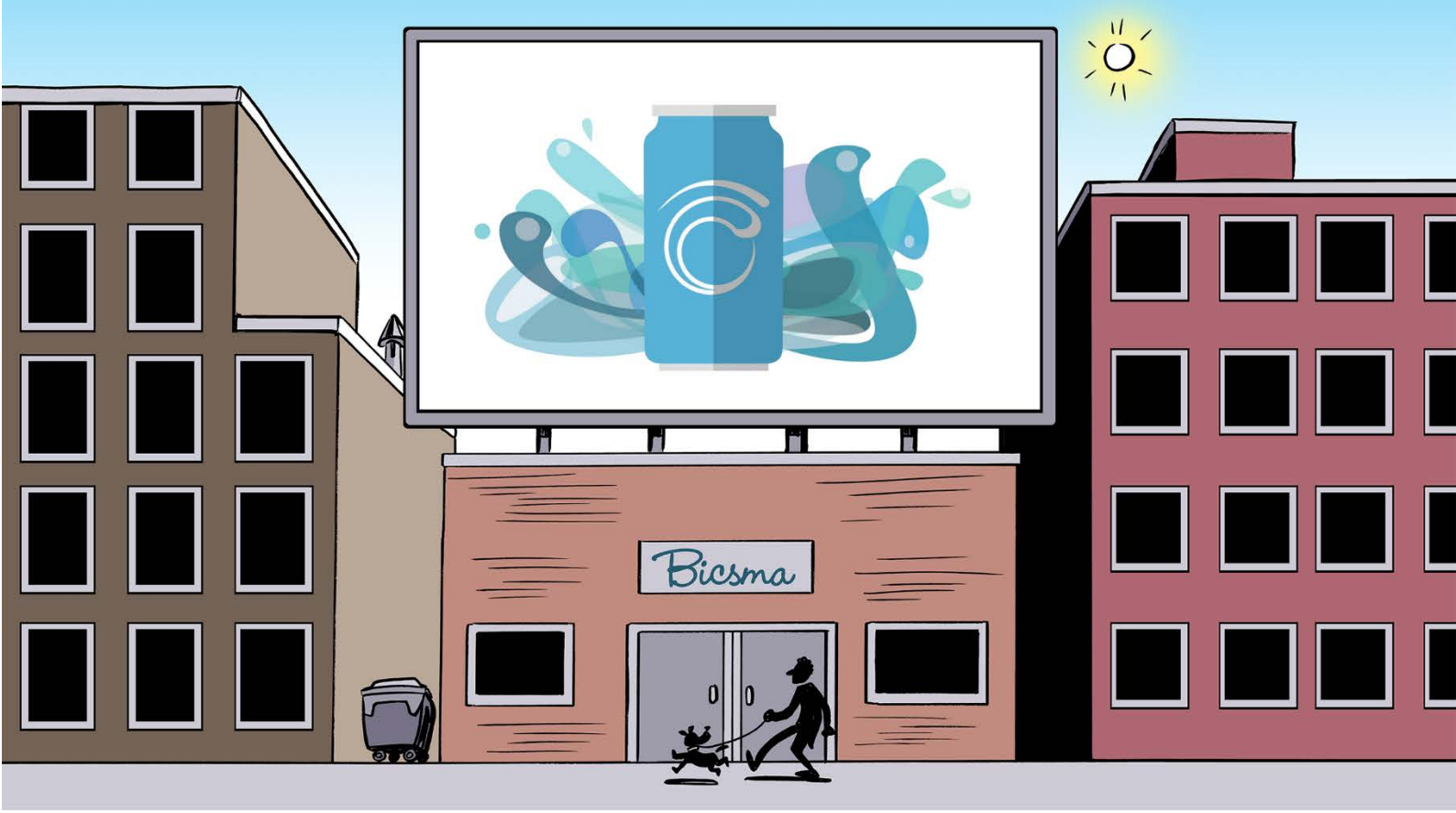

Bicsma

BICSMA´S BYOD POLICY

Table of Contents

1. Document features

1.1 Custodian contact details

Name:
Location:
Telephone:
E-mail:
URL:

1.2 Reviews

Date of most recent review:

Date of next review:

Date	Author	Version	Modifications

1.3 Paragraph list

Name	Function	Role	Date	Paragraph

1.4 Distribution list

Name	Function	Role	Version	Medium/ format

2 Framework

2.1 Introduction

Bicsma BV recognises the advantages of using personally-owned (mobile) devices for work purposes. At the same time, Bicsma BV is aware of the risks incurred by the use of such devices. This Bring Your Own Device (BYOD) policy aims to bring the risks under control by outlining the conditions on which personally-owned devices may be used for work purposes. This policy shall be regarded as a supplement to Bicsma's strategic information security policy.

The provisions set out in this policy apply to devices provided by the employer and devices purchased by the employee, unless expressly stated otherwise.

