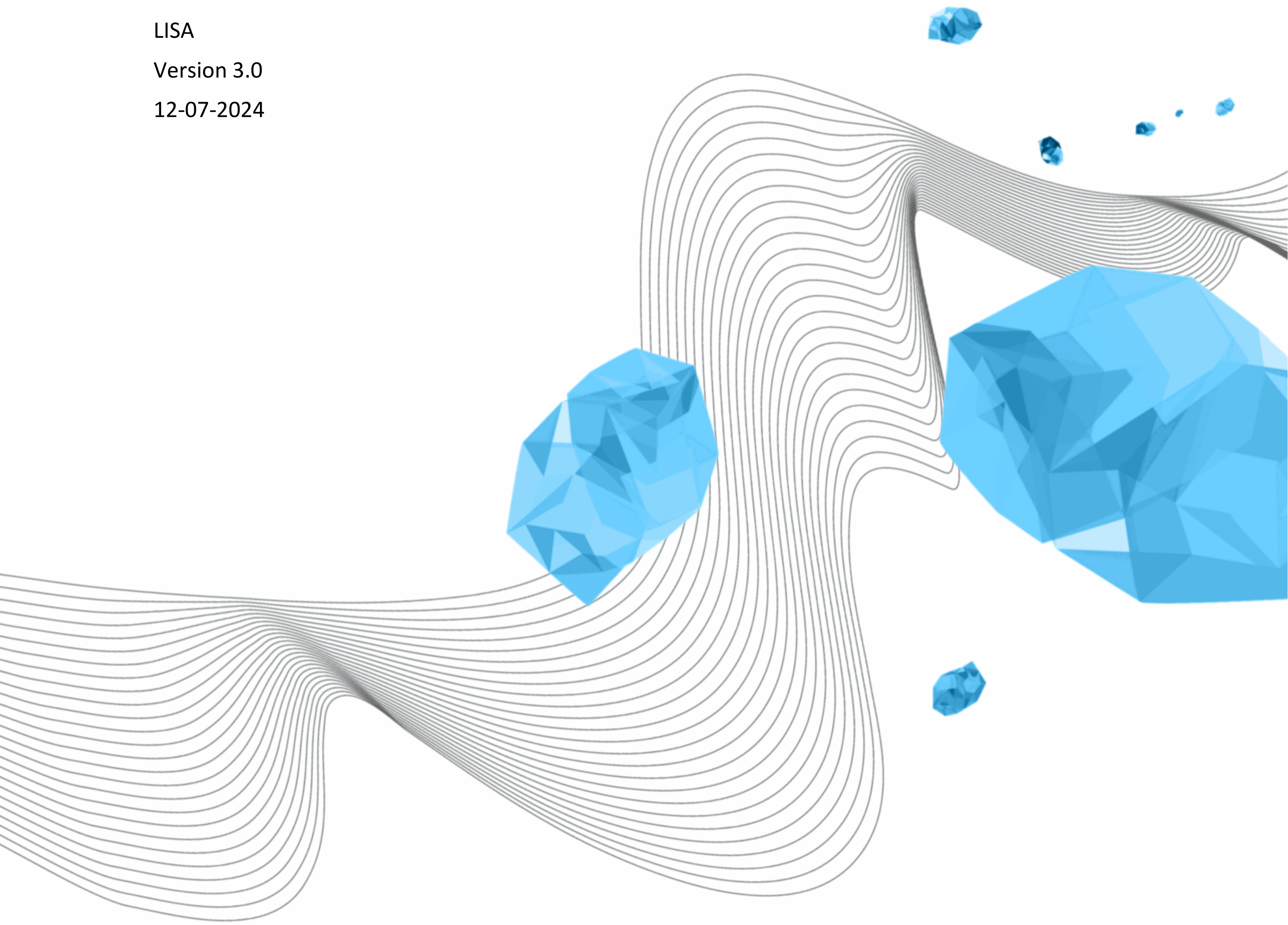
Status: Approved
Date of adoption by MT-LISA: 08-07-2024
Reviewed: 04-07-2024
Author: Henk Swaters

PATCH MANAGEMENT GUIDELINES UNIVERSITY OF TWENTE

LISA
Version 3.0
12-07-2024



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
Patch Management Guidelines University of Twente

REFERENCE
LISA-394

VERSION (STATUS)
3.0

DATE
12-07-2024

AUTHOR(S)
Henk Swaters

DOCUMENT HISTORY

VERSION	DATE	AUTHOR(S)	COMMENTS
3.0	12-07-2024	P.G.M. Peters	Translated

DISTRIBUTIELIJST

VERSION	DATE	AUTHOR(S)	DISTRIBUTED TO
3.0	15-07-2024	H.W.Swaters	UT Website

REFERENCES

VERSION	DATE	AUTHOR(S)	TITLE
3.0	04-07-2024	Henk Swaters	Patchmanagementrichtlijn Universiteit Twente

TABLE OF CONTENTS

1 INTRODUCTION

The patch management guideline of the University of Twente (UT) describes the measures and procedures for effective implementation of patch management. This guideline is per the information security policy of the central government, the Code for Information Security (NEN/ISO 27002:2007) and the National Service Information Security Baseline (BIR). See the attachment for details.

