Digital Policy Office

INFORMATION SECURITY

Practice Guide

for

Social Media Security

Version 1.2

July 2024

COPYRIGHT NOTICE

Amendment History

Change Number	Revision Description	Pages Affected	Revision Number	Date
1	Security risks and considerations related to personal data protection were included; Security tips for common social media platforms were updated.	7; 14-19; 22	1.1	June 2021
2	Change “Office of the Government Chief Information Officer” (or “OGCIO”) to “Digital Policy Office” (or “DPO”)		1.2	July 2024

Table of Contents

1. Introduction

Social media is gaining popularity for both personal and business use. Proper use of social media can improve public image and becomes an effective promotion tool. On the other hand, there are many security risks associated with the use of social media. Bureaux and Departments (B/Ds) should exercise care, evaluate risks and apply proper protection when using social media as official tools for communication with the public.

1.1 Purpose

The purpose of this document is to provide common security considerations and best practices to B/Ds on the management and use of social media. The best practices on the use and management of social media are described in **Section 4**. Social media is one kind of Internet-based applications that requires proper use of Internet in order to safeguard the security of IT environment. For the consideration of Internet security, please refer to **Annex B**.

This document should be used in conjunction with established government requirements and documents including the Baseline IT Security Policy [S17], the IT Security Guidelines [G3] and other relevant procedures and guidelines, where applicable.

1.2 Normative References

The following referenced documents are indispensable for the application of this document.

- Baseline IT Security Policy [S17], the Government of Hong Kong Special Administrative Region
- IT Security Guidelines [G3], the Government of Hong Kong Special Administrative Region
- Information technology – Security techniques – Information security management systems – Requirements (second edition), ISO/IEC 27001:2013
- Information technology – Security techniques – Code of practice for information security controls (second edition), ISO/IEC 27002:2013

1.3 Terms and Convention

For the purposes of this document, the terms and convention given in S17, G3, and the following apply.

Abbreviation and Terms	
NA	NA

1.4 Contact

This document is produced and maintained by the Digital Policy Office (DPO). For comments or suggestions, please send to:

Email: it_security@digitalpolicy.gov.hk

Lotus Notes mail: IT Security Team/DPO/HKSARG@DPO

CMMP mail: IT Security Team/DPO

2. Information Security Management

Information security is about the planning, implementation and continuous enhancement of security controls and measures to protect the confidentiality, integrity and availability of information assets, whether in storage, processing, or transmission and its associated information systems. Information security management is a set of principles relating to the functions of planning, organising, directing, controlling, and the application of these principles in harnessing physical, financial, human and informational resources efficiently and effectively to assure the safety of information assets and information systems.

Information security management involves a series of activities that require continuous monitoring and control. These activities include but not limited to the following functional areas:

- Security Management Framework and the Organisation;
- Governance, Risk Management, and Compliance;
- Security Operations;
- Security Event and Incident Management;
- Awareness Training and Capability Building; and
- Situational Awareness and Information Sharing.

Security Management Framework and Organisation

B/Ds shall establish and enforce departmental information security policies, standards, guidelines and procedures in accordance with the business needs and the government security requirements.

B/Ds shall also define the organisation structure on information security and provide clear definitions and proper assignment of security accountability and responsibility to involved parties.

Governance, Risk Management and Compliance

B/Ds shall adopt a risk-based approach to identify, prioritise and address the security risks of information systems in a consistent and effective manner.

B/Ds shall perform security risk assessments for information systems and production applications periodically and when necessary so as to identify risks and consequences associated with vulnerabilities, and to provide a basis to establish a cost-effective security program and implement appropriate security protection and safeguards.

B/Ds shall also perform security audit on information systems regularly to ensure that current security measures comply with departmental information security policies, standards, and other contractual or legal requirements.

Security Operations

To protect information assets and information systems, B/Ds should implement comprehensive security measures based on their business needs, covering different technological areas in their business, and adopt the principle of "Prevent, Detect, Respond and Recover" in their daily operations.

- Preventive measures avoid or deter the occurrence of an undesirable event;
- Detective measures identify the occurrence of an undesirable event;
- Response measures refer to coordinated actions to contain damage when an undesirable event or incident occurs; and
- Recovery measures are for restoring the confidentiality, integrity and availability of information systems to their expected state.