By using a mobile device to perform work activities on behalf of Bicsma BV and/or connecting a mobile device to the corporate network of Bicsma BV, the user automatically accepts Bicsma BV's strategic information security policy and BYOD policy. Access to the corporate network may only be granted upon the user's explicit agreement to these policies. Users and devices that do not comply with this policy may not gain access to the corporate network.

2.2 Definitions

Terms and definitions are used in line with Bicsma BV's strategic information security policy. The following terms that are not included in the strategic information policy are defined as follows:

Application

Any software that can be installed on a device by the user or the (IT) management organisation.

Management organisation

The team or staff members performing activities on the device on behalf of Bicsma BV.

Bring Your Own Device (BYOD)

A situation in which employees use their own devices to perform work activities for Bicsma BV or connect to Bicsma BV's corporate network.

Compromise

A situation in which it has been confirmed that the security measures were breached, which (might) have led to an adverse impact on the confidentiality, integrity and availability of the device or the information stored thereon.

Third party

Person other than the owner or user of the device.

User

Employee of Bicsma BV or any other party who carries out work activities for Bicsma BV by using a mobile device and connects the device to Bicsma BV's corporate network.

Mobile device

Mobile device that can process electronic data and can be connected to a network. Examples of mobile devices include laptops, smartphones and tablets, as well as Google Glass, smart watches and media players. Mobile devices are referred to as "devices" or "mobile devices".

Passcode

A password, pass phrase or any other unit of knowledge that serves as a means of authentication and is used to prevent unauthorised access to a device or software. Passcodes also include graphic elements and swipe codes used as means of authentication.

PIN

A (generally) 4-digit numeric code used to gain physical access to a device.

2.3 Scope

This policy applies to all mobile devices that are not owned by Bicsma BV and that are used to establish a connection with the Bicsma BV corporate network.

2.4 Target group

All users of mobile devices shall comply with the provisions set out in this policy.

2.5 Policy

The use of mobile devices owned by employees and third parties and the connection of these devices to Bicsma BV's corporate network shall take place in such a way that the related risks to Bicsma BV's information assets are reduced to a minimum.

2.6 Provisions

The provisions set out below are based on Bicsma BV's strategic information security policy. This BYOD policy is not meant to replace but to supplement Bicsma BV's strategic information security policy.

This policy may be adjusted due to developments in the environment, the business operations, the legal and regulatory requirements, the architecture, etc. Minor adjustments to this policy require the information security process owner's approval. Major adjustments to this policy shall be submitted to the Management Team for approval. It is the information security process owner's responsbility to assess whether the adjustments proposed fall in the category of minor or major adjustments. In the event of a difference of opinions, the Management Team may be asked for advice.

Securing the device

Article 2.6.1

All passcodes shall comply with the provisions set forth in Bicsma BV's Password Policy.

PIN codes fall outside the scope of this provision. PIN codes shall consist of more than 4 digits. The use of PIN codes is mandatory. PIN codes may not contain values that coincide with the standard settings of the device.

Article 2.6.2

Sharing passcodes or PIN codes with third parties is strictly forbidden.

Article 2.6.3
In the event that the passcode or PIN code has been entered incorrectly 10 consecutive times, the device shall be wiped. In special cases and upon the Security Manager's approval, the device may be locked out after 10 failed login attempts. Lockouts shall be arranged in such a way that they can only be reset by the management organisation.

Article 2.6.4
The device shall be configured in such a way (hardening) that ensures the proper functioning of the available and applicable security measures.

Article 2.6.5
The device shall lock after 10 minutes of inactivity.

Article 2.6.6
Where applicable, the device shall be equipped with an antivirus, a firewall and a Mobile Device Management (MDM) software. The antivirus, firewall and MDM software are configured by the management organisation.

Article 2.6.7
The device's operating system and software shall be kept up to date. This also applies to antivirus software and firewalls. Updates shall be installed within a week after their publication, unless expressly stated otherwise by the management organisation.

Article 2.6.8
Unused ports and ports considered as insecure by the management organisation shall be blocked and disabled.

Article 2.6.9
Voicemails shall be protected by a passcode, a PIN code or another means of authentication. The passcode or PIN code may not coincide with the standard settings.

Article 2.6.10
Access shall be denied to all devices that fail to meet the requirements set out in this policy document.

Wi-Fi

Article 2.6.11
In order to protect the device against outside attackers, the network connection should be turned off when in disuse.

Article 2.6.12
Automatic connection to available wireless networks shall be disabled on the device.

Article 2.6.13
The use of Wi-Fi Protected Setup (WPS) is strictly forbidden and shall be disabled on the device.

Article 2.6.14
When on Bicsma BV premises, user shall connect directly to Bicsma BV's WLAN.

