information Technology	

Publication List:

1.	All administrative units of the state.
2.	The ministry's website.

Page 2	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
-----------	-------------------------	-----------	---	---



Table of Contents:

Definitions.....	4
Introduction.....	5
Purpose.....	5
Scope of Application.....	5
Objectives.....	5
Protection of Social Media Account Security for Government Institutions.....	6
First: Account Management.....	6
Second: Content Management.....	6
Third: Privacy, Confidentiality, and Security.....	7
Guidelines for Social Media Users.....	7
First: Devices Used to Access and Interact with Social Media.....	7
Second: Password Characteristics.....	8
Third: Enabling Additional Authentication Features on Certain Social Media Platforms..	9
Fourth: Publishing and Engagement Standards.....	9
Fifth: Verification of Official Accounts.....	10
Sixth: In the Event of a Security Breach of an Institutional Account.....	11
Seventh: Procedures for Recovering Accounts on Certain Social Media Platforms.....	11
Eighth: In the Event That Account Recovery Is Not Possible.....	11
Ninth: Related Publications.....	12

Page 3	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
-----------	-------------------------	-----------	---	---

Definitions

The Ministry:

Ministry of Transport, Communications and Information Technology.

Administrative Units of the State:

Refers to ministries, military and security agencies, councils, and other executive units that derive their authority from the state, whatever their name, including public legal persons, such as public institutions and public bodies, which are based on managing a public service or economic facility (as defined in Sultanic Decree No. 75/2020 regarding the administrative apparatus of the state).

Social Engineering:

An expression for low-tech or non-technical means used to attack information systems; such as impersonation, tricks, extortion, and threats.

Beneficiary:

All segments of society who contribute their general participation, including citizens and residents of the Sultanate, governmental bodies, civil society organizations, and non-governmental organizations, as well as private entities operating in the Sultanate.

Social Media:

These are sites that allow users to communicate virtually and share various events such as daily, political, and social issues. Content publishing is done in several formats such as texts, images, and video files. Examples of social media platforms include: Facebook, X, Instagram, LinkedIn, and others.

Official Account:

The unit's dedicated social media account that has been approved and represents the media front for that unit, publishing its statements and news.

Page 4	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
-----------	-------------------------	-----------	---	---



Introduction

The Sultanate is witnessing remarkable progress in the communications and information technology sector to keep pace with continuous technological developments, as many government services have been made available via the Internet, and the number of government units communicating with beneficiaries via social media has increased. In view of the increasing security incidents and surrounding risks and the growing threats against social media programs and sites, the Ministry of Transport, Communications and Information Technology strives diligently to improve the level of protection of official accounts used in social media programs and sites and their associated applications to protect them from hacking or attempts to impersonate their official status for the purpose of broadcasting rumors or misuse. The Ministry is working to update and establish security guidelines and measures to comply with challenges and requirements.

Purpose

Updating the security guidelines and measures for official social media accounts of the state's administrative units and their related applications to comply with security challenges and requirements.

Scope of Application

All administrative units of the state.

Objectives

This guide aims to enhance the security of social media accounts for the administrative units of the state, provided that it does not conflict with the internal security policies of the units or those issued by the Ministry of Transport, Communications and Information Technology.

Page 5	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
-----------	-------------------------	-----------	---	---



Protecting the Security of Social Media Accounts Affiliated with the Unit

This guide provides a set of security procedures and measures to protect government accounts on social media (Annex 1), in order to limit potential threats and work on:

First: Account Management

The unit must designate an employee responsible for managing its official accounts, and this should only be done after issuing a decision authorizing him to carry out this task, provided

that this decision includes the name of the employee and his job title. The employee responsible for managing this account/accounts must observe the following controls when selecting him:

- The employee's knowledge of the issues that will be discussed and communicated with the public through the various accounts.
- The employee's awareness of the risks related to social engineering, potential fraud methods, and how to counter them and avoid falling into related security errors.
- Possession of communication skills with the public and proficiency in the language.
- Technical awareness of using social media sites.
- The employee's readiness to be in contact with the public through social media channels and to deal with situations that may require a response or any other action at any time of the day and throughout the week (outside official working hours).
- The employee's awareness that he represents the unit and therefore represents the government in everything that is presented through the unit's accounts.
- Adherence to providing comprehensive and transparent information to the beneficiary.
- Not using the unit's accounts for personal purposes that do not serve the unit's objectives and directions in any way.
- Not using personal accounts for communicating with the public in everything related to the unit's affairs.

