TikTok Policy of Metropolia University of Applied Science

Contents

Administrative information

Title: TikTok Policy of Metropolia University of Applied Science
Version: First edition
Validity date: 8 March, 2024
Owner(s): Roope Rannikko, Information Security Specialist
Approver(s): Kimmo Nikkanen, Chief Information Officer, CIO
Classification: Public
Intended Audience: The university community that possess devices and other information assets provided and contolled by the Metropolia. This documents directs the use of a social media device at Metropolia, where the device is used for publishing content on the TikTok social media service.
Change history:
First edition published on 8 March, 2024.

Definitions

TikTok = A Chinese-owned social media platform/service where users share videos.

Information security = All the arrangements that ensure information's confidentiality, availability and integrity.

Data protection; Privacy protection = Arrangements aimed at ensuring the appropriate processing of personal data and the preservation of their privacy. Personal data protection is sought to be implemented, among other things, through information security.

Confidentiality = no one or an unauthorized agent can't have access to information or data.

Policy = The content of a policy guides actions and decisions concerning the topic of the policy. An organization can have a number of policies; one for each of the activity areas that is important to the organization. Some policies are independent of each other, while other policies have a hierarchical relationship.

Information asset = Any data that has value to the organization and therefore requires protection. Information assets should be identified, taking into account that an information system consists of protected functions, processes, and data.

Social media device = A tool or device used for accessing and communicating on social media platforms. For example, an employee might use a smartphone with the TikTok app installed on their social media device. Employees can request a social media device to himself or herself through user support, which then provides them with the necessary equipment. These devices are used for creating content on platforms like TikTok. While other social media applications can be installed on a social media device, it's essential to follow security guidelines regarding social media usage. It's important to note that a social media device is distinct from an employee's personal phone or work computer, as it is specifically intended for producing social media content.

Information security incident = One or more related unexpected or undesirable security events that jeopardize the security of information and services and negatively impact an organization's operations. Security incidents can arise from various causes, including data breaches.

Personal data breach; privacy violation = An unauthorized or unwanted event related to personal data, resulting in data destruction, loss, alteration, unauthorized disclosure, or access by an entity without proper processing and viewing rights. An information security incident can lead to consequences such as compromised data monitoring, identity theft, fraud, reputational damage, or the exposure of pseudonymized or confidential personal information.

Data breach; security breach = Unauthorized intrusion into a computer system, service, or device, or unwarranted use of an application utilizing acquired credentials. A data breach may involve data beyond personal data or privacy information of a natural person, such as financial data.

Introduction

The TikTok Policy of Metropolia University of Applied Sciences (hereafter referred to as the TikTok policy) instructs the use of the TikTok social media service within the context of the university environment, as well as the device specifically acquired for this purpose (referred to as "a social media device"). This document provides guidelines on how IT Services, the IT department of Metropolia, expects the higher education community to interact with the TikTok application. The use of TikTok on a device provided by the university (also known as the employer) is prohibited. Additionally, the web version of TikTok should not be accessed on institution-managed devices, and logging into the service using an organization-provided email or username is not allowed. To introduce TikTok for a department, school, innovation hub, or individual project, a separate social media device must be acquired by submitting a service request to IT Services. It's important to note that a social media device is distinct from an employee's personal work device or privately owned equipment. Social media devices are always managed by Metropolia. This TikTok policy applies to the entire higher education community that utilizes institution-managed or provided devices. It does not pertain to devices that are not owned by Metropolia, such as privately owned personal devices like mobile phones or computers. Privately owned personal devices may be used as individuals see fit for themselves.

Scope

The TikTok policy applies to the higher education community that has received a device from Metropolia University of Applied Sciences. The policy supports the implementation of Metropolia's information security policy alongside Communication and Marketing's communication principles for reaching the university community. It reinforces the university's brand and promotes a positive influencer role to stakeholders. Additionally, the document guides the use of TikTok on the institution-managed devices for departments, schools, innovation hubs, and single projects. While primarily aimed at Communication and Marketing's TikTok usage, the content can be applied to other actors as needed, providing guidelines for a broader audience. The document includes detailed instructions on using TikTok as well as related role and responsibility matters. Personal devices not owned by the university fall outside the scope of this policy. Individuals may install TikTok on their personally owned devices if desired. However, logging into TikTok with an institution-provided email or username is strictly prohibited. The university's email and usernames are Metropolia's information assets, managed by the institution.

