FANO 有光科技 Labs

BRING YOUR OWN DEVICE POLICY

This policy sets out how you should use your own device when connecting to the corporate network and accessing corporate data of Fano Labs Limited. It is divided into the following sections:

- Acceptable use
- User responsibilities / Corporate IT responsibilities
- Devices & support
- Monitoring & privacy
- Device reset and data deletion
- Policy enforcement
- Security controls

You should read carefully and sign at the end of this policy to acknowledge understanding and agreement to the terms contained in it. You must sign this policy as one of the conditions for your employment at Fano Labs Limited.

Acceptable Use

1. Fano Labs Limited defines acceptable business use as activities that directly or indirectly support the business of Fano Labs Limited.
2. The company defines acceptable personal use on company time as reasonable and limited personal communication or recreation, such as reading or game playing
3. Employees are blocked from accessing certain websites during work hours or while connected to the corporate network at the discretion of the company. Such websites include, but are not limited to:
    - Any personal instant messaging service, such as LINE, WeChat, WhatsApp, or Facebook Messenger.
    - Social networking sites, such as Facebook, Twitter, LinkedIn, Instagram, Pinterest, or Flickr.
4. Device camera and/or video capabilities are only allowed in the following occasions:
    - The capture of graphic and/or video contents using your device is explicitly approved by your line manager and is essential to your job.
    - Business-related video conferencing.
5. Devices may not be used at any time to:
    - Store or transmit illicit materials.
    - Transmit materials to third parties that have no current business relations with Fano Labs Limited or to the general public.
    - Store or transmit pornographic, hate-inciting materials or any materials if transmitted may amount to hate crimes, vilification, unlawful discrimination, harassment or bullying.

- Capture, store or transmit personal data, images of any staff member, customers, suppliers and any parties that are not part of our normal business functions or that are not allowed and covered by our Data Protection Policy.
- Store or transmit proprietary information belonging to another company.
- Engage in outside business activities.

6. The following apps are allowed (please refer to the Allowed Apps List):
    - MS Office and apps of similar function (e.g. Google Apps, OpenOffice)
    - Travel-related apps used for business travel (e.g. hotel booking, flight booking, transportation, weather sites, maps and GPS apps)
    - Social networking apps used for business functions of Fano Labs Limited (e.g. LinkedIn, posting on Fano Labs Limited's official Facebook page, official Twitter tweets)
    - Graphic / image editing & conversion apps for business functions of Fano Labs Limited
    - Cloud storage and apps of similar function (e.g. Dropbox, Box.com, iCloud, and Google Drive)
7. The following apps are not allowed (please refer to the Excluded Apps List for Your Own Device. Should discrepancy exist between this and the Excluded Apps List, the latter shall prevail):
    - Apps that display, store or transmit pornographic, hate-inciting materials or any materials that may contravene laws relating to hate crimes, vilification, unlawful discrimination, harassment or bullying
8. Employees may use their mobile device to access the following company-owned resources: email, calendars, contacts, documents, etc.
9. Fano Labs Limited has a zero-tolerance policy for texting or emailing while driving and only hands-free talking devices while driving are permitted.

User Responsibilities / Corporate IT Responsibilities

1. Employees are responsible for ensuring no disallowed apps or software is installed on the device.
2. Employees are responsible for making sure that only the allowed operating systems, browsers and apps are installed and used.
3. Employees are responsible for making their own backups of their personal data in case of a data / security breach and/or if Fano Labs Limited needs to do a remote wipe of all data on the device.
4. Employees are responsible for connecting to the corporate network and accessing corporate data in an appropriate & ethical way as advised by IT, in this policy and in any other relevant policy or procedure. You shall take all practicable steps to ensure the security of the corporate network and data.
5. Employees must report lost or stolen devices to the company within 24 hours. You are responsible for notifying your mobile carrier immediately upon loss of a device.
6. Corporate IT will check your device on first-time connection to the corporate network and, on your departure from the organisation, your device's compliance with this policy and will remove any software or data as necessary.

7. Corporate IT will support you and resolve any connectivity issues you encounter.
8. Fano Labs Limited takes no responsibility in any data loss, financial loss or damages arising out of your connection of your device to the corporate network and data.