Second: Content Management

- The unit must establish an official mechanism for publishing on its social media, provided that it complies with the security requirements issued in the security design framework document for electronic services and applications.
- The unit's communication with the beneficiary must be purposeful and not random to ensure that the message is broadcast correctly and quickly.

Page 6	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
-----------	-------------------------	-----------	---	---



- The employee responsible for managing the unit's accounts must retweet or favorite suggestions and opinions of the beneficiary that contribute to developing or improving the services provided by the unit and its policies, provided that it does not conflict with the unit's direction.

Third: Security, Confidentiality, and Privacy

The employee responsible for managing the unit's accounts must adhere to the following:

- Take all necessary measures to protect information and data from any potential risks, such as hacking or broadcasting misleading messages.
- Ensure the use of the official website when attempting to log in to the unit's accounts.
- Coordinate with the information security department and the technical team in the unit for the purpose of:
 - Providing the necessary protection from the risks of phishing, social engineering, or attacks on web applications.
 - Raising employees' awareness of the risks related to social engineering and potential fraud methods, and how to counter them and avoid falling into related security errors.

Guidelines for Managing Unit Accounts on Social Media

Security measures and procedures contained in the unit's information security policy must be taken, and emphasis must be placed on applying the following requirements:

First: Devices Used for Accessing and Interacting with Social Media

The unit must follow the best methods and means to protect the device used to manage social media accounts affiliated with it by applying the following:

- A dedicated device must be used for social media accounts related to the unit, and its use for any other purposes is prohibited.
- Do not use the personal device of the account supervisor for managing the unit's accounts.
- Secure the device with a strong password (it is not recommended to use a PIN or pattern, as there are many tricks and means to access them).
- Activate automatic screen/device lock after a few seconds of inactivity.
- Do not install any other applications on the device or use the Internet or email for purposes unrelated to the institution's interaction with social media accounts, in order to reduce the possibility of it being infected with malicious software or hacked.

Page 7	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
-----------	-------------------------	-----------	---	---



- The application for the social media service must be downloaded from the official app store (such as Google Play or Apple Store), and no programs of unknown origin should be downloaded from outside the official stores.
- Ensure that the device tracking and automatic locking feature is activated in case of theft or loss, to facilitate its recovery and protect the device.
- Refrain from accessing unnecessary applications and functions on devices, or downloading and installing games and other applications prevalent in some social media programs.
- Do not download any third-party application (such as applications that contain additional features beyond the official applications), or suspicious or unofficial applications.
- Do not allow any other application to synchronize with social media programs or allow it to use the permissions of official programs.
- Use a trusted network for Internet connection and avoid public and free wireless networks.
- Ensure that the operating system, browser, and social media applications are updated with the latest versions regularly to avoid security threats.
- Ensure that anti-virus and anti-malware programs are updated regularly.
- It is prohibited to use external Proxy or VPN programs for Internet connection.
- Avoid accessing unknown links that are sent via email or appear on Internet pages.
- The number associated with the account belonging to the government unit, not to employees assigned to those tasks, to facilitate account recovery in case of loss.

Second: Password Characteristics

Protecting passwords and email is a fundamental part of protecting unit accounts on social media sites. The unit must observe the following:

- Use different and strong passwords for each email - the user who opens - and social media accounts, and it is prohibited to reuse the same password on any other electronic accounts or sites. The unit must set an internal policy that defines standards for creating and using passwords, and as an example for those standards:
 1. Create a password that is not less than 12 characters.
 2. Use a mixture of uppercase and lowercase letters, numbers, and symbols, such as (Da\$2yN^%gtu1^).
 3. Commit to changing the password periodically (monthly).
 4. Do not save or store passwords on devices used to manage accounts.

Page 8	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
-----------	-------------------------	-----------	---	---



5. Enter a phone number and an additional email, and know some details such as the creation date of the account, the last login date, the last used password, and the answers to the security questions that were set when creating the account, as these details will be used later to recover the account if you are unable to log in to it.
6. Do not use personal information in the account password, such as phone numbers, dates of birth, institution name, employee names, etc.

