This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert organization logo by clicking on the placeholder to the left.

Social Media Security Standard Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press "Ctrl" + "H" keys simultaneously
- Enter "<organization name>" in the Find text box
- Enter your organization's full name in the "Replace" text box
- Click "More", and make sure "Match case" is ticked
- Click "Replace All"
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This standard aims to define how <organization name> must ensure social media security in terms of setting up, running, publishing content at, and monitoring of <organization name>'s social media accounts on social media platforms. The ability of <organization name> to use social media in accordance with this standard will assist in preserving the availability, integrity and confidentiality of <organization name>'s data and information.

The requirements in this standard are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to ECC-1:2018, CSCC-1:2019 and OSMACC-1:2021, in addition to other related cybersecurity legal and regulatory requirements.

Scope

This standard covers all <organization name>'s information technology assets and applies to all personnel (employees and contractors) in <organization name>.

Standards

1	Asset Management
Objective	To ensure that the <organization name> has an accurate and detailed inventory of information and technology assets related to social media in order to support the <organization name>'s cybersecurity and operational requirements to maintain the confidentiality, integrity and availability of information and technology assets.
Risk Implication	If <organization name>'s inventory on information and technology assets related to social media is not properly managed, this can result in lack of control over social media usage, confidentiality breaches and data leaks.

Requirements	
1-1	<organization name>'s social media accounts, and information and technology assets related to them, must be identified and inventoried. The inventory must be updated at least once a year.
1-2	Once a new <organization name>'s social media account is created, it must be added to the inventory.
1-3	If <organization name>'s social media account is deleted, it must be accordingly marked in the inventory.
2	Identity and Access Management
Objective	To ensure the secure and restricted logical access to <organization name>'s information and technology assets in order to prevent unauthorized access and allow only authorized access for users which are necessary to accomplish assigned tasks related to social media.
Risk Implication	If access to <organization name>'s information and technology assets related to social media is not properly managed, this can result in credential exposure, unauthorized access and serious reputational damage.
Requirements	
2-1	When setting up the account, only social media accounts designated for organizations, not individuals must be used. If possible, official <organization name>'s social media accounts must be verified and marked accordingly by social Media providers.
2-2	Registration for social media must be performed only by using official information (official specific social media email and official mobile number), and not personal information.

2-3	Email addresses published publicly for contact purposes on official <organization name>'s social media accounts must be generic and nonspecific rather than resembling organizational email addresses of the <organization name>'s personnel.
2-4	Different email addresses must be used for each official <organization name>'s social media account.
2-5	<organization name>'s social media accounts must be verified whenever possible and a consistent identity across all <organization name>'s social media accounts used must be maintained; to facilitate knowledge of official accounts, and to discover fraud or unofficial accounts.
2-6	Only secure, specific and unique password for each <organization name>'s social media account must be used. The password must be changed regularly, and the use of passwords must not be repeated.
2-7	Passwords must not be copied or shared under any circumstances neither outside nor within of <organization name>.
2-8	Multi-factor authentication must be used for <organization name>'s social media accounts logins.
2-9	If possible, Single Sign-On (SSO) must be implemented for all official <organization name>'s social media accounts.
2-10	Security questions must be activated, regularly updated and documented in a safe place.
2-11	<organization name>'s social media accounts access rights must be managed based on business need, considering the sensitivity of the accounts, the level of access rights and the type of devices and systems used.

2-12	Access to official <organization name>'s social media accounts must be available for authorized personnel only, upon request and verification.
2-13	If possible, access to each official <organization name>'s social media account must be granted to at least two authorized people.
2-14	If possible, relevant roles must be set for people with access to official <organization name>'s social media accounts, determining their management rights and permissions in terms of account operating.
2-15	Access rights of service providers of social media management, social media monitoring or brand protection must be restricted to minimum.
2-16	Access to <organization name>'s social media accounts must be restricted to specific devices.
2-17	User identities and access rights used for <organization name>'s social media accounts must be reviewed at least once a year.
2-18	Personnel must be informed that accessing official <organization name>'s social media accounts must be performed only when necessary and the personnel must sign off once the official <organization name>'s social media account is not used by them.
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 related to social media.
Risk Implication	If <organization name>'s information systems and information processing facilities are not properly protected against cyber

	risks related to social media, this can result in cyber-attacks, data leakage and data loss.
Requirements	
3-1	Applications for social media must be downloaded and installed only from known and trusted sources.
3-2	Updates and security patches for social media applications used in <organization name> must be applied at least once a month (if available).
3-3	Reviews and hardening of configurations of <organization name>'s social media accounts and technology assets related to them must be performed at least once a year.
3-4	Reviews and hardening of default configurations, such as default passwords, pre-login, and lockout, for <organization name>'s social media accounts and technology assets related to them must be performed at least once a year.
3-5	Restriction of 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 must be ensured.
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 name>'s information (including sensitive information) while utilizing Bring Your Own Device (BYOD) policy.
Risk Implication	If mobile devices are not properly protected against cyber risks and adequately managed, this can result in confidentiality breach and unauthorized access.
Requirements	

4-1	Mobile devices for <organization name>'s social media accounts must be managed centrally using a Mobile Device Management system (MDM).
4-2	Updates and security patches on mobile devices used for <organization name>'s social media presence must be applied at least once a month (if available).
4-3	Mobile devices used for <organization name>'s social media presence must be adequately protected using either password or biometrics.
4-4	Accessing official <organization name>'s social media accounts must be performed only from a device compliant with <organization name>'s related policies.
4-5	Accessing official <organization name>'s social media accounts must be performed only from a trusted network.
4-6	Official <organization name>'s social media accounts must be accessed only using secure sessions (HTTPS).
4-7	In case a mobile device used for <organization name>'s social media presence is lost or damaged, this event must be timely reported in order to implement relevant corrective measures.
5	**Data and Information Protection**
Objective	To ensure the confidentiality, integrity and availability of <organization name>'s data and information as per organizational policies and procedures, and related laws and regulations.
Risk Implication	If <organization name>'s data and information is not properly protected and privacy settings are misconfigured, this can result in confidentiality breach, reputational damage and legal implications.