Security Event and Incident Management

In reality, security incidents might still occur due to unforeseeable, disruptive events. In cases where security events compromise business continuity or give rise to risk of data security, B/Ds shall activate their standing incident management plan to identifying, managing, recording, and analysing security threats, attacks, or incidents in real-time. B/Ds should also prepare to communicate appropriately with relevant parties by sharing information on response for security risks to subdue distrust or unnecessary speculation. When developing an incident management plan, B/Ds should plan and prepare the right resources as well as develop the procedures to address necessary follow-up investigations.

Awareness Training and Capability Building

As information security is everyone's business, B/Ds should continuously promote information security awareness throughout the organisations and arrange training and education to ensure that all related parties understand the risks, observe the security regulations and requirements, and conform to security best practices.

Situational Awareness and Information Sharing

As cyber threat landscape is constantly changing, B/Ds should also constantly attend to current vulnerabilities information, threat alerts, and important notices disseminated by the security industry and the GovCERT.HK. The security alerts on impending and actual threats should be disseminated to and shared with those responsible colleagues within B/Ds so that timely mitigation measures could be taken.

B/Ds could make use of threat intelligence platforms to receive and share information regarding security issues, vulnerabilities, and cyber threat intelligence.

3. Overview of Social Media

3.1 Introduction to Social Media

Social Media is the interaction with platforms where participants contribute content and communicate with each other. It has gained enormous popularity in recent years. Initially, the users of social media platforms, such as Facebook, Instagram and YouTube, build networks of friends with shared interests. Nowadays, it is not merely for personal sharing, but also for commercial or government as communication channels for interacting and collaborating with the public or its target audience so as to solicit or monitor opinions and views. However, in the aspect of cyber security, this may give rise to certain associated risks.

Within the Government, the decision in engaging social media should be driven by business cases and supported by management. The scope, threats, technical capabilities and potential benefits should be considered. In order to defend against the rapidly evolving social media threats, there should be a risk management programme to assess and mitigate the risks to an acceptable level. Mitigation measures, based on a defence-in-depth approach[1], should be considered in protecting the participants, the platform and services, and government staff and data.

3.2 Common Social Media Category

With the growing popularity and power of social media, users enjoy the benefit of different networking brought by the social media platforms. Below are the common social media categories which are widely used by the users.

Social Networks

- Social networks allow users to connect with people and the brands online. These platforms encourage knowledge-sharing and enable human-to-human interaction.

Media Sharing Platforms

- Media sharing platforms allow users to share a wide range of visual content like videos, images, infographics, and illustrations. Unlike social networks, these platforms are focused solely on sharing visuals and are optimised to help creators upload their visual content and interact with other viewers.

[1] Defence in Depth (DiD) is an approach in which a series of protection measures and controls are layered in order to protect information systems and data assets

Discussion Forums and Social Community

- Discussion forums and social community are the online discussion sites where people can hold conversations in the form of posted messages for collective knowledge. Users can be anonymous or register a username in the forums and then subsequently log in to post messages.

Blogging Networks

- Blogging networks allow users and companies to publish content online and help increase visibility from viewers to discover the published content. This type of social media is often used to build engagement and get people familiar with the owner of the blog.

4. Social Media Security Risk and Threats

A risk management programme should be in place for B/Ds to understand the threats and evaluate the risks to the social media participants, the platform and service, as well as B/Ds (i.e. subscriber) and the involved data.

- Participants: General public users such as citizens who participate in the social media platform.
- Social media platform and service: Web media platforms that allow the Government and the general public to have communication, collaboration, interaction and information sharing.
- B/Ds: Subscriber of social media services from commercial or public service providers.

4.1 Threats to Social Media Participants

There are threats associated with members of the public that participate (e.g. citizens posting messages on a discussion forum) in social media platform. Security threats in relation to social media platform may include privacy threats, loss of login credentials, malicious content and code, social engineering attacks, etc. The information leaves a perpetual digital footprint that is difficult to eradicate from the online world, and may provide materials for identity thefts.

Privacy Threats

Social media, such as discussion forums and blogs, allows participants to post information or content to the public. These forms of communication may bring privacy issues by placing too much personal information. It allows profiles to be produced based on individual's behaviour on which detrimental decisions may be taken. If the participants posted too much personal information on social media platforms, it could lead to potentially unfavourable situation for the participants.

Stolen or Lost Login Credentials

If the password is not well selected or properly protected, malicious people may find ways to steal the password. After unauthorised logging to the user accounts, fraudulent messages may be posted or the account may be used to spread malicious software.

Malicious Content, Code and Phishing Links

Social media is growing in popularity as one of the attack vectors because of the number of users and the amount of personal information that is posted. Attackers may make use of this channel to spread malicious content, code or phishing links. If a social media site has security vulnerabilities, attackers are able to create customised applications that appear to be legitimate and infect the users' computers without their knowledge.

Social Engineering Attacks

Social media builds online communities of people with a certain level of interpersonal trust. Malicious people might impersonate a trusted person of the users and then convince them to disclose sensitive information. In addition, attacks like viruses, trojans or rumours can be spread easily and rapidly when some social engineering skills are used.

4.2 Threats to Social Media Platform and Services

There are threats associated with the social media platform and services, such as a discussion forum, blog and instant messaging provided by a service provider. For the impact of threats, the normal operation of the platform may be disturbed, the services may be interrupted, and the data may be unauthorised accessed and disclosed.

The following are common threats that are particularly against social media platform and services:

Buffer Overflow

Buffer overflow is probably a well-known form of software security vulnerability. In a classic buffer overflow exploit, the attacker sends data to a program, which it stores in an undersized stack buffer. The result is that information on the call stack is overwritten, including the function's return pointer. The data sets the value of the return pointer so that when the function returns, it transfers control to malicious code contained in the attacker's data.

Remote Code Execution Vulnerability

Vulnerabilities are exploited by an attacker to execute malicious code and take complete control of an affected platform/system with the privileges of the user running the application. After gaining access to the platform/system, attackers will often attempt to elevate their privileges.

Spamming and Flooding

Spamming is a common attack targeted at social media websites to spread spam. It abuses the use of electronic messaging systems by sending unsolicited bulk messages indiscriminately. Forum spamming is the type of message that is either abusive, marketing gimmicks or useless information. Spamming can happen as often as possible, especially when the forum is left un-moderated. It could take place in just a couple of hours, or even minutes and may even bring the forum server out of service because of the message flooding. This will consume the information system resources and has a negative impact on the service level to other normal services. More importantly, participants may find the social media platform filled with useless information and lose interest in participating in any further discussions.

Web Application Attacks

Web applications are dynamic web pages that use scripting to provide additional functionalities to the participants. However, these additional functionalities may mean more opportunities to exploit the web application. This opens up social media websites to a wide range of vulnerabilities exploitable by attackers. There could be attacks through keystrokes logger to capture user keystrokes, including account usernames and passwords. While a personal social media account being hijacked may be annoying and personally costly or embarrassing, the hijacking of a government official account may have more serious implications. Unofficial posts or messages may be seen by the public as official messages or may be used to spread malicious software by encouraging users to click links or download unwanted applications.

Below are some common examples of web application attacks:

- Broken Authentication
  Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys or session tokens, or to exploit other implementation flaws to impersonate other users' identities temporarily or permanently.

- Broken Access Control
  Access control refers to a system that controls access to information or functionality. Broken access controls allow attackers to bypass authorisation and perform tasks as though they were privileged users such as administrators. For example, a web application could allow a user to change which account they are logged in as simply by changing part of Uniform Resource Locator (URL), without any other verification.

- Sensitive Data Exposure
  Many web applications and application programming interfaces (APIs) do not properly protect sensitive data, such as financial, healthcare, and personally identifiable information (PII). Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

- Cross Site Scripting (XSS)
  Cross site scripting is a type of web application attack in which the end user's web browser is induced to execute malicious code. The end user's personal information may be stolen by the malicious code, which enables the attacker to impersonate the end user, or manipulate the end user's computer to launch an attack against a third party without either the victim's or the third party's knowledge.

- Cross Site Request Forgery (CSRF)
  Cross site request forgery is a type of web application attack which causes an end user's web browser to execute actions of the attacker's choosing without the user's knowledge. By embedding a malicious link in a web page or sending a link via email or chat, an attacker may cause the users of a web application to perform unwanted actions. More specifically, the attacker causes the user's browser to make requests to a web site to which it has been authenticated, without the user's or the web site's knowledge. These actions may result in compromised end user data and operations, or even an entire server or network.

