maximobility.

DATA & SYSTEM CORPORATE SECURITY STANDARDS

INTRODUCTION

This document describes Maxi Mobility's security policy, both at the hardware and software levels. Having a unified security policy pursues several objectives:

- Ensuring that the data we handle, both private company data (financial, tax, owners, sales), as private data of our customers and our employees are safe against possible attempts of theft, copy or inappropriate use.
- Guarantee to our clients, investors and partners that the use of data within our company meets or exceeds the security standards of a modern company.
- Offer all the Maxi Mobility employees the necessary tools so that they can carry out their work with confidence that they are doing it in a safe environment
- Unify all the security procedures under one roof, simplifying their compliance while reinforcing pillars on which we base the security of the data.

SUMMARY

The standard security policy is divided into several areas:

- Basic measures of cybersecurity
- Standards of Corporate systems
- Basic security measures within the development team
- GDPR compliance and DLP prevention
- Corporate digital security committee

These security measures are fundamental for a company like ours that can guarantee the integrity and privacy of the data, but the most important part of a security policy is that we comply with it. The first and most important line of defense that Maxi Mobility has against possible

maximobility.

intrusions or attempts to steal data is our employees and their expertise. We ask you please read this document carefully and be consistent in the application of its measures.

BASIC MEASURES OF CYBERSECURITY

In this section you can find the most basic security measures that are common to all Maxi Mobility users. These measures, although in many cases simple and obvious, are the most important weapon we have to prevent data leaks or intrusions in our systems.

1. Your keys to ALL systems are personal and non-transferable, do not share them with anyone, not even IT or your boss / supervisor. IT will never ask for your password.

2. JumpCloud is our SSO (Single Sign On) system. At this moment JumpCloud controls the Google password, Dropbox, VPN and in some cases Tableau. In the future, most applications will be managed from here. Your password will expire every 90 days and must have a complexity of 8 characters, an uppercase, a lowercase and a number. The deployment of JumpCloud is being carried out by country, if you think that your locality has already been deployed and you do not have Jumpcloud enabled yet, you can write in the Slack channel #it_security for us to enable it.

3. Make sure you have "two-step identification" enabled in Google (If you try to access from a new device, your phone will ask for your permission). If you do not have it enabled, contact IT on channel #it_security. As of Q2 2019 you will not be able to access Gsuite without 2FA enabled.device

4. Block your device when you get up, if you do not, once enabled on your device, JumpCloud will do it for you.

5. If you have mail on the phone, it is **MANDATORY** to have a lockscreen through PIN or pattern/fingerprint. If your terminal is a company owned, you will have the google MDM installed. If you lose it

or it is stolen, report it to IT immediately. For those who want to have the

maximobility.

MDM enabled on their personal telephones (extra measure of security against theft, professionally and personally), it can also be enabled by requesting it through the channel #it_security.

6. You are responsible for what happens with the information you share digitally, for labor and legal purposes. This means that if you share information with unauthorized people, the consequences of its use are your responsibility.

7. Be very careful with “Phising” ... If you do not know the sender of an email, or are not expecting the mail, NEVER open links or attachments. Any link that asks for financial, tax or identity data should be treated as "suspicious". If you find an email of this type, it is important to report it to global.it@cabify.com or on the slack channel #it_security.

8. Be very careful with who and at what level of permissions you share documents. The standard tool for sharing files with external files is Dropbox Enterprise. Sharing files through the drive will be progressively disabled during 2019.

9. Do not share information on server names, passwords or code in general in any public or private forum on the Internet ... NEVER.

10. Do not install any application by API against google without consulting first (This means that if you ask for your account of cabify to give you access, it is using API). There will be periodic sweeps of the applications connected by API, and we will cut what we do not know ... so the applications that are not allowed will stop working.

STANDARDS OF CORPORATE SYSTEMS

The homogeneity of hardware and software is important in a network of security, the more homogeneous the systems we have, the least possible security holes we will have. With this in mind, we have designed these

system standards, which must be followed unless expressly authorized by IT Global:

maximobility.

1. The computer equipment we work with should not be outdated, so the max-life of these equipment should not be surpassed: a. Laptops: 3 recommended, 5 maximum
    b. Switches: 4 recommended, 6 maximum
    c. Firewalls: 4 recommended, 6 maximum
    d. Tablets: 2 recommended, 4 maximum
    e. Servers: 3 Recommended and maximum, must transition to the cloud based instead of being replaced
2. The operating systems accepted in laptops are:
    a. Windows: Windows 10 Build 1709 or newer
    b. Apple: MacOS 10.12 Sierra or newer
    c. Linux: Ubuntu 16.04 or newer
    d. Chrome OS: No version needed
3. All Apple, Windows and Linux systems must have enabled automatic updates, installing the mandatory automatic installation at least once a week.
4. All Apple and Windows systems must have the corporate Antivirus / anti-spyware installed, at the moment the standard is Palo Alto Traps. If your device does not have it installed, communicate it on channel #it_security.
5. All systems working remotely must have the VPN Globalprotect Cloud service available on their computers and activated when they are out of the office.
6. In Q4 2019, encryption of the hard disks of all devices, whether Windows or Mac, will be launched remotely. ... the decrypted key will be saved in a repository owned by the company.
7. Treatment of the company's hardware:
    a. The users are responsible for the treatment they give to the company's devices. The logical wear due to the use of the devices as well as possible accidents will be accepted (example, a glass of water spilled). The repair by accident will be the responsibility of the company.
    b. Negligent treatment of the equipment or accidents that could be prevented (Example, laptop has fallen to the pool) will not be accepted. The repair in case of negligence will be charged to the user.

c. The equipment must be returned to IT under conditions similar to those received, this means that if stickers or

maximobility.

accessories have been placed, it is the responsibility of the user to remove them before returning the equipment.

d. In case of theft, it is necessary to file a complaint immediately with the police, and provide this complaint as soon as possible to the IT department. It is essential to inform as soon as possible the IT deparment once the theft is known in order to block accounts. The replacement of stolen equipment is at the expense of the company, but a second theft of equipment stolen in a period less than 2 years will be borne by the user, since it constitutes little respect by the employee of the material of the company.

8. The use of USB external memory must be limited to memories that are encrypted. All data transfer to external must be made through approved methods (Dropbox) and never through external memories. These should be limited to data transfers between internal company devices.
9. The laptops accepted in the company are as follows:

a. Standard (Base): HP Probook 440: i5, 8gb ram, 128gb SSD, FullHD, Windows 10 Pro (or similar if not economically viable).

b. Performance (Users needing extreme power): HP Elitebook 840, i7, 16gb Ram, 256 SSD, Wind10 pro (or similar if not economically viable).

c. Executive (Heads, GMs, C-Level): HP X360 1030: i5 8gb RAM, 256 SSD, Win10 Pro (or similar if not economically viable). d. KAM (Team Members with sales to key clients): Microsoft Surface Pro: i5, 8gb RAM, 128 SSD, Win10 Pro

e. Development (or approved by Global Head / GM): Apple Macbook pro 13, i7, 16gb RAM, 256 SSD

10. No Software, except that approved by the Global IT department, can be installed on the company's equipment. The only exceptions to this rule will be the software used by the development team, whose installation and responsibility falls on the product team.
11. Local copies of data should be the exception, not the norm. The proper way to work in Maxi mobility is in the cloud, specifically in

Google Drive.

maximobility.

BASIC SECURITY MEASURES WITHIN THE DEVELOPMENT TEAM

1. All equipment in the product team must be encrypted with systems of at least 256 bits.
2. All internal systems with internet connection must be protected through a proxy with Oauth2 authentication.
3. In case of loss or theft of any equipment that is part of our product team, it is imperative to report it immediately as described here. In case you can't access it, please contact your manager and ask them to do it for you.
4. In case of loss, theft or suspicion of a credential problem, it is imperative to report it immediately as described here. In case you can't access it, please contact your manager and ask them to do it for you.
5. Any communication to the panic email will result in the default blocking of the reported account and initiation of security investigation, so you have to be relatively sure that an incident has occurred.
6. All passwords must be generated by the automatic secure password manager that we have standardized within the product team.

COMPLIANCE WITH GDPR AND PREVENTION OF DLP

The European data protection regulations that came into force in 2018, known as GDPR, are mandatory regulations for companies and their employees. It is very important that we follow some basic rules to comply with it.

The main idea of the GDPR is that the personal data of the people should not be shared, stored or treated without the express consent of the person who owns this data, and that the companies and / or employees will follow basic rules with the treatment of These data ensure that these data are not lost, are accessed by unauthorized persons or stored for no reason.

1. Personal data protection measures must be treated with the same care for information of both clients and employees
2. Employees must handle private information with care, never keeping

personal information (health, financial, contact ...) where it can be accessible by unauthorized personnel.

maximobility.

3. The amount of personal information used and stored must be as low as possible for the fulfillment of the task to be performed. 4. Personal information must not be shared with anyone, whether natural or legal person, outside the organization Maxi Mobility without having signed a document certifying that you adhere to current regulations

5. Our systems, whether internal or contracted, must have the capacity to erase or tokenize personal information that is required within a maximum period of 14 days for non-financial information.
6. Employees must refrain from sending personal data by email except with the express consent of the person whose data is being shared. 7. All data in the shared folders of the company are audited automatically, and personal data (health, financial, tax or contact) shared outside the organization or open to all users of Maxi Mobility SLU will be automatically deleted without prior notice. 8. Anyone with knowledge of a data breach, whether personal both customers and employees, as proprietary and confidential company has to report the leak immediately email dpo@cabify.com

DIGITAL SECURITY CORPORATE COMMITTEE

Maxi Mobility takes the data security of both our customers and our employees very seriously, so a corporate digital security committee has been created that meets at least once a quarter, and will have a report on the state of the company. monthly security distributed.

1. The safety committee will be coordinated by the IT department and the product department, with the product safety manager as a specialist and the IT security manager as coordinator.
2. The safety committee must have at least one member who is C-Level to ensure that digital security is present in the strategic decisions of the company.
3. The changes made by the safety committee will be reflected in this document on an annual basis, and must be accepted by the workers upon entering the company and once a year through the following form.