Objectives

The purpose of this document is to prohibit employees from using the TikTok service on devices and platforms connected to Metropolia University of Applied Sciences. TikTok should not be installed on any device managed or given by Metropolia, including employer-provided phones. Additionally, the web version of TikTok should not be used on university's devices, even if accessed through a private email account. Instead, employees should contact IT Services to obtain a separate device, known as "a social media device," and a corresponding user account for communication on social media services like TikTok. This document reinforces employee security and privacy by providing guidelines for consistent practices within the university community. The goal of Communication and Marketing is to increase the visibility of the university on platforms popular among young people, such-as TikTok media, thereby enhancing its appeal to potential applicants.

Principles

By following the TikTok policy, employees ensure the proper implementation of the university's information security policy. The creation of this policy was preceded by a risk assessment conducted by the IT Service regarding the security of the TikTok platform. The document demonstrates appropriate risk management practices within the university. It reinforces confidentiality in information security to prevent university community data from falling into the hands of external parties, including state intelligence services. TikTok, owned by the Chinese company ByteDance, is not considered to align with the university's privacy principles due to suspicions of close ties with the Chinese government. Additionally, Metropolia's "licence to SOME" principles, available at the university's intranet under the Communication and Marketing tab, take center stage within the TikTok policy.

Responsibilities

Detailed responsibilities can be found in Annex 1 of this document. IT Services is responsible for security solutions as outlined in Annex 1. The primary responsibility of Communication and Marketing is to ensure appropriate communication on the TikTok platform. Employees should not install TikTok on devices provided by Metropolia or use their university username or email for the service. Instead, they must make a separate service request to IT Services to start publishing content on TikTok. Before creating a TikTok account, the supervisors of a department, school, innovation hub, or individual project should consult with Communication and Marketing. Employees may only publish information that is suitable for the public audience according to the university's classification policy. When creating TikTok content, employees should follow social media guidelines for communication addressed by IT Services together with Communication and Marketing.

Related policies, compliance, and review

The TikTok policy is reviewed annually by Chief Information Officer and IT security experts, following the information security's annual planning cycle by the university. If the policy requirements are violated, they are treated as IT violations according to the university's disciplinary process. Deviations from the TikTok policy can be made when the IT Management of Metropolia deems it necessary and has obtained the IT management's approval to do so. In such cases, a risk assessment with justifications should be conducted to explain why the TikTok policy does not serve its purpose, which is to guide the use and establishment of TikTok accounts within the university community.

The guidelines that support the TikTok policy are as follows:

- **Metropolia's Information Security Policy**: Guides the university's information security solutions.
- **Regulation for Handling Email**: Specifies the use of email within the university.
- **General Policy on the Use of Information Systems**: Describes the general principles for using information services.
- **Policy on Consequences for IT Offences**: Provides disciplinary guidelines if the operating principles are violated.
- **Data Classification and Secure Storing**: Defines the sensitivity of information for the organization.
- **Safety Guidelines for Using Social Media Services** (Briefly, Social Media Security Guidelines): Instructs the university community on secure practices with social media accounts.

- **Data Security and Data Protection Breach** (Briefly, Incident Reporting Guidelines): Provides instructions for handling information security incidents and general information about digital threats.
- **Communication and Marketing's Vision**: We communicate boldly, responsibly, and impactfully. We invite dialogue.
- **Metropolia's Social Media Guidelines and Channels**: Describes how to communicate about university matters to stakeholders. Metropolia aims to be actively present on social media, produce diverse and timely content for followers, and strengthen its influencer role by engaging in responsible dialogue with other stakeholders.
- **Data Protection Policy and Guidelines**: Explains the rules and legal requirements related to the processing of personal data (Metropolia's data protection policy is currently only available as in Finnish).
- **Privacy Breach Guideline**: Provides guidance on handling security breaches related to personal data within the university.