- Injection Flaws
  The technologies that social media uses make it vulnerable to injection attacks such as Extensible Markup Language (XML) and Structured Query Language (SQL) injection. Additionally, social media applications often rely on client side code, so they rely heavily on client side input validation which an attacker can bypass.

Inappropriate or Offensive Content

Inappropriate or offensive content may be posted or uploaded by participants on social networking websites. Inappropriate or offensive content may include material without copyright authorisation, contents exceed the generally accepted norms or limits of decent taste and ethics, instructions in cyber attack or drug use, etc. The posting of such material could affect the image of the Government. The ultimate responsibility of holding such content that may be illegal is another concern.

Unauthorised Content Variation or Service Disruption

Online vandalism involves the acts of damage or destruction to an online asset that may affect the image as well as reputation of the Government. The act can range from web defacement to disruption of service.

Phishing

Phishing is an effective attack targeting a specific user or user group to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link. Phishers rely on knowing the target's personal information such as interest, travel plans, social circle etc. Most of the time, personal information is collected by just looking up on social media. Phishers utilise social media as an alternative way to send phishing messages, as the social media platform bypasses traditional email security controls. The links that are posted on the social media by phishers may look identical to a legitimate site with only a tiny variation in spelling or a different domain to trick users.

Availability and Performance

There may be out of service situation due to hardware or software problems, or the system may reach its capacity limit leading to degraded performance. If disaster events occur, the service may be totally unavailable and business continuity will be affected. Also, the service provider (or its subcontractors) may go out of business or may hold the data hostage in case of disputes. The trustworthiness, reliability and capability of the service provider (and its subcontractors) are important for ensuring the continuation of the social media service.

4.3 Threats to B/Ds and Data

The service provision of a social media platform on these sites will have the advantage of easily reaching out to a mass population of participants. For this reason, public social media platforms are often deployed for the purpose of social media. Regardless of whether the deployment is on in-house infrastructure or by outsourcing to a service provider, there will be concerns in the threats to the government staff and data.

The following are common threats that are particularly against the government staff and data:

Disclosure of Internal / Classified Information

Sensitive or classified information may be disclosed intentionally or unintentionally and bring discredit on or embarrass the Government.

Data Retention and Destruction

Various reasons may cause the termination of the collaboration between B/D and a service provider such as technology changes, popularity, reaching the end of the contract term and not be renewable. Under such circumstances, there may be a data loss risk that B/D is unable to retrieve all the data from the social media platform. On the other hand, the service provider may not have proper procedures for the disposal of the government data.

Data Misuse

Social media providers may not be fully protecting the privacy of subscribers or participants, so as to ensure that the data is not used for other purposes and not disclosed to third parties. Service providers may gather registration information of participants for their marketing purposes which to an extent could become a nuisance to participants.

Limited Control on Services and Data

Under the subscription agreement of the social media services, data is typically stored and processed under cloud based environment. There will probably a limited control over the platform or even the government data within that environment. For example, you may not be able to request an image backup of the full hard disk since it will contain data from other subscribers.

Lack of Awareness

Lack of awareness could lead to various degrees of security vulnerabilities. Social engineering attacks may target at government staff, where responsible officer such as administrator may be tricked into giving away identity information. In addition, staff may post internal or classified information on social media that would affect the image of the Government.

Impersonation

Impostors often create accounts on social media that resemble those of celebrity, business organisations or government officials. Some impersonating accounts may carry a connotation of deception and bring misleading messages to the public for the information collection or financial gain.

5. Social Media Security Measures and Controls

5.1 Social Media Usage Lifecycle

5.1.1 Provision of Social Media Account

When considering the adoption of social media in the Government, B/Ds should identify the needs for using social media and how social media would support their business. A policy on the acceptable use of social media should be established to specify the business and security requirements for the use of social media service.

5.1.1.1 Setting up Social Media Account

Based on the usage and security requirements, B/Ds should develop adequate processes and procedures for the provision of social media account. In particular, security configurations of social media account should be enforced in accordance with the government security requirements. For sample configurations regarding security hardening, please refer to **Annex A**.

B/Ds should appoint an officer from the senior management to be the head of administrator of social media account and at least two officers to be the administrators of social media account to setup, access and manage the social media account for B/Ds.

