n

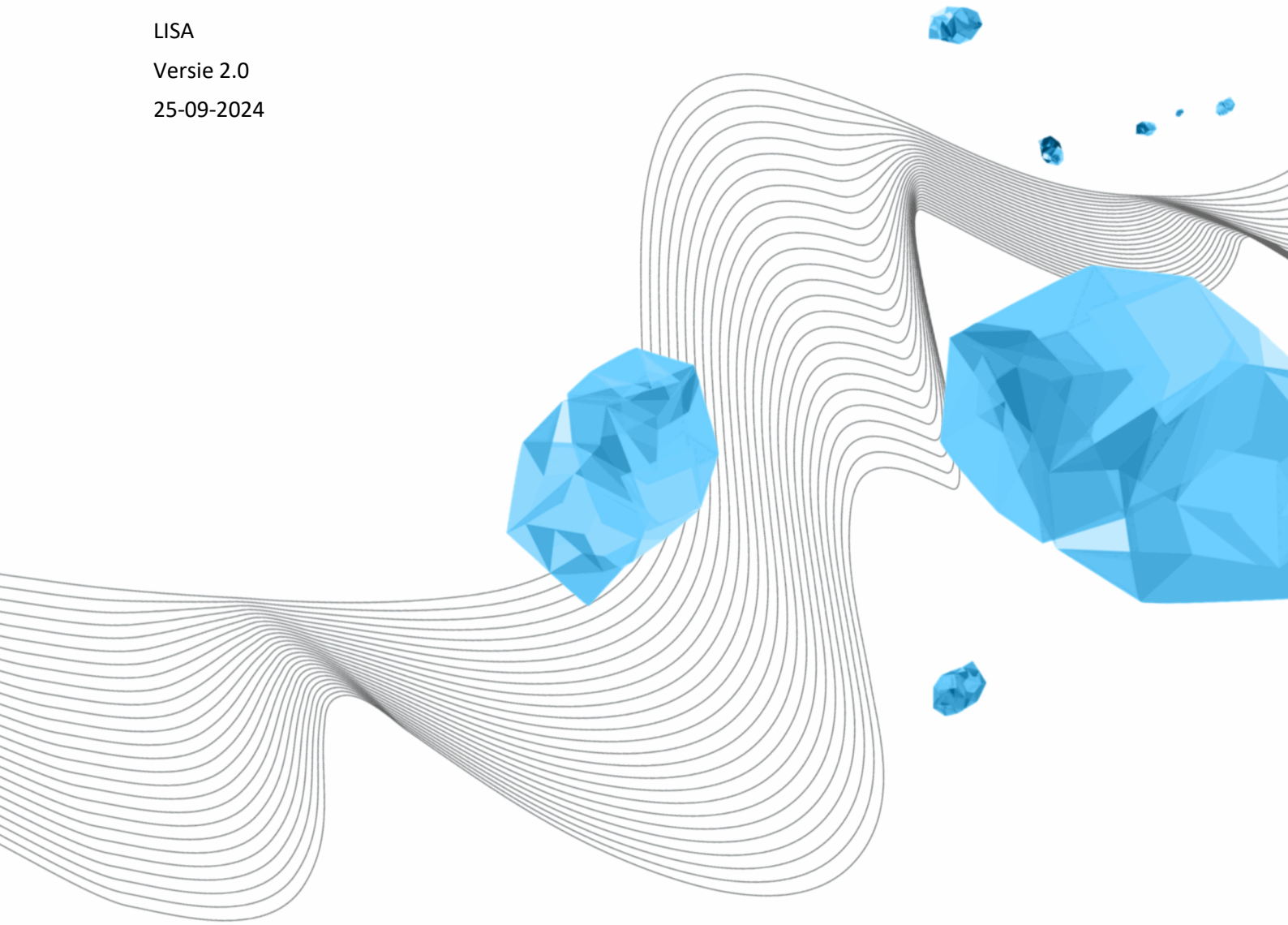
Status: Definitief versie 2.0
Datum vastgesteld door MT-LISA: 11-11-2024
Auteur: Henk Swaters

# BEHEER- EN BEVEILIGINGSKADERS VOOR WERKPLEKSYSTEMEN

LISA

Versie 2.0

25-09-2024



UNIVERSITY OF TWENTE.

# COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Beheer- en Beveiligingskaders voor Werkpleksystemen

KENMERK
LISA-xxx

VERSIE (STATUS)
2.0

DATUM
25-09-2024

AUTEUR(S)
Henk Swaters



# DOCUMENTHISTORIE

| VERSIE | DATUM | AUTEUR(S) | OPMERKINGEN |
|---|---|---|---|
| 0.1 | 13-09-2024 | H.W.Swaters | Initiële versie |
| 0.2 | 17-09-2024 | H.W.Swaters | Feedback verwerkt |
| 1.0 | 25-09-2024 | H.W.Swaters | Feedback verwerkt |
| 2.0 | 23-10-2024 | H.W.Swaters | FAQ toegevoegd |

# DISTRIBUTIELIJST

| VERSIE | DATUM | GEDISTRIBUEERD AAN | OPMERKING |
|---|---|---|---|
| 0.1 | 13-09-2024 | Afdelingshoofd CS, Teamleider CS, Dir. LISA, Accountmanagers LISA | Feedback gevraagd |
| 0.2 | 17-09-2024 | Afdelingshoofd CS, Teamleider CS, Dir. LISA, Accountmanagers LISA | Feedback gevraagd |
| 1.0 | 25-09-2024 | MT-LISA | Feedback gevraagd |
| 2.0 | 23-10-2024 | MT-LISA | Ter vaststelling |

# INHOUDSOPGAVE

1 Inleiding ..... 4
2 Definities: ..... 4
3 kaders ..... 4
4 Review van de kaders ..... 5
5 FAQ ..... 5

# 1 INLEIDING

Het beheer en de beveiliging van werkpleksystemen aan de Universiteit Twente (UT) is van essentieel belang voor het waarborgen van de informatieveiligheid en het ondersteunen van de dagelijkse werkzaamheden van medewerkers.

Het gebruik van niet-beheerde of verouderde systemen, evenals het niet tijdig inleveren van apparatuur, kan leiden tot beveiligingsrisico's en operationele inefficiënties. Daarnaast leidt de toenemende vraag naar ondersteuning van verouderde of niet-gestandaardiseerde systemen tot voor de UT ongewenste en te voorkomen beheer.

Om deze risico's te beheersen en de noodzakelijke ondersteuning te minimaliseren, stelt de UT deze kaders vast. Dit richt zich op het waarborgen van een gestroomlijnd beheer van werkpleksystemen, waarbij zowel de veiligheid als de efficiëntie worden gewaarborgd. Door heldere kaders te scheppen rondom het gebruik, de inlevering, en het beheer van werkpleksystemen kunnen onnodige herinstallaties of reparaties van verouderde hardware te voorkomen.

# 2 DEFINITIES:

| | |
|---|---|
| UT-werkpleksysteem | Werkplekdevice voor generieke ICT taken welke door de UT aangeschaft is en waar informatie van de UT op verwerkt wordt. Dat kan bijvoorbeeld een desktop, laptop, smartphone of tablet zijn. |

# 3 KADERS

Deze kaders zijn aanvullend op het bestaande informatiebeveiligingsbeleid, -gedragscodes en richtlijnen. Deze kaders richten zich op UT-werkpleksystemen.

1. **Geen herinstallatie van verouderde systemen**: Systemen die technisch verouderd zijn, worden niet opnieuw geïnstalleerd.
2. **Geen reparatie buiten garantie**: Hardware van systemen die buiten de garantie vallen, wordt niet gerepareerd. Dit geldt ook voor uitbreidingen van hardware.
3. **Herinstallatiegrens op 5 jaar**: Systemen ouder dan 5 jaar komen niet meer in aanmerking voor herinstallatie als ze voldoen aan de voorwaarden uit punt 1 en/of 2.
4. **Gegevensbeheer**: Er staat geen cruciale data op de harde schijf van een werkpleksysteem, tenzij deze ook veilig is opgeslagen op een netwerkschijf. Dit verkleint het risico bij verlies of diefstal.
5. **Inlevering van oude systemen**: Tijdens de uitlevering van een systeem wordt het oude systeem altijd ingeleverd, ongeacht de staat of data die nog op het apparaat staat.
6. **Centraal beheer en beveiliging**: Alle werkpleksystemen worden centraal beheerd en voldoen aan de gestelde beveiligingsmaatregelen van de UT.

7. **Isolatie van onveilige systemen**: Werkpleksystemen die niet voldoen aan de beveiligingsmaatregelen van de UT en die een risico vormen, worden onmiddellijk van het netwerk geïsoleerd totdat ze aan de eisen voldoen of worden vervangen.
8. **Handhaving bij uitdiensttreding**: wanneer medewerkers uit dienst gaan wordt UT-appatuur ingeleverd.
9. **Bewustwordingscampagnes**: Regelmatige bewustwordingscampagnes onder medewerkers over de risico's van niet-beheerde systemen en het belang van tijdige inlevering en beveiliging van apparatuur.
10. **Inventarisatie en monitoring**: Er wordt door LISA periodiek een inventarisatie uitgevoerd van alle werkpleksystemen binnen de UT om te controleren of deze voldoen aan de security-eisen en hierover aan de CISO gerapporteerd.

# 4 REVIEW VAN DE KADERS

Deze kaders wordt minimaal iedere drie jaar herzien. De volgende herziening vindt plaats medio 2027. Er kunnen reden zijn voor een tussentijdse evaluatie. Als die evaluatie er aanleiding toe geeft zal het beleid eerder worden aangepast.

De CISO van de Universiteit Twente is verantwoordelijk voor de kaders.

Kaders worden vastgesteld door MT-LISA.

# 5 FAQ

**Wat wordt precies bedoeld met "technisch verouderd" in punt 1?**

Een systeem wordt als "technisch verouderd" beschouwd wanneer het niet langer wordt ondersteund door de fabrikant met beveiligingsupdates of nieuwe software-updates. Dit kan variëren per type systeem, maar over het algemeen houdt het in dat het systeem niet langer voldoet aan de vereiste beveiligingsstandaarden.

**Wat gebeurt er met systemen die ouder zijn dan vijf jaar maar nog steeds functioneren?**

Systemen ouder dan vijf jaar komen niet meer in aanmerking voor herinstallatie of reparatie, tenzij ze voldoen aan specifieke voorwaarden (bijvoorbeeld als ze nog binnen de garantie vallen). Als het systeem functioneel is maar niet meer voldoet aan de beveiligingsstandaarden, zal vervanging sterk worden aanbevolen.

**Hoe wordt bepaald of een systeem buiten de garantie valt?**

De garantieperiode van systemen wordt centraal bijgehouden in een registratiesysteem. Dit wordt beheerd door de IT-afdeling (LISA). Gebruikers kunnen contact opnemen met LISA om de garantie van hun systeem te controleren. Daarnaast geldt dat de UT geen systemen zonder garantie aanschaft.

**Kunnen er uitzonderingen worden gemaakt voor hardware buiten de garantie?**

Nee, er worden geen systemen zonder garantie aangeschaft. Dit geldt ook voor Apple-producten, die verplicht via LISA en de afdeling Inkoop worden aangeