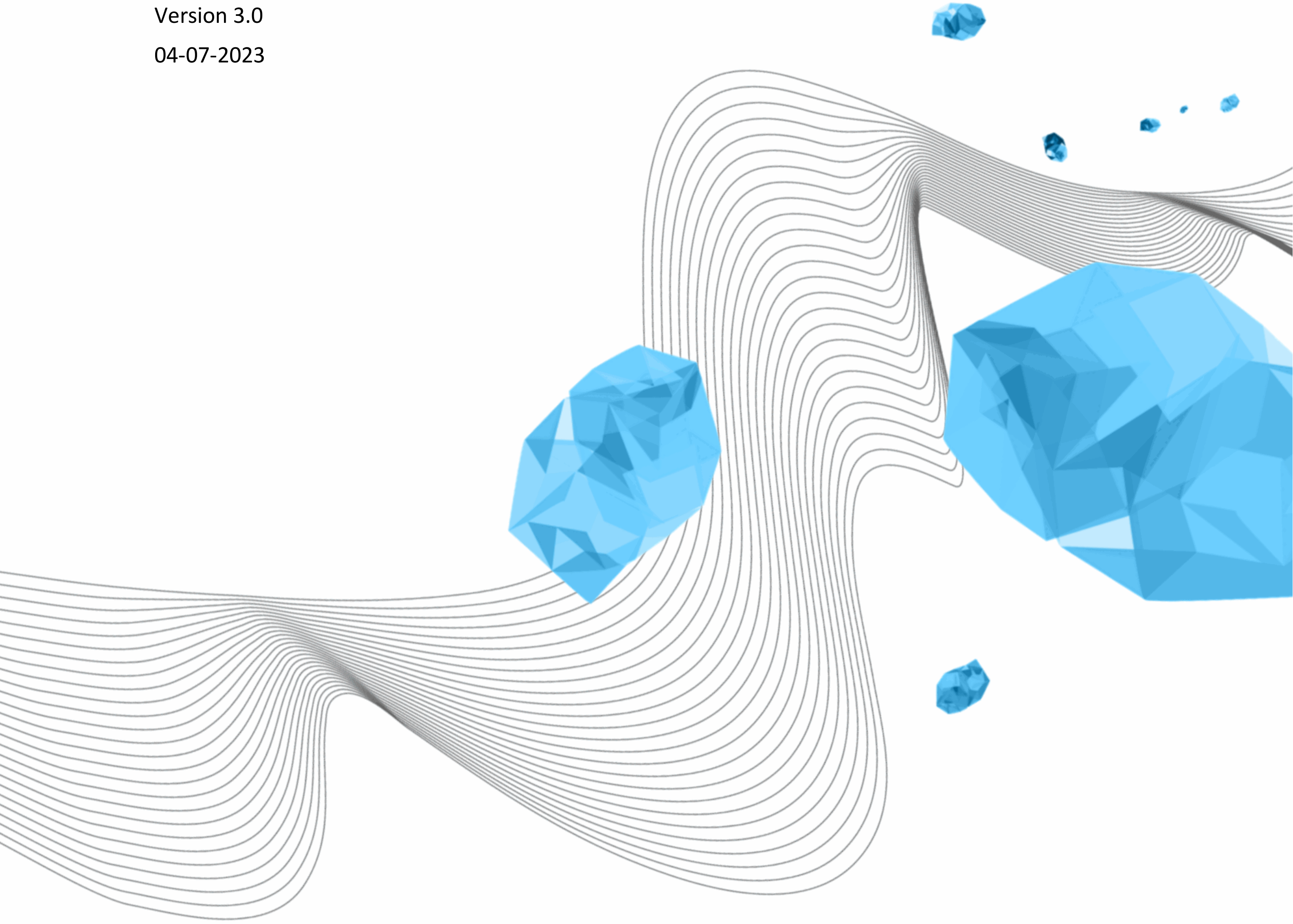
LIBRARY, ICT SERVICES & ARCHIVE

Status: Definitief
Date of adoption by MT-LISA: 10-07-2023
Reviewed: 04-07-2023
Author: Peter Peters

RESPONSIBLE DISCLOSURE POLICY

LISA
Version 3.0
04-07-2023



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
Responsible Disclosure Policy

REFERENCE
LISA-0388

VERSION (STATUS)
3.0

DATE
04-07-2023

AUTOR(S)
Peter Peters

COPYRIGHT
© Universiteit Twente, Nederland.