Article 2.6.15
Outside of Bicsma BV premises, user shall connect to the corporate network by using Bicsma BV's VPN environment. This provision does not apply to certain services available on the internet. These services, such as webmail, are listed by the management organsiation.

Article 2.6.16
With Bicsma BV's WLAN, the following types of keys may be used:

• WPA2 in Personal Mode with AES-CCMP

• WPA2 in Enterprise Mode with 802.1x

Data protection

Article 2.6.17
Mobile devices shall be used in compliance with the provisions set out in the Corporate Communications Policy and the Corporate Data Management Policy.

Article 2.6.18
All corporate information and data stored on BYOD devices are Bicsma BV's property. Users may only process this information and data insofar as deemed necessary for the performance of their work activities on behalf of Bicsma BV.

Article 2.6.19
Bicsma BV's information and data are classified into security categories. Users may only access, save, share, disseminate, process or delete data if the security category of the data expressly allows for these actions.

Article 2.6.20
A copy shall be made of all the corporate data generated or saved on mobile devices. The copies shall be stored on the logical storage media made available by the management organisation. In the event that such copies are not generated automatically, the user shall ensure that the relevant copies are stored on the media within one working day from the creation of the data.

Article 2.6.21
Corporate data saved on the device or shared electronically with the help of the device shall be encrypted. Users shall follow the management organisation's provisions on network protocols, algorithms, key length, securing keys and certificates.

Article 2.6.22
When using third-party network services (services provided by any other party than Bicsma BV), cryptographic protocols shall be used.[1]

Article 2.6.23
Locally saved passcodes and PIN codes shall be encrypted.

Article 2.6.24
Corporate data saved on the device may not be copied or stored on logical[2] and physical[3] storage media other than the data carries provided by Bicsma BV's management organisation.

Article 2.6.25
Mobile data carriers connected to the device shall be used in accordance with the provisions set out in Bicsma BV's Mobile Data Carrier Policy.

---

[1] Use HTTPS where available
[2] Network share, Cloud share, etc.
[3] Paper, media cards, etc.

Article 2.6.26
When travelling to countries where the government has the right to monitor devices, the user shall erase all corporate data from the device permanently and irretrievably. If this is not possible, the user may not take the device to that country.

Device management

Article 2.6.27
Only devices with an OS are granted access to the corporate network. The management organisation maintains a list of supported devices. The list can be found on the corporate Intranet.

Article 2.6.28
In order to protect Bicsma BV's information assets, the management organisation may adjust the configuration of the device's OS or adjust the applications that run on the device. This may include the installation of supplementary applications, patches and updates.

Article 2.6.29
Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

Article 2.6.30
Automatic backup to external environments (e.g. Dropbox or other Cloud Storage facilities) shall be disabled to prevent unauthorised access to corporate data.

Article 2.6.31
Bicsma BV reserves the right to wipe, reset or block the device if deemed necessary for the protection of corporate data. The user shall be aware that this might lead to the loss of user's private data stored on the device.

Article 2.6.32
Bicsma BV reserves the right to determine what applications and services may run on the device and wipe the device if deemed necessary for the protection of corporate data.

Article 2.6.33
In the event that a concrete risk can be reasonably assumed, Bicsma BV reserves the right to limit access to the websites specified by the management organisation.

Article 2.6.34
Bicsma BV reserves the right to block or remove applications that send data to other locations than the corporate network. This applies to applications sending location data, contact lists or memory data to the producer of the application or third parties.

Article 2.6.35
Bicsma BV shall not remove any application or data from the device unless deemed necessary.

Article 2.6.36
In the event that non-compliance with this policy is detected or the device is compromised, the management organisation denies access to the Bicsma network.

Article 2.6.37
In the event that non-compliance with this policy is detected or the device is compromised, the management organisation may wipe the device. The management organisation shall make every effort to consult the user prior to wiping the device, so that the user can secure his/her personal data stored

on the device. However, in situations where a concrete risk can be assumed and risk mitigation requires immediate action, the device may be wiped without consulting the user.

Article 2.6.38
Upon termination of employment, the management organisation shall wipe the device. Devices are wiped in consultation with the user so that the user can secure any personal data stored on the device.

Article 2.6.39
In the event of technical problems with the device or an application stored on the device, the management organisation only provides support to the user if the application was installed on the device by the management organisation. The management organisation provides support in the event that it can be reasonably concluded that the problems are due to the use of the device for Bicsma work purposes.

In the event that the user needs assistance, the user shall first review the available user manuals. Helpdesk shall be contacted in the event that the problem could not be solved by the user.

Behaviour and the use of devices

Article 2.6.40
User shall strive to keep corporate data and private data as separate as possible. User only stores corporate data on the device insofar as the data is needed for the work performed by user.

Article 2.6.41
User shall make every reasonable effort to protect the integrity of the device and the data stored on the device by taking appropriate security measures and avoiding risky behaviour.

Article 2.6.42
In addition to complying with the policies of Bicsma BV[4], user agrees to observe the current Best Practices for the safe use of Mobile Equipment and the Internet. This applies to use for work as well as use for private purposes.

Article 2.6.43
User may not use the internal storage capacity of the device or use any other logical or physical storage media made available by the management organisation as a backup facility for private data. In the event that the management organisation detects such use, it will delete any such private data.

Article 2.6.44
User shall refrain from any undesired behaviour as regards the use of the device or activities performed through the device. This includes harassment, physical or psychological pressure, intimidation, spying on or stalking of others, the breach of security measures, any activities that fall in the category of "hacking", and any unlawful acts.

Article 2.6.45
Users who are employees of Bicsma BV may not use the device to perform business activities for any other party than Bicsma BV.

Article 2.6.46
It is strictly forbidden to let third parties use the device or the accounts and profiles created on the device or used with the help of the device.

[4] Including but not limited to Bicsma BV's Acceptable Use Policy

Article 2.6.47
User may not impersonate other users by using the device. This includes that the creation and use of multiple accounts and profiles are strictly forbidden.

Article 2.6.48
Besides the applications installed or made available by the management organisation, the device may only use applications that have been determined as "secure" by the management organisation. [5]

Article 2.6.49
User may only install applications on the device that come from an "official" source. Official sources may include Google, Apple or Microsoft "App stores", the producer's website or App store, or Bicsma BV's Intranet.

Article 2.6.50
The device may not be used to install or store illicit applications, electronic books, multimedia files or any other content that might violate the rights of a copyright holder.

Article 2.6.51
User may only access systems, networks, network services, applications, user accounts or data in an appropriate manner.

Article 2.6.52
User shall report any (possibly) unsafe situation related to the device or Bicsma BV's network (services) to the helpdesk without undue delay. Unsafe situations include suspected or confirmed breaches of security measures and the loss or theft of the device. The same provision applies in the event that user replaces the device, or deletes or partially deletes or removes applications installed by the management organisation.

Article 2.6.53
Failure of the device, malfunction of the device or connectivity issues shall not relieve users from the proper performance of the tasks assigned to them by Bicsma BV.

Privacy

Article 2.6.54
Bicsma BV makes every effort to respect all users' privacy. Wherever possible without exposing Bicsma BV's information assets to unacceptable risks, BICSMA BV attempts to separate users' personal data and personal communications from corporate data and business communications. Wherever possible, security measures are confined to corporate data and business communications.

Article 2.6.55
In order to ensure compliance with this policy and verify the integrity of the device and the data stored on the device, Bicsma BV performs manual and automated checks and other types of monitoring activities. Checks are carreid out by the management organisation or other designated staff members. It is inevitable that these activities involve user's personal data. In the event that user refuses to subject

[5] The Management Organisation maintains a list of such secure applications on the Intranet. In case of doubt, User shall contact the helpdesk.

the device to such tests, Bicsma BV maintains the right to clear, reset or block access to the device to protect its corporate data and preserve the reliability of its information assets.

Article 2.6.56

In order to ensure compliance with this policy and verify the integrity of the device and the data stored on the device, Bicsma BV retains the right to log and monitor activities on the device and data exchange performed by using the device. Specific logging and monitoring activities aimed at a specific user or device take place solely in the event of suspicion of misuse of the device or violation of the provisions set out in this policy. This requires prior permission from the Security Manager and the Data Protection Officer. In such cases, Bicsma BV complies with the provisions set out in the EU General Data Protection Regulation.

Liability

Article 2.6.57

Bicsma BV is not liable for costs arising from the use of third-party networks. In special cases and on an individual basis, a manager may decide that such costs may be reimbursed. However, reimbursement is only considered in cases where access takes place via a VPN connection made available for this purpose and is used for activities that serve corporate interests.

Article 2.6.58

User shall bear all costs incurred by the purchase and / or use of applications or services other than those installed or prescribed by the management organisation.

Article 2.6.59

Bicsma accepts no liability, directly or indirectly, for damage caused by:

- Defects in the device or the software
- Loss of the device
- Loss of data or damage to data stored on the Device
- The performance of work by the Management Organisation
- Performing activities or other actions on the device
- Deleting, resetting or blocking the device
- Crashing of the device or software
- (Un) aware misuse of the device
- The presence of malware on the device
- Compromise of the device or the data stored on the device

3. Miscellaneous

3.1 Reservations

Product owners responsible for a service or application on behalf of Bicmsa BV may impose further restrictions and conditions on the use of mobile devices.

3.2 Document maintenance

This policy is reviewed twice a year by the information security process owner or a staff member delegated by the information security process owner. See Section 1.2 for the date of the next review. Proposed adjustments to the policy are treated the same way as adjustments to the strategic information security policy.