BRING YOUR OWN DEVICE POLICY

LISA

Version 4.0

19-10-2023

UNIVERSITY OF TWENTE.
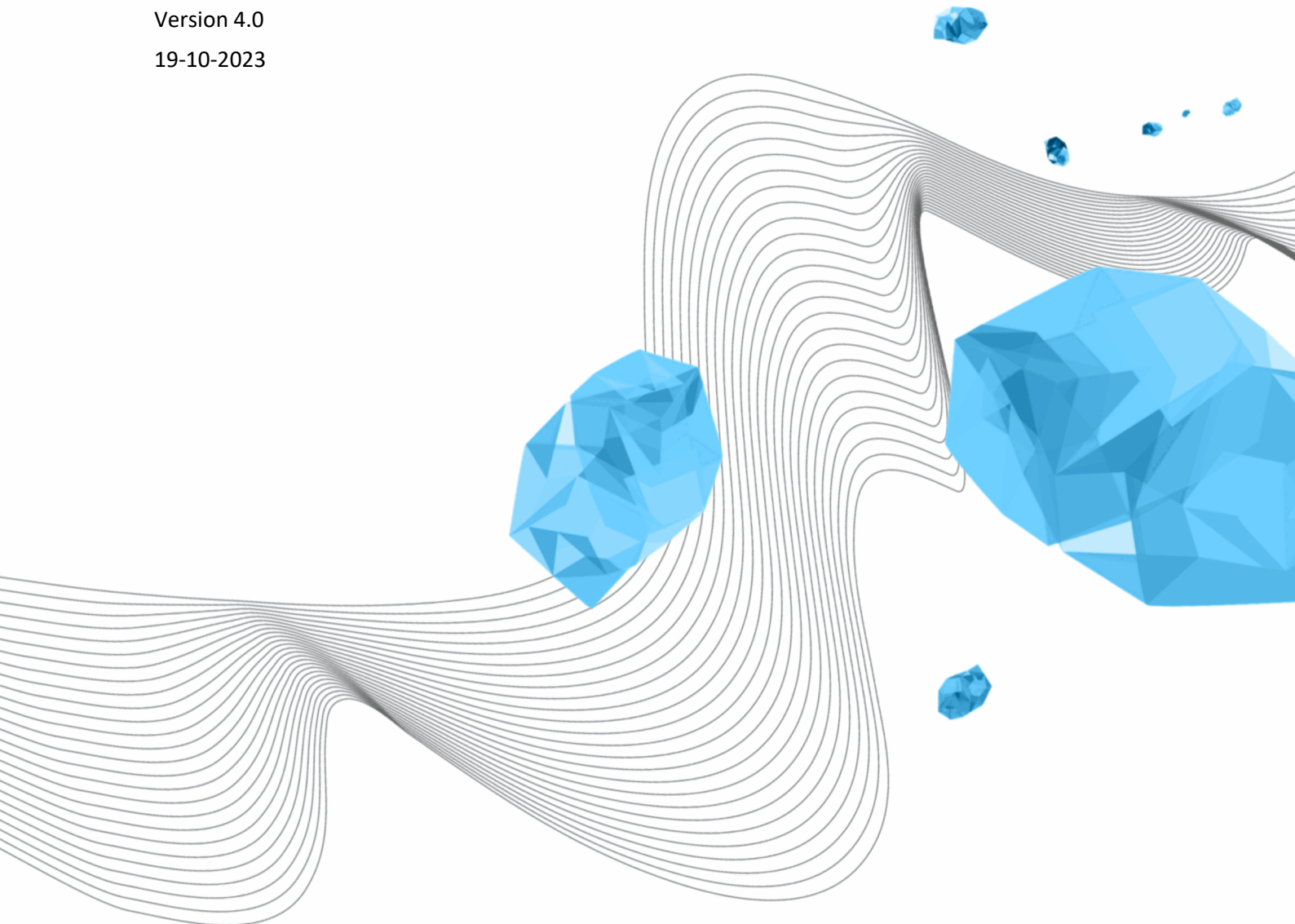
COLOPHON

ORGANIZATION
Library, ICT Services & Archive

TITLE
Bring your own Device Policy

REFERENCE
LISA-389

VERSION (STATUS)
4.0

DATE
19-10-2023

AUTHOR(S)
Henk Swaters

COPYRIGHT
© University of Twente, The Netherlands.

