UBER

Network & Device Acceptable Use Policy

Revised - March 2017

CONFIDENTIAL

This document is the property of Uber. It contains information that is proprietary, confidential or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Uber.

1. Objective

This policy ("Policy") defines the standards and requirements for access and use of the communications infrastructure, network and systems ("Network") of Uber Technologies, Inc. and/or its affiliates or subsidiaries (collectively, "Uber"), including any data and tools on or available through the Network. This Policy also defines the standards and requirements for use of any computers, mobile devices or other tools to access the Network ("Devices"), including Devices owned and/or issued by Uber ("Uber Devices") or that are owned by persons or parties other than Uber ("Non-Uber Devices").

This Policy will be enforced consistent with internal Uber protocols and applicable laws.

2. Scope

This Policy applies to any person who accesses or uses the Network, including but not limited to full-time and part-time employees of Uber, interns, temporary and contingent workers, sub-contractors, and vendors or consultants engaged by Uber (collectively, "Personnel").

3. General Principles

3.1. Personnel are permitted to access the Network solely for legitimate business purposes that are consistent with their roles and responsibilities.

3.2. Personnel must comply with formal written instructions or guidelines issued/or provided by Uber EngSec or Uber Legal governing access or use of the Network and all data on the Network, and all Uber Devices.

3.3. Personnel are prohibited from circumventing or attempting to circumvent any security measures or technical restrictions relating to the Network and all data on the Network, including measures and restrictions relating to the use of Uber Devices and Non-Uber Devices to use or access the Network or data on the Network.

3.4. Personnel shall not use or access the Network in any way or for any purpose that is or is reasonably likely to be disruptive to the Network or Uber's business, jeopardizes the safety and security of the Network, or is not permitted under applicable laws.

3.5. Personnel shall avoid introducing malware and other harmful materials into the Network, such as by exercising caution before opening attachments or clicking on hyperlinks.

3.6. Personnel who discover or suspect unauthorized access or use of the Network should report these activities to security@uber.com.

3.7. Employees of Uber or its subsidiaries who are found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Personnel who are not employees of Uber or its subsidiaries (such as contractors or contractor personnel who are granted temporary access to the Network for the performance of a particular project or contract) may be subjected to revocation of the individual's right to use the Network or to access Uber systems or premises and, in serious cases, the entire contract with the vendor or contractor may be terminated as a result of the 'Personnel's violation of this Policy.

4. Internet, Email, and Other Communications

4.1 Personnel should generally only access and use the Network for purposes of performing work on behalf of Uber. Incidental personal use of the Internet through the Network, Uber email or other authorized communication tools is allowed when such use does not: (a) interfere with Uber's operations; compromise functioning of the Network; (b) consume more than a trivial amount of resources that could otherwise be used for business purposes; or (c) interfere with the Personnel's employment or other obligations to Uber.

4.2. Personnel must exercise caution when opening attachments and clicking on hyperlinks. Personnel must not open emails and attachments or click on hyperlinks that are received from unknown sources or otherwise appear suspicious. Report all suspicious activity to security@uber.com.

4.3. Personnel are strictly prohibited from accessing or using the Network for any of the following activities or purposes:

- Pursuing personal profit--making or other commercial activities that are not necessary to fulfill their responsibilities or obligations to Uber.
- Downloading or copying unlicensed software or files from untrusted third--party sources on the Internet without prior approval from security@uber.com.
- Copying, moving or storing non-public Uber information to local hard drives or portable electronic media such as external hard drives or USB drives, unless required for a defined business need.
- Copying, publishing, sharing or storing Uber information on or to unauthorized third--party platforms and services unless prior approval is obtained from security@uber.com. New vendor engagements involving transfer of Uber information to a third-party should be submitted to EngSec Compliance for review prior to any such transfer, as explained on here.
- Sending customer or user payment card or other financial account information, Social Security numbers, driver's license or other state, government or national identification numbers and similar types of sensitive data in the form of clear text. If you need to send such information electronically, contact security@uber.com for assistance.
- Bypassing, disabling or tampering with Uber's security controls, software, equipment, or security logs.
- Visiting websites with pornographic, obscene or otherwise objectionable content unless required for a defined business need. In a case of the latter, prior written approval is required from the Personnel's Manager.
- Introducing malicious software into the Network, such as viruses, worms, Trojan horses, etc.
- Communicating with end users or customers of the Uber service unless, unless required for purposes of the Personnel job responsibilities.

- Engaging in any form of harassment, discrimination or other conduct prohibited by Uber's employee Code of Ethics.

- Creating or forwarding "Chain letters", "Ponzi", or other "Pyramid" schemes of any type.

- For Personnel who have been issued an Uber email address, using any email address other than such address to conduct business for Uber. This includes but is not limited to use of personal email addresses such as Hotmail or a personal Gmail address.

- Using instant messaging software (such as AIM, Yahoo! Messenger, MSN, etc.) to transfer or communicate Uber information, other than software made available by Uber.

- Copying, moving or storing non--public Uber information to local hard drives, portable media such as removable drives or to a non Uber system unless explicitly authorized to do so in the performance of their regular duties. If expressly authorized to store non-public Uber information onto portable media, it must meet Uber's encryption standard. All USB drive usage is logged and monitored for data loss protection.

5. Passwords

5.1. Personnel must comply with the following password requirements:

- Passwords have complexity requirements that are dependent on the length of the password:
  - No password may be less than 8 characters long
  - Passwords that are less than 14 characters long must contain characters from 3 of the following four categories.: Upper case (i.e.A-Z), lower case (i.e. a-z), numerals (i.e. 0-9), and punctuation (i.e. !@#$%^&*()_+|~-=\{}[]:";'<>?,./);
  - Passwords that are less than 20 characters long must contain characters from 2 of the following four categories.: Upper case (i.e.A-Z), lower case (i.e. a-z), numerals (i.e. 0-9), and punctuation (i.e. !@#$%^&*()_+|~-=\{}[]:";'<>?,./); and
  - Passwords that are longer than 20 characters have no character set restrictions or requirements.
  - Passwords may not be composed of single words that can be found in a dictionary.
  - Passwords may not contain the user ID with which a password is associated; and
  - Each password must be different than the 3 previous passwords associated with a user ID.

5.2. Personnel must protect the confidentiality and security of their passwords, including by not writing down their passwords. The use of a secure password storage utility is encouraged. A password manager tool is available here.

5.3. Personnel may not share their passwords with any other Personnel and may not access or use the password of any other Personnel.

5.4. Personnel must immediately change their passwords when any unauthorized access to their passwords is suspected and report such activities to security@uber.com. In those cases where application or operating system functionality does not enable Personnel to change their own passwords, then the Personnel must immediately contact it@uber.com to have their passwords changed.

6. Full- Disk Encryption

6.1. Devices, including Personal Devices, used to access the Network shall be configured with full disk encryption (FDE) software. This includes Uber laptops as well as mobile phones, tablets, or PDAs.

- Acceptable FDE solutions include Windows Bitlocker, Apple FileVault 2, iOS Data Protection, and Android System Encryption.
- Other solutions will be evaluated as necessary.

6.2. All Devices used to access the Network shall be configured to require a password prior to access.

7. Authorized Devices

7.1 Personnel are only permitted to access the Network using authorized Devices. Authorized devices are limited to (1) Uber Devices; and (2) Non-Uber Devices mobile for which Mobile Device Management software ("MDM") has been installed.

7.2 Personnel may not access the Network using Non-Uber Devices for which MDM has not been installed by Uber, except with the prior approval of the EngSec Compliance team. Please contact engsec-compliance@uber.com to request such approval.

7.3 Uber reserves the right to de-authorize the use of any Non-Uber Device for accessing the Network at any time and for any reason.

8. Other Prohibitions

Personnel may not engage in any of the following actions when accessing or using the Network:

8.1. Take any action that would amount to a security breach or disruption of Network communications. Security breaches include, accessing data of which the Personnel is not an intended recipient or logging into a server or account that the Personnel is not expressly authorized to access, unless these duties are within the scope of the Personnel's regular duties. Disruption includes Network sniffing, port scanning, ping sweeps or floods, packet spoofing, denial of service, and forged routing information.

8.2. Use any program/script/command, or send messages of any kind, with the intent to interfere with, or disable, any individual's session, via any means, locally or via the Internet/Intranet/Extranet.

8.3. Connect to unauthorized third -party connections or make changes to existing connection configurations without prior approval from Security@uber.com.

9. Monitoring By Uber

9.1. Uber Devices and the Network remain at all times the property of Uber.

9.2. All data that is composed, transmitted, accessed, or received via Uber Devices or the Network is considered to be part of the official records of Uber and, as such, is subject to disclosure to Uber, law enforcement, or other third parties.

9.3. Personnel communications made using Uber Devices or the Network may not be kept private or confidential, including if Personnel send or receive personal communications using such equipment.

9.4. Information relating to Personnel's use of Uber Devices and the Network, including files stored on or transmitted through Uber Devices or the Network (including personal communications transmitted through Uber's Devices or Network) may be retained for as long as necessary by Uber.

9.5. To the extent permitted under applicable law, Uber reserves the right to access, collect, inspect, review, monitor, decrypt, delete, copy, remove, change, transfer, record, store, block, disclose (including within Uber and its subsidiaries and affiliates, and to third parties), and otherwise process all files and data stored on or transmitted using Uber Devices or the Network, and any communications made using Uber's Devices and Network, at any time and without further notice.

9.6. Uber reserves the right, in accordance with applicable law, to monitor, take custody of, or search any Device used to access the Network (other than Uber's guest Wifi networks only) at any time and for any reason. This includes, but is not limited to, monitoring any information received, stored or sent via the Network through email or the Internet, and removing confidential information stored on Devices upon termination of employment with Uber.

Printed Name:

GYAN PRAKASH

Signature:

Gyan Prakash

Date Signed:

02/23/2021

Beeline ID:

UBRW000100380