Policy requirements

When using a TikTok account, it's essential to consider the more detailed guidelines provided in this section. In addition to the instructions in the chapter, the key rules for proper TikTok account usage are described in Social Media Security Guidelines, the Social Media Guidelines and Channels instruction, and the Data Classification and Secure Storing rule. These documents provide further clarity on how to use TikTok appropriately within the university context.

First phase: Actions to take before starting to use TikTok

- To create a TikTok account, a service request must be submitted to IT Services. The service request should clearly indicate that it pertains to a device, commonly referred to as a **'social media device'**, specifically intended for using the TikTok service.
- The service request should explicitly state that it concerns TikTok usage on a device managed by the university, necessitating a separate social media device for the employee.
- The service request should include details such as the number of social media devices required, the TikTok account holder(s), and the name of their supervisor. Account holders should primarily use these devices.
- If someone other than Communication and Marketing wishes to create a social media account, they must consult with the previously mentioned department on the matter, before submitting the service request to IT Service.
- IT Services will provide the requested devices and issue a separate email for social media account usage. The organizational e-mail acquired for using a social media account is explained in more detail in Social Media Security Guidelines.
- During the service request process, user support will remind the requester of the security guidelines related to social media, the university's social media guidelines, and data classification principles.
- Social media devices intended for TikTok usage are managed by IT Services. These devices must have the capability for remote management by IT Services.
- Each social media device is associated with its own account, such as an Apple ID per device. These accounts serve as device-specific identifiers within the university.
- A **device account** means that the account's contact information is used for interactions within the device's app store. For Apple devices, the Apple ID address is provided as a separate organizational email address, given by IT Services after the department has gotten a service request from a user. Below is an example of contact information for app store purposes:
    - **Email**: tutkimushankeX@metropolia.fi
    - **First Name**: John
    - **Last Name**: Smith
    - **Phone Number**: The phone number associated with the social media device's established mobile subscription, e.g., 123456789.

Second phase: using the TikTok service

- To log in to TikTok, use the specified email address provided by IT as to use the email for TikTok-related or other social media purposes. Choose email and password as your login credentials when registering to the TikTok service. Do not log in to TikTok using third-party accounts (such as Google or Facebook) through the app. Below is an example of how to log in to TikTok:
    - **Email**: researchprojectX@metropolia.fi
    - **First Name**: John
    - **Last Name**: Smith
    - **Phone Number**: Use the phone number associated with the social media device's established mobile subscription, e.g., 123456789
    - **Username**: User-defined (e.g., tutkimushankeX)
    - **Password**: User-defined. The password should not be the same as what you use for university services. It must be unique for TikTok login.
- Using TikTok on devices provided by Metropolia, such as work computers and work phones, is prohibited. TikTok is allowed only on a separate device specifically acquired for this purpose, known as a 'social media device'. This device should be used exclusively for TikTok.
- Downloading the TikTok application on Metropolia-managed devices is prohibited except for the designated social media device. You may download the TikTok app on the social media device.
- Other social media applications, such as Facebook or Instagram, can also be downloaded onto the social media device. The social media device is primarily used for creating content on social media.
- On the TikTok device, a separate email provided by IT Service is used. No employee's or organization's email account should be used on this device, unless otherwise is stated on the matter.
- Viewing TikTok content on university-managed information assets are prohibited, even if the social media service is accessed through a browser and registered with a personal private email.
- TikTok can be used on personal devices that are not connected to the university together with provided the service is accessed using an individual's private email account.
- All application purchases made on the social media device must be done using registered gift cards. Personal or university bank cards should not be entered into the app store on the social media device. Entering bank credentials for the social media device or TikTok service is also prohibited. All payments related to the social media device are processed as gift card transactions.
- Each social media device will have its own separate connection. IT Services is responsible for obtaining the connection for each device.
- To establish an internet connection, the device uses mobile data.
- The social media device should not be used for university information technology setvices. TikTok content is created on the social media device using the TikTok application primarily.
- The TikTok application can be downloaded from the social media device's app store for using TikTok services.
- If the account custodian delegates communication on TikTok, for example, to an intern, the custodian holder is responsible for the intern's actions.
- The custodians and supervisors must ensure safe behavior when using TikTok services. Communication and Branding; maintain up-to-date security awareness regarding safety risks related to TikTok. They also provide guidance to others interested in appropriate TikTok usage.
- For the social media device used in creating TikTok content, a designated location is defined where the device is stored. This area serves as the social media device's security zone, accessible only to authorized personnel.
- An up-to-date list must be maintained for social media devices taken outside the security zone. When the device is no longer in use, it should be returned to the security zone.
- For any security or data protection incidents, contact the IT department. They handle exceptions and incidents related to information security and privacy as the first point contact.