Third: Activating Additional Security Features in Some Social Media Sites

There is a wide range of social media programs that provide additional protection features, and activating them is of utmost importance to increase the level of protection related to user accounts and the institution. Below we review the activation of two-factor authentication, which is a mandatory feature:

- **Facebook:**
 1. Activate Login Alerts and Two-Factor Authentication: https://ar-ar.facebook.com/help/909243165853369?helpref=about_content
 2. Log out remotely (log out of Facebook): https://ar-ar.facebook.com/help/211990645501187?helpref=faq_content
 3. Avoid Spam and Scams: https://ar-ar.facebook.com/help/1584206335211143/?helpref=hc_fnav
- **X:**
 - Activate login verification: <https://support.twitter.com/articles/20171414>
- **Instagram:**
 - Activate Two-Factor Authentication: <https://help.instagram.com/566810106808145>
- **YouTube:**
 - Activate Two-Step Verification for Gmail account: <https://support.google.com/accounts/answer/185839?hl=en>
- **Snapchat:**
 - Activate Two-Factor Authentication: <https://support.snapchat.com/en-US/article/enable-login-verification>

Fourth: Standards for Interaction with Beneficiaries from Unit Accounts on Social Media

The unit must not respond to any threat or attempt at extortion and immediately communicate with the relevant authorities in case of any such incident. It is also prohibited to comment, interact, or publish anything that explicitly or implicitly contains:

Page 9	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
-----------	-------------------------	-----------	---	---



- Insulting religious or sectarian beliefs or abusing them.
- Defamation, slander, or discrimination.
- Dealing with or publishing false and unreliable information.
- Participating in or commenting on anything that incites or supports illegal activities.
- Comments and shares that violate any intellectual property rights or legal rights.

Fifth: Official Account Verification

The account verification service allows identifying original accounts that represent the concerned entities with legal personality. The unit must adhere to the following requirements when verifying its account:

- The unit's profile must reflect the unit's role and field of work.
- The unit's profile picture must express its activity or logo.
- Ensure that the account username matches the channel or unit name.
- Provide general detailed information about the unit that matches the description on the unit's electronic website. This applies to all public information such as contact numbers, email addresses, working hours, etc.
- Do not use programs to increase followers, as they conflict with verification standards and transparency.
- Update and verify the account profile well before requesting verification, because changing this information later may lead to the cancellation of verification.

How to Verify Accounts:

- 3 To verify an X account, follow the steps on the official website:
<https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts>
- 4 To verify a Facebook account, follow the steps on the official website:
https://www.facebook.com/help/www/196050490547892?helpref=platform_switcher&ref=platform_switcher
- 5 To verify an Instagram account, follow the steps on the official website:
<https://help.instagram.com/854227311295302>

Page 10	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
------------	-------------------------	-----------	---	---



Sixth: In Case of Compromise of One of the Unit's Accounts

In case one of its official accounts on social media is compromised, the unit must take the following measures:

- 6 Immediately notify the concerned authorities.
- 7 Immediately change the password and recover the account.
- 8 Take the following measures to limit and stop the hacking process:
 - Delete any post sent without knowledge.
 - Alert followers about the hacking and deny anything that may have been published through the account, if found.
 - Delete third-party application permissions, if found.

Seventh: Procedures for Recovering Accounts on Some Social Media Sites

The unit must follow the following steps to recover its accounts on social media through the attached links:

- **To recover a Facebook account:** <https://ar-ar.facebook.com/help/117450615006715>
- **To recover an X account:** <https://help.twitter.com/ar/safety-and-security/twitter-account-hacked>
- **To recover an Instagram account:** <https://help.instagram.com/149494825257596>
- **In case of compromise of any Google account or its related services, try to recover the account via:** <https://support.google.com/accounts/answer/6294825?hl=ar>
- **To recover a Snapchat account:** <https://support.snapchat.com/en-US/a/reset-password>

Eighth: In Case Account Recovery Fails

If account recovery fails through the methods mentioned above, the unit must take a final measure, which is direct communication with the official website and reporting the matter.