DOCUMENTHISTORIE

VERSION	DATE	AUTHOR(S)	COMMENTS
2.0	23-06-2023	H.W.Swaters	Review MT-LISA, UCM
3.0	08-09-2023	H.W.Swaters	Feedback processed
4.0	19-10-2023	H.W.Swaters	Preventing binding license agreements

DISTRIBUTIELIJST

VERSION	DATE	AUTHOR(S)	DISTRIBUTED TO
2.0		H.W.Swaters	
4.0	24-11-2023	H.W. Swaters	Published on Cyber Security website

TABLE OF CONTENTS

1   INTRODUCTION

Employees, students and external parties often use their own equipment for their work or study. This equipment is called Bring Your Own Device (BYOD). With this BYOD, students, staff and external parties will then have access to information, ICT services and applications from the University of Twente. This raises questions about the desired assistance and the necessary security of BYOD. The consequences for the UT are formulated in this policy.

This policy is in addition to the existing policies. For everyone who uses information, ICT services and applications from the University of Twente, the Information Security Policy is applicable, which means that the basic security measures from the information security policy must be applied to the BYOD. The privacy policy, the codes of conduct and the health and safety policy also apply, regardless of whether a UT device or BYOD is used. *Additionally, the "Own Applications" policy applies if the system is used for business purposes.*

Use of BYOD is only permitted with a personal account of the UT. You may not use an administrative account or an account with administrative rights on a BYOD. It is also not permitted to use or store sensitive or personal data of the UT on a BYOD.

When using a BYOD, (security) measures can be applied to the device. For example, the hard drive can be automatically encrypted or remote erasure can be made possible. The device's owner accepts these measures and implications by using a BYOD.

2   GENERAL

1. For employees, a laptop or desktop managed by LISA is made available with the proper security measures, ideally suited as a workplace computer for most employees.
2. Use of BYOD is only permitted with a personal account of the UT. You may not use an administrative account or an account with administrative rights on a BYOD. It is also not permitted to use or store sensitive or personal data of (employees of) the UT on a BYOD. An exception is the use of the mailbox, as long as the device is adequately secured and used safely (see the university's information security policy and password policy).
3. For everyone who uses information, ICT services and applications of the University of Twente, the Information Security Policy, the Privacy Policy, the Codes of Conduct, policy 'Use of personal applications' and the Working Conditions Policy apply, regardless of whether a UT device or BYOD is used.
4. The information security policy contains the minimum security measures that also apply to the BYOD used for work and study.
5. Concerning the purchase of equipment for employees, obligations under European tenders apply. This can only be deviated from with good reasons.
6. Working with your personal equipment can entail risks to working conditions. Employees must discuss this with their supervisor and are supported by HR through information on the HR website and the efforts of the Occupational Health and Safety coordinators.
7. In securing the UT network, LISA takes into account that the equipment used may not be guaranteed to be free of malware.
8. For the use of web applications in the back office of various administrative processes, it is assumed that the employee has a managed standard workstation.

9. For the use of web applications that are part of the front office of various administrative processes, standards are the starting point. This means that users can expect the web applications to work with their device and browser.

10. If an education program has requirements for the hardware or software that students must have access to, this is communicated to the students well in advance, similar to the way information about purchasing books is provided.

3   COSTS AND FEES

11. The University does not reimburse private equipment purchases or damage caused to personal devices due to business use. This also includes costs arising from security measures, such as remote wiping.

4   SUPPORT

12. Support is provided via manuals on the UT service portal, accessible to users, for:
    a. being able to use the wireless network and VPN,
    b. the use (via a secure connection) of e-mail and to synchronize their agenda,
    c. how (via a secure connection) user data (e.g. on network drives) can be accessed.

13. Support is provided via manuals on the UT service portal.

14. The Educational Services (CES-CELT) provides information on its website about how and which equipment, applications, and cloud services can be effectively used in education.

15. Employees can choose to use private purchases for UT purposes; this does not entail any obligations for the UT.

16. If defective (parts of) private equipment are defective, the user is referred to their supplier for repair and warranty.

5   RESEARCH

17. LISA must advise if a research project makes different choices about the equipment to be used.

6   REVIEW OF THIS POLICY

This policy will be reviewed at least every three years. The following review will be in mid-2026. There may be grounds for an interim evaluation. If that evaluation gives cause to do so, the policy will be adjusted sooner.

The CISO of the University of Twente is responsible for this policy.

MT-LISA determines this policy.