Third phase: Ending TikTok service usage and actions in special situations

- When the TikTok account is no longer needed, it will be deactivated. Deactivation of the TikTok account occurs within the TikTok service.
- If necessary, the TikTok account custodian can be changed, for example, due to an employee transition or when social media account usage is delegated to another employee by a supervisor. The supervisor is responsible for up-to-date management of the TikTok account custodian and users, determining who produces content within the TikTok service.
- Account custodian changes should be reported to IT Services, which will document the matter, such as in the Requeste service request system.
- When a TikTok account is deleted, it should be reported to IT Services, which will document the matter, such as in the Requeste service request system.
- If an organizational email account intended for social media use is no longer needed, IT Services will deactivate the account. The account holder must inform IT Dervices of the unnecessary status of the organizational email account. It is advisable to request deactivation of the organizational account only when it is no longer used on other social media platforms or for creating other social media content.
- If an organizational email account has been acquired solely for TikTok service usage, it can be deactivated simultaneously when the TikTok account custodian informs IT Services for TikTok account deletion.

Appendixes

Annex 1: The responsibilities of the Metropolia TikTok policy

Role	Responsibility
IT Management	Ensures the appropriateness of the TikTok policy and approves changes made to this policy. Advises the Chief Information Officer (CIO) on implementing information security.
Information Security Specialist	Is responsible for writing and maintaining the TikTok policy on the IT department's Wiki pages. Reviews the relevance of the policy annually with the CIO. Advises the CIO on implementing IT security.
Chief Information Officer (CIO)	Participates in the review of the police. Responsible actor who decides whether the policy is still up-to-date or if the document needs to be reviewed among the IT Management. The CIO oversees Metropolia's cybersecurity.
IT Services	Acquires a social media device for using TikTok and provides a separate email account for those who want to communicate on TikTok. Maintains an up-to-date security guide for social media.
Managers or Supervisors who wish to establish a TikTok social media account	If their subordinate's job includes using a TikTok service, they are responsible for ensuring information security of the social media account. They decide which social media devices are used for TikTok communication and who is the custodian of the social media account. Before implementing the TikTok account, they consult with the Communication and Marketing.
TikTok Account Custodian	Consults communication services to assess the necessity of a TikTok account. After consultation, submits a request to IT Service for a separate email account and social media device for the TikTok account. Sets up the TikTok account. Ensures the account's security and appropriate communication. Adheres to the guidelines in this document for data security. If needed, they seek additional guidance from IT Services and refer to the Social Media Security Guidelines for social media accounts on the Wiki pages.
The employee of the Metropolia University	Does not install TikTok on devices managed by the university. Does not use TikTok via a web browser. Does not log in to the TikTok platform using the university-provided email address and username.

	Installs the TikTok application only on a separate social media device. Follows the university's regulations, policies and guidelines regarding social media security. Reports security and privacy incidents to the IT Services.
Human Recourse Services (HR)	Manages IT violations that break the TikTok policy´s guidelines.