- **Facebook:** If your institution has been hacked or targeted by a phishing attack, send a report to a Facebook representative, explaining the case. https://ar-ar.facebook.com/help/1216349518398524/?helpref=hc_fnav
- **X:** If your institution has been hacked or targeted by a phishing attack, contact X via the following form: <https://help.twitter.com/ar/forms/account-access>

Page 11	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
------------	-------------------------	-----------	---	---



- **Instagram:** If an Instagram account is compromised, the steps below explain how to recover it. <https://help.instagram.com/149494825257596>
- **YouTube:** If any Google account or its related services are compromised, the steps below explain how to recover it:
<https://support.google.com/youtube/answer/76187?hl=ar&sjid=6782854619008142946-EU>
- **Snapchat:** If the account is compromised, the steps below explain how to recover it:
<https://www.followchain.org/snapchat-account-compromised/#:~:text=How%20to%20fix%20Snapchat%20account%20compromised%201%201.,Send%20the%20form%20%26%20wait%20for%20Snapchat%E2%80%99s%20response>

Ninth: Related Publications

- Security Design Framework for Government Electronic Services and Applications (Circular 2/2016).
- Security Settings and Design Framework for Smart Devices and Peripheral Devices (Circular 3/2017).

Page 12	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
------------	-------------------------	-----------	---	---



Annex (1)

Audit Checklist

Task	Status	Notes	Date
Management Tasks in the Unit:			
1. Use a dedicated device for social media accounts related to the unit, and prohibit its use for any other purposes.			
2. Employee's awareness of the risks related to social engineering, potential fraud methods, and how to counter them and avoid falling into related security errors.			
3. Employee's commitment not to use official accounts for personal purposes that do not serve the unit's objectives and directions in any way.			
4. Employee's commitment not to use personal accounts for communicating with the public in everything related to the unit's affairs.			
5. An official mechanism for publishing on social media is in place and approved by the unit, in compliance with circulars issued in this regard.			
Information Technology Team Tasks:			
1. Open accounts using the official email of the unit.			
2. Activate automatic screen/device lock after a few seconds of inactivity.			
3. Do not install any other applications on the device or use the Internet or email for purposes unrelated to the unit's interaction with social media accounts.			
4. Download the social media service application from the official app store (such as Google Play or Apple Store).			
5. Ensure that the device does not contain any unknown programs or any programs downloaded from outside the official stores.			
6. Activate the tracking and automatic locking feature for the device via satellites in case of theft or loss.			

Page 13	Issue Date July 2024	copy 2	Security guidelines for using social media	Ministry of Transport, Communications and Information Technology
------------	-------------------------	-----------	---	---



7. Prohibit access to unnecessary applications and functions on devices, or downloading and installing games and other applications prevalent in some social media programs.			
8. Do not download and delete any third-party application (such as applications that contain additional features beyond the official applications), or suspicious or unofficial applications.			
9. Do not allow and cancel any other application to synchronize with social media programs or allow it to use the permissions of official programs.			
10. Disable the location identification feature in applications.			
11. Activate login alerts for all applications and programs.			
12. Activate additional security features, Two-Factor Authentication.			
13. Ensure that a phone number and an additional email are entered for account recovery purposes.			
14. Ensure that the answers to the security questions set when creating the account are known.			
15. User awareness of risks.			
16. Ensure the existence of a log that includes some details such as the account creation date, last login date, and last used password.			
17. Set an internal policy to define standards for creating and using passwords.			
User Tasks:			
1. Commit to using a trusted network for connection and refrain from using public and free networks.			
2. Commit to updating the operating system, browser, and social media applications with the latest versions regularly.			
3. Update anti-virus and anti-malware programs regularly.			
4. Refrain from using Proxy or VPN programs for Internet connection.			



5. Avoid accessing unknown links that are sent via email or appear on Internet pages.			
6. Do not open files or open links from suspicious or unknown sources.			
7. Password not less than 12 characters.			
8. Password contains a mixture of uppercase and lowercase letters, numbers, and symbols.			
9. Password does not contain sequential letters like "abcd1234" or keyboard sequences like "asdfghjkl".			
10. Commit to changing the password periodically (monthly).			
11. Personal profile reflects the personal/unit role and field of work.			
12. Personal profile picture expresses its activity or logo.			
13. Detailed general information about the unit is available that matches the description on the unit's electronic website. This applies to all public information such as contact numbers, email messages, working hours, etc.			
14. Refrain from changing the profile picture, information, contact details, and general site information, as this may cancel account verification without mentioning any clear reason! Therefore, the personal profile must be updated and verified well before requesting verification, because changing this information later may lead to the cancellation of verification.			
15. Ensure the existence of a log that includes some details such as the account creation date, last login date, and last used password.			