The administrators should create, name and form the social media user account which represents the Government or B/D with information approved by the head of administrator. The information includes but not limited to:

- Account description
- Business information
- Contact details (e.g. Email address, Website)
- Address
- Profile photo
- General information

5.1.1.2 Social Media Usage Policies

To regulate the use of social media by administrators and users, a security policy for appropriate use of social media should be formulated. The common security measures and controls of social media platform in different areas include but not limited to:

- General Management
- Account
- Password
- Security Setting
- Posting
- Network and Endpoints
- Awareness

The details of the secure use of social media services are listed in **Section 5.2 Secure Use of Social Media Services** for security consideration.

5.1.1.3 Use of Social Media Analytics

Social media analytics is the process of gathering and analysing data from social media platforms. The collected information includes but not limited to:

- Personal information which is shared on social media platforms (e.g. profile information, content, usage, and third party websites and apps)
- Device information (e.g. device IDs, attributes, operations, signal, network and connections, and cookie data)
- Information from third-party partners and services, including advertisers and app developers (e.g. account information, user setting, and social interaction activities)

B/Ds should refer to the information leaflet on Online Behavioural Tracking published by the Privacy Commissioner for Personal Data (PCPD).

- Online Behavioural Tracking (https://www.pcpd.org.hk/english/resources_centre/publications/files/online_tracking_e.pdf)

Social media analytics tool helps the user understand the audience and how they interact with the posts in the social media pages. It provides the insights, metrics and dashboard about the social media account including but not limited to:

- Number of followers
- Age groups of followers
- Engagement of audience to the posts
- The time and location of followers visit the social media page
- Number of posts on the social media page
- Number of times the content was displayed
- Number of people who access the content
- Number of people interacted with the content (e.g. likes, shares, retweets, replies or mentions)

The administrator of social media account should make use of social media analytics to deliver better service and engage with all sectors of the community.

5.1.2 Decommissioning of Social Media Account

B/Ds should regularly review the usage of Social Media. If the social media account has not been used for more than six months, the administrators should consider deactivating the account. The head of administrator of social media account should escalate this matter to senior management of B/D for approval.

5.2 Secure Use of Social Media Services

In view of the potential threats that may be introduced by using social media, B/Ds should conduct risk assessments to assess the associated risk and estimate the potential impact before subscribing social media services. When B/Ds decide to subscribe to social media service, security measures and controls should be implemented to prevent and mitigate the identified risks to an acceptable level.

5.2.1 Users

Account

- Log out of social media account after use every time, especially when using publicly shared computer or mobile phone that sharing with others.
- Use separate email accounts for registration on a social media platform and your personal communication, whenever feasible.
- Do not use the government email account for registration on any social network sites if participation is not official.
- Avoid auto sign-in social media apps.
- Monitor any anomalous behaviour from the email that links to social media account and ensure the account is not compromised.

- Ascertain whether the social media platform will share user's personal information with third parties, what kinds of data will be shared, and for what purposes.

Password

- Employ a strong password by complying with the departmental password policy. For example, use at least eight characters with a mix of upper and lower case alphabets, numbers and special characters.
- Recommend enabling multi-factor authentication or at least two-factor authentication to add an extra layer of protection.
- Use a unique login name and password for each social media account.
- Change the password of social media accounts regularly.
- Use one-time password (OTP) to log into social media account when using public computers (e.g. in a library or internet cafe).
- Change your password immediately if you suspect anything went wrong in your account.
- Do not share passwords or verification code of social media accounts with others.
- Do not use an easily guessable password or the same password for various social networking sites.

Security Setting

- Perform regular security checking on the current security and privacy settings, user access and user publishing privileges.
- Check login sessions regularly and terminate unrecognised sessions immediately
- Follow any suggested security settings by the provider and configure your privacy settings according to your need.
- Enable two-step verification to enhance the security of the account.
- Enable end-to-end encryption where appropriate.
- Enable to get alerts about unrecognised logins (from an unrecognised computer or mobile device).
- Enable passcode lock on the phone and set up inactivity time with no more than a few minutes.
- Check the settings of applications regularly that you recently used or allowed. Remove applications that you no longer need.
- Check your past posts regularly and delete those you no longer want to share.
- Review the latest privacy policy and assess the associated personal data privacy risks.