DOCUMENT HISTORY

VERSION	DATE	AUTOR(S)	REMARKS
3.0	04-07-2023	P.G.M. Peters	Rewritten to adhere to the standard format. Added Out of Scope chapter Added Bounty chapter

DISTRIBUTION LIST

VERSION	DATE	AUTOR(S)	DISTRIBUTED TO
3.0	10-7-2023	P.G.M. Peters	LISA-MT

REFERENCES

VERSION	DATE	AUTOR(S)	TITLE
2.0	2-10-2017	Rianne te Brake	Responsible Disclosure University of Twente

Content

1 INTRODUCTION

What Is Responsible Disclosure? Responsible disclosure, or coordinated vulnerability disclosure, is when security researchers or ethical hackers discover vulnerabilities, weaknesses, or flaws in software, hardware, or systems and report them to the affected organisation or vendor.

The University of Twente considers the security of your and our data very important, which is why we protect our systems. Despite our efforts, a weakness could still occur in these systems.

If you have found a vulnerability in one of our systems, please let us know so we can take measures immediately. We want to work with you to protect our users and systems better.

This policy applies to all systems and applications owned, maintained and operated by the University. This policy does not apply to systems and applications the University has no responsibility over, including systems owned by students, student associations and third parties on the University's network.

2 WHAT WE PROMISE YOU

- We feel it is essential that vulnerabilities are reported to us as soon as possible so that we can take immediate action to secure our environment. All notifications will, therefore, always be gratefully received. We will not consider any legal steps against those who notified us and gained unauthorised access to sensitive information if they have complied with the points in Chapter 3.
- We will treat your notification with confidentiality and will not share your personal details with third parties without your consent unless necessary to comply with a statutory obligation.
- We will respond to your notification within five working days with our assessment of your report.
- We can inform you of our progress in resolving the issue.
- We can publish the relevant content of the resolved issue on our website unless there are reasons not to do so. That might be the case if the fixed issue has led to discovering a related vulnerability that has not yet been resolved or when publication could damage the University's reputation.
- In publishing the resolved issue, we will credit you, if you wish, as the person who discovered and reported it.

3 WHAT WE ASK OF YOU

To be eligible for the promises in Chapter 2, you must obey the following rules.

- Do not attack physical security or people (social engineering).
- Do not use any form of Distributed Denial of Service attacks.
- Do not report run-of-the-mill issues.
  We have published examples on our Responsible Disclosure website.
- Email your findings to responsible-disclosure@utwente.nl.
  Submitting a notification under a pseudonym is allowed. If you feel the data is so

sensitive that you wish to encrypt it, we ask you to notify us beforehand. We will then provide you with an email address to which you can send your PGP encrypted email.

- Provide sufficient information to reproduce the issue so we can resolve it immediately. In most cases, providing the IP address or URL of the affected system and a description of the vulnerability will suffice. Still, more information may be necessary in the case of complex vulnerabilities.
- Delete all confidential information obtained through the breach as soon as possible after reporting it, but always after consulting us to ensure we can reproduce the issue.
- Do not misuse the problem by downloading more data than necessary to demonstrate the breach. Do not inspect, remove or alter third-party data.
- Do not share the issue with others until it has been resolved.
- Do not publish anything about the resolved issue unless this has been discussed with us.

4 OUT OF SCOPE

We do not reward trivial vulnerabilities or bugs that can not be abused. An up-to-date list of examples is available on the Cyber Safety website, https://www.utwente.nl/en/cyber-safety/responsible/.

5 BOUNTY

The University does not provide a monetary bounty.

We can, however, add your name to our Hall of Fame with a link to your online profile. This only applies to the first person reporting a specific vulnerability.

6 REVIEW OF THIS POLICY

This policy will be reviewed at least every five years. The following review will be in mid-2028. 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.