Requirements	
5-1	Technology assets for management of <organization name>'s social media accounts must not contain classified data, per relevant regulations.
5-2	Before setting up and using the official <organization name>'s social media accounts, relevant privacy policies and rules of social media providers must be read, understood and accepted. If these privacy policies and rules are not acceptable by <organization name>, relevant risks must be assessed and then either accepted or relevant official <organization name> social media accounts must not be created.
5-3	Privacy policies and rules of social media providers must be read, understood and accepted upon any changes during usage of the official <organization name>'s social media accounts. If these privacy policies and rules are no longer acceptable by <organization name> after introduced changes, relevant risks must be assessed and then either accepted or relevant official <organization name>'s social media accounts must be deleted.
5-4	Official <organization name>'s social media accounts default privacy settings must be reviewed and adjusted to balance between the purpose of the account and the <organization name>'s internal privacy requirements.
5-5	Geo-location feature must be disabled for official <organization name>'s social media accounts and not be added to published content.
5-6	Sensitive information, in particular: ● <organization name>'s confidential information ● personal data

	must not be disclosed without approval in social media under any circumstances. Such information may be published only, if necessary, upon written approval, and by authorized personnel of <organization name>.
5-7	Only validated and reviewed information or announcements must be published using official <organization name>'s social media accounts.
5-8	All images, photos and files published using official <organization name>'s social media accounts must be either with rights owned by <organization name> or copyright free.
5-9	Any content reposted or forwarded via the official <organization name>'s social media accounts must be from known and trusted sources.
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 name>'s operations.
Risk Implication	If collection of logs and monitoring of events related to social media is not properly managed, this can result in vulnerability to cyber-attacks and reputational damage.
Requirements	
6-1	All notifications and cybersecurity alerts for <organization name>'s social media accounts and cybersecurity events logs on related technology assets must be activated.
6-2	<organization name>'s social media accounts must be followed and monitored to ensure that they do not post any unauthorized content, or login any unauthorized access. Each

	official <organization name>'s social media account must be monitored, even if currently unused.
6-3	Social media networks must be monitored to ensure the <organization name> is not being impersonated.
6-4	Usage of official <organization name>'s social media account must be monitored in terms of permission rights granted to various applications.
6-5	Content published using official <organization name>'s social media accounts must be regularly monitored and reviewed to check whether it is aligned with internal requirements.
6-6	Destination of outgoing communication from official <organization name>'s social media accounts must be regularly monitored.
6-7	Social media must be regularly scanned for <organization name>'s secrets, confidential information and unapproved use of branding.
6-8	Automated monitoring for any change in the accounts pattern, indicators of compromise, or the publication of any unauthorized content or impersonation of the <organization name> must be performed.
6-9	Social media monitoring must be configured in a way that enables integration with <organization name>'s brand monitoring and protection services (if provided within <organization name>).
7	Cybersecurity Incident and Threat Management
Objective	To ensure timely identification, detection, effective management and handling of cybersecurity incidents and threats related to social media to prevent or minimize negative impacts on <organization name>'s operation.

Risk Implication	If <organization name>'s inventory on information and technology assets related to social media is not properly managed, this could lead to negative effects.
Requirements	
7-1	A plan to recover the <organization name>'s social media accounts and to deal with cyber incidents must be developed.
7-2	Any incident regarding official <organization name>'s social media accounts, especially: ● Social media deception ● Brand impersonation ● Confidential information leaks ● Credentials theft must be handled according to the <organization name>'s Incident Response plans and procedures.
7-3	Personnel with access to official <organization name>'s social media accounts must be aware of how to report suspicious or unusual events and incidents related to social media presence, so they would be adequately handled.
8	Third-Party Cybersecurity
Objective	To ensure the protection of assets against the cybersecurity risks related to third parties including outsourcing and managed services in social media area as per organizational policies and procedures, and related laws and regulations.
Risk Implication	If <organization name>'s assets are not properly protected against the risks related to third parties in social media, this can result in unauthorized access, data loss or leakage, reputational damage and financial losses.
Requirements	

8-1	A need assessment for the use of social media management, automated monitoring or brand protection services along with associated cybersecurity risks must be conducted.
8-2	Non-disclosure clauses and secure removal of <organization name>'s data by the third-party upon service termination must be ensured.
8-3	Communication procedures to report vulnerabilities and cyber incidents related to social media are established and implemented.
8-4	Requirements for the third-party to comply with cybersecurity requirements and policies to protect <organization name>'s social media accounts, and related laws and regulation are followed.

Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>
2- **Standard Review and Update:** <cybersecurity function>
3- **Standard Implementation and Execution:** <information technology function>
4- **Standard Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the standard at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.

2- All personnel at <organization name> must comply with this standard.

3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.