Posting

- Think twice before posting personal information that might be trivial at first instance. Although some of this information may seem harmless (e.g. your pet's name), it actually may provide rich pickings for malicious person. Malicious people might be able to gather that information to impersonate you to gain access to your sensitive information.
- Consider how widely your information is being shared before posting (e.g. friends only or everyone).
- Do not post personal information more than needed, such as your address, date of birth, telephone number, and information about your schedule or routine.

- Do not post sensitive information or illegal content on the social media platform.
- Do not send sensitive information over the Internet before verifying a site's validity and security.
- Do not share or forward posts or emails from one social media platform to another as they may have sensitive information about the account.
- Do not use personal social media account to post internal information such as staff IDs, organisation structure, business deals, business plans or business schedule, as well as information about clients or business partners.
- Respect others' privacy, do not share other people's personal information before obtaining their permission.

Network and Endpoints

- Always use a secured connection (including secured Wi-Fi network) to connect to social media platform (either URL or mobile app) to protect login account.
- Apply latest security patches on social media applications.
- Install anti-malware software and latest security patches on endpoints, enable real-time protection and keep the malware definition files up-to-date.
- Enable passcode lock on the phone and set up inactivity time with no more than a few minutes.
- Do not access social media accounts from untrusted devices in public areas.

Awareness

- Be aware of "social engineering" attacks that use manipulation or deception in an attempt to access information.
- Be alert to messages sent by people that they do not know well, and should avoid clicking links coming from people or sources they do not know.
- Be sceptical of strangers and use the block button to stop spammers if necessary.
- Be alert when receiving an invitation from others, verify its safety by checking the information and reviews of it.
- Be mindful of entangling apps and social media / email accounts.
- Be alert about security alerts and news of social media platforms.
- Be cautious of the links that are posted on the social media pages. A malicious website or link may look identical to a legitimate site with only a tiny variation in spelling.
- Follow the best practice in the Section 3 of the "Practice Guide on the Use of Electronic Mail" for using email in official duties. (https://itginfo.ccgo.hksarg/content/imx/email_practice_guide.asp)
- Do not trust everything you read online especially from strangers. People may post false or misleading information even their own identities.
- Do not click on unsolicited links from strangers or sources you do not know. Nevertheless, even you are visiting pages of someone you know, always be cautious when clicking on links or photos, because links, applications or other file formats may include malicious code.
- Do not accept to download and install applications or plug-ins that you do not know well.
- Do not trust someone you have just met online any more than you would trust a stranger encountered on the street.

- Do not run social media mobile app on any rooted Android devices or jailbroken iOS devices.

5.2.2 Administrators

The administrators are required to follow the security measures and controls for general users in **Section 5.2.1** and extra dedicated security measures and controls for administrators to carry out their designated job duties.

The following are security measures and controls for administrators:

General Management

- B/Ds should define the roles and responsibilities of the administrators of social media account, including usage, management and operation.
- B/Ds should appoint at least two officers to be administrators with adopting segregation of duties control.
- Formulate social media usage policies to ensure sensitive data and classified information will not be disclosed. The policies should provide clear guidelines to make participants aware of what information to share, with whom they can share it, and what not to share.
- Establish disciplinary procedures in case of violation of policy.

Account

- Use separate accounts for managing official social media pages and personal social media account, whenever feasible. If the social media platform requires the use of authentic and personal account to be the administrator or editor, B/Ds are advised to identify suitable management tools (e.g. Facebook Business Manager) to have a better account management across pages.
- Deactivate the social media accounts or close the pages that are no longer used or inactive.
- Comply with the regulatory and intellectual property rights.

Password

- Use a unique password for each official social media account.
- Enforce multi-factor authentication whenever feasible.
- Keep password of official social media account solely by the administrator of the social media account and should not share with others.
- Update password and recovery information immediately when designated staff leaves the position of the Government.

Posting

- Establish an approval process for all social media posting across official social media pages.
- Establish and compile content requirements and procedures for posting.
- Establish internal channels and procedures for reporting any misuse or security concern.
- Monitor the posts to the social media pages of social media account regularly.

All posts should be reviewed and approved by the administrators to ensure compliance with the social media policies.

- Remove illegal content and filter comment spam by moderations. The moderation process can be supplemented by the establishment of a mechanism to identify and report the source of cyber attacks (e.g. phishing) and potential technology crimes (e.g. Internet deception).