2 PATCH MANAGEMENT

A patch (fix, hotfix) is an update that updates part of the software to fix a bug or error discovered after release. This patch management guideline focuses on patches that resolve Availability, Integrity and Confidentiality (BIV) vulnerabilities. This patch management guideline does not cover updates or upgrades that only add new functionality unless they contain patches.

The UT emphasises the importance of patch management because failure to do so increases the vulnerability of systems. This guideline applies to all employees managing hardware and software within the UT organisation.

3 PATCH MANAGEMENT CYCLE

3.1 RECEIPT AND ASSESSMENT

Once a new patch is available, the IT management team must document and review it.

3.2 IMPACT ANALYSIS

Perform an impact analysis to determine how the patch may affect existing functionalities and systems.

3.3 TEST ENVIRONMENT

If possible, first run the patch in a separate test environment.

3.4 FALLBACK OPTIONS

Have a detailed rollback plan if the patch causes problems in the production environment.

4 MEASURES

The following measures have been established for the UT:

4.1 TECHNICAL INTEGRITY

The technical integrity of program packages and infrastructure software is checked utilising a signature or hashing mechanism and a checksum from the supplier, obtained through a trusted channel. A reliable mechanism such as Puppet or Windows Update can do this automatically.

4.2 RISK EVALUATION

The risks associated with installing a patch should be evaluated if a patch is available. If the risk of misuse and damage is low, the patch can be scheduled for the next maintenance round of the system. If the risk of misuse or damage is high, the patch will be carried out urgently.

4.3 TESTING AND ROLLBACK

All patches should be tested before installation, but for system software where the vendor provides reliable and tested patches, evaluation and testing can be skipped if there is a mechanism to roll back an errant patch.

4.4 EMERGENCY PATCHES

Emergency patches (there is a known exploit or a high-security risk) are addressed as quickly as possible but no later than within one day. If this is not possible, for example, because the rollout is not feasible or takes too much time, adequate mitigating measures will be taken in consultation with the system owner.

4.5 AUTOMATED PATCH MANAGEMENT TOOLS

Automated patch management tools such as Microsoft MECM, WSUS, Jenkins, or other CI/CD pipelines can be used to streamline the patching process.

Ensure these tools are up to date and properly configured to manage all relevant systems and applications.

4.6 COMMUNICATION AND DOCUMENTATION

Clearly communicate planned patch activities to all stakeholders, including expected downtime and user impact.

Document all steps of the patching process, including the results of impact analysis, testing, and final implementation.

Document which patches were applied to which systems and when.

4.7 CHANGE MANAGEMENT

Coordinate implementation and approval according to existing change processes.

5 RESPONSIBILITIES

5.1 IT ADMINISTRATOR (RESPONSIBLE FOR EXECUTION)

- Execute patch management guidelines promptly and adequately for systems under their administration.
- Periodically provide an evaluation of the implementation of the patch management cycle and indicate areas for improvement.
- In the case of emergency patches, where the rollout is not possible or takes too much time, adequate mitigation measures must be taken in consultation with the system owner.

5.2 MANAGER OF IT ADMINISTRATOR (PROCESS RESPONSIBLE)

- Ensure that the patch management guideline is implemented promptly and adequately.
- Ensure all IT administrators and developers know patch management procedures and tools.
- Organise periodic training to share best practices in patch management and raise awareness.

5.3 SYSTEM OWNER (ULTIMATELY RESPONSIBLE FOR THE APPLICATION OF PATCHES)

- Have an impact analysis performed to understand the possible consequences of the patch on the existing functionalities and the system's stability.
- In consultation with the IT management team and security management, decide which patches should be applied and when.

5.4 SECURITY MANAGEMENT (MONITORING AND AUDITS)

- Regularly monitor, assess or audit to ensure all patches have been applied correctly and that the patch management process is being followed.
- Document any deviations and corrective actions.
- Prepare periodic reports on patch management status, including statistics on patches applied, outstanding patches, and compliance status.
- May decide to designate a patch as an emergency patch in urgent cases.

6 REVIEW OF THIS POLICY

This guideline is reviewed annually to ensure it remains current with the latest security standards and practices. The following review will take place in mid-2025. There may be grounds for an interim evaluation. If this evaluation gives reason to do so, the guideline will be amended sooner.

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

MT-LISA establishes these regulations.