Devices & Support

1. The following devices are allowed under this policy:
    - Smartphones: iPhones, Android phones, BlackBerry phones, and Windows phones.
    - Tablets: iPads, and Android tablets.
    - Notebooks and laptops running iOS or Windows XP/10.
2. Only connectivity issues (i.e. connectivity to corporate network and to corporate data sources) are supported by Fano Labs Limited's IT team.
3. Devices must be presented to IT for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.
4. If you suspect your device security might have been compromised or a data breach has happened on your device involving corporate data, you should report and present your device to IT for immediate damage control. In such case, Fano Labs Limited may discontinue your access to the corporate network and data and/or wipe out all data on your device. You are responsible for constantly backing up your personal data in case such an incident happens.

Monitoring & Privacy

Fano Labs Limited places the following monitoring controls on all devices that access the corporate network and data:

1. Restriction of the types of devices and operating systems to only legitimate and supported ones.
2. Checking of apps that are allowed in the allowed apps list.
3. Monitoring of time spent on and types of web resources that are not business related.
4. Any controls to manage workplace productivity, service quality control or enforcement of company policies.
5. Any controls to protect the safety of employees, business assets, intellectual property or other proprietary rights.
6. Checks to prevent vicarious liability where the employer assumes legal responsibility for the actions and behavior of employees.
7. Monitoring in order to comply with statutory or regulatory obligations that provide, or give reasonable cause, for the preventive monitoring of employees.

FANO 有光科技 Labs

Device Reset and Data Deletion

1. Fano Labs Limited may at any time, with or without prior notice to you, reset your device and/or remotely wipe out all data on your device.
2. You are strongly advised to back up your own personal data at all times.

Policy Enforcement

Data security is highly important to Fano Labs Limited, our customers and our business partners. While a Bring Your Own Device Policy assists our business and has become a common business practice of many leading business organisations, we must protect the interests of the company and of other related stakeholders. A violation of this policy may result in consequences of varying degrees of severity.

1. We reserve the right to disconnect devices or disable services without notification.
2. Violation of this policy and other related policy arising from a Bring Your Own Device Policy may result in disciplinary actions including immediate termination of your employment.
3. We encourage any staff member or any party to report any violation or potential violation of this policy by our staff, whether or not the violation happens in the course of his/her carrying out his/her job duty.
4. Abiding by this policy demonstrates our core values of being professional and trustworthy to our staff members, customers and other stakeholders.

Security Controls

In order to prevent unauthorised access, devices must be password-protected using the features of the device and a strong password is required to access the company network.

1. The company's strong password policy is: Passwords must be at least eight characters long with a combination of letters, numbers and symbols. Passwords must be changed every 180 days.
2. The device must lock itself with a password or PIN if it's idle for 15 minutes.
3. After five failed login attempts, the device will lock. Contact IT to regain access.
4. Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
5. Employees are automatically prevented from downloading, installing and using any app that does not appear on the company's list of approved apps.
6. Smartphones and tablets that are not on the company's list of supported devices are/are not allowed to connect to the network.
7. Employee access to company data is limited based on user profiles defined by IT and is automatically enforced.
8. The employee device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, or 3) IT detects a data or policy breach, a virus or a similar threat to the security of the company data and technology infrastructure.

FANO 有光科技 Labs

APPENDIX – ALLOWED APPS LIST

- MS Office and apps of similar function (e.g. Google Apps, OpenOffice)
- Travel-related apps used for business travel (e.g. hotel booking, flight booking, transportation, weather sites, maps and GPS apps)
- Social networking apps used for business functions of Fano Labs Limited (e.g. LinkedIn, posting on Fano Labs Limited's official Facebook page, official Twitter tweets)
- Graphic / image editing & conversion apps for business functions of Fano Labs Limited
- Cloud storage and apps of similar function (e.g. Dropbox, Box.com, iCloud, and Google Drive)

APPENDIX – EXCLUDED APPS LIST

Apps that display, store or transmit pornographic, hate-inciting materials or any materials that may contravene laws relating to hate crimes, vilification, unlawful discrimination, harassment or bullying