Network and Endpoints

- Install a firewall and other network security devices at the Internet gateway, and ensure staff's computers have all the latest security patches and are installed with anti-malware software with up-to-date malware definition files to provide an extra layer of defence against cyber-attacks and phishing scams.

Awareness

- Be alert about security alerts and news of social media platforms and inform staff who are using such sites on the related messages.
- Conduct regular awareness training to educate staff about the government security policy and strengthen security awareness around the threats associated.

For the government designated staff using the official social media accounts, the security consideration of posting on the official pages includes but not limited to:

- Comply with the code of conduct in the Government which also applies to online interactions.
- Comply with the code of conduct, policies and terms of service of the social media platforms.
- Perform risk monitoring of potential reputation risk before posting in social media platforms.
- Do not post any classified data, including sensitive staff information and personally identifiable information (PII).
- Do not spread fake news, information, photos and videos in the platforms.
- Do not post any advertisement of products/services or non-publicised government or B/Ds activities.
- Do not post any information, photos or videos that violate privacy ordinance, copyright or intellectual property.
- Do not post any improper or unauthorised use of a trademark, sale or promotion for the sale of counterfeit goods and defamation.
- Do not spread spam, hoax, phishing and scam.
- Do not post information that may affect the neutrality of government staff.
- Do not post any content promoting illegal activities, cyber attack with malicious intentions or sale of certain regulated goods and services (e.g. drugs, online gambling).

For better protection of personal data on social media platforms, B/Ds should observe the following guidelines as developed by the Privacy Commissioner for Personal Data (PCPD).

- Guidance on Protecting Personal Data Privacy in the Use of Social Media and Instant Messaging Apps (https://www.pcpd.org.hk/english/resources_centre/publications/files/social_media_guidance.pdf)

- Privacy Implications for Organisational Use of Social Networks (https://www.pcpd.org.hk/english/resources_centre/publications/files/sn_organisational_e.pdf)
- Protecting Online Privacy – Be Smart on Social Networks (https://www.pcpd.org.hk/english/resources_centre/publications/files/SN2015_e.pdf)

5.3 Breach of Social Media Accounts and Security Incident Handling

Suspicious activities of social media accounts include automated likes, unknown status updates and receiving notifications that the account has been accessed from an unknown location. The security incident handling procedures are required to review with necessary modifications for handling such suspicious symptoms. Users should report promptly and escalate if an information security incident occurs in accordance with the security incident handling procedures.

In particular, B/Ds should consider the following best practices for handling the breach of social media account:

- Temporarily deactivate the social media account.
- Collect and review all logs, artifacts of malicious activity for investigation and possible legal.
- Change account passwords immediately.
- Change the password for the associated emails.
- Verify the password recovery options set for the social media account and alternative email address.
- Verify auto-forward options for the account and associated emails.
- Remove any suspected apps from the applications page of the social media account.
- Report the incident to the Government Information Security Incident Response Office (GIRO) when necessary, such as involving the leakage of classified information.

*** ENDS ***

Annex A - Security Tips for Common Social Media Platforms

The security and privacy controls on different social media platforms may vary and change overtime. Administrators of social medial account should conduct regular review on the relevant controls to ensure the existing security controls meet the requirements of B/Ds. B/Ds should refer to the official advice when developing their security policies.

1. Facebook

Description	URL
Safety Centre	https://www.facebook.com/safety
Basic privacy settings and tools	https://www.facebook.com/help/325807937506242/

2. Twitter

Description	URL
How to protect and unprotect your Tweets	https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public

3. Instagram

Description	URL
Privacy settings and information	https://help.instagram.com/196883487377501

4. YouTube

Description	URL
Privacy and safety	https://support.google.com/youtube/topic/2803240?hl=en&ref_topic=6151248

5. WhatsApp

Description	URL
Security and Privacy FAQ	https://faq.whatsapp.com/general/security-and-privacy/

6. WeChat

Description	URL
Account Security	https://help.wechat.com/cgi-bin/micromsg-bin/oshelpcenter?opcode=2&lang=en&plat=android&id=170417vMBnEB170417InAF36&Channel=helpcenter

7. Telegram

Description	URL
Security	https://telegram.org/faq#security

8. LinkedIn

Description	URL
Account and privacy settings overview	https://www.linkedin.com/help/linkedin/answer/66?lang=en

9. Snapchat

Description	URL
Privacy settings	https://support.snapchat.com/en-GB/a/privacy-settings2

Annex B - Proper Use of Internet

B.1 Introduction

Internet access allows government staff to disseminate information, communicate and conduct business transaction with the public effectively. It could increase productivity and improve communication, however, there are risks associated when government users do not exercise care in accessing Internet. This annex lists some common risks associated with Internet access and provides security measures to be held by users and network administrators.

B.2 Risks Associated with Use of Internet Access

Risks and threats to government are:

a) Data loss or leakage of sensitive information (including classified information and personal data)

Internet access provides a convenient way of data transfer. Without proper data protection control in place, sensitive information may be leaked or accidentally disclosed to unauthorised parties. For example, staff may intentionally send out or post classified information to the Internet.

b) Stolen credential – causing unauthorised access

With a wide range of Internet website or services, there are bogus websites which would try to trick users to input their credentials. If users are not aware of the fake websites and input their credentials, their information may be used for unauthorised access to system.

c) Malicious Content or Malware

As Internet access service allows users to access a wide range of website and services via their departmental workstations or devices, potentially exposing these workstations or devices to malicious content or malware which may in turn infect other workstations or devices in the same network.

d) Social Engineering Attacks (e.g. Phishing)

Hackers or attackers may gather information users posted on Internet, especially social media, and perform targeted attacks, for example, sending fake emails pretending from senior management to gain unauthorised access to information/system.

e) Cyber-stalking

Cyber-stalker may perform stalking on users based on information collected on Internet. There are some cases happened that users were burglarised after they posted personal information (such as holiday photographs) on social media platform.

f) Involving illegal activities

When involving illegal activities (e.g. knowingly accessing malicious websites resulting in DDoS attack, hacking, downloading/hosting pirated software, infecting by ransomware for money, etc.) through government internet services or affecting government data/system, this would affect government reputation or image. Such incident will bring the Government into disrepute and involved staff members may be subjected to punitive actions.

B.3 Guiding Principles for Users

To better protect government assets, B/Ds should provide regular training and reminders to users in proper use of Internet.

All government staff should understand the obligations and responsibilities when using the Internet services provided by the Government, and should follow the terms of usage of the Internet services provided. The Guiding Principles on the Use of Internet Services can be available as follows:

https://itginfo.ccgo.hksarg/content/itsecure/techcorner/practices/Guide_use_of_Internet.htm

B.4 Guiding Principles for Administrators

B/Ds should arrange regular and ad hoc training, with emphasis on the proper use of Internet services, in promoting staff awareness of information security. Besides educating users their responsibilities, B/Ds administrators should also exercise due care and due diligence in protecting government network when providing Internet services to users.

Administrators **shall**:

a) Follow best practices in the Practice Guide for Internet Gateway Security (https://itginfo.ccgo.hksarg/content/itsecure/docs/Guidelines/Current/core/IGS.pdf).
b) Update their departmental IT security policies and guidelines by incorporating the updated Guiding Principles as appropriate.

c) Notify new users and regularly notify all users to observe the Terms of Service for Internet Access Service (IAS) and to secure staff's acknowledgement and acceptance of the terms of service and remind them that each user is accountable to all of his/her activities on the information systems and the consequences of such activities.

d) Perform System Logging of User Activities

   i. maintain the records of the fixed IP addresses assigned to the workstations or devices under their management.

   ii. maintain the list of dynamic assignment of IP addresses to all network devices (or commonly referred as a DHCP list) because Internet Access Service (IAS) system has no such information in identifying the client workstations in B/Ds.

   iii. maintain the activity log of B/Ds' own local proxy servers. B/Ds are encouraged to enable X-Forwarded-For (XFF) header field in such local proxy servers connecting IAS to indicate the IP addresses of client workstations.

   iv. log and review user activities for the following purposes:

   - System diagnosis and trouble-shooting;
   - Capacity planning and service improvement;
   - Identification of IP addresses upon investigation; and
   - Provision of information upon B/Ds' request or as required by law.

e) Retain the Internet access log for at least 6 months.

f) Deploy network level protection at gateway (e.g. gateway to Internet Access Service, Internet gateway).

g) Deploy anti-malware at workstations and devices that would access Internet.

h) Apply security patches to all systems, workstations and devices.

i) Avoid data transfer via unencrypted protocols such as File Transfer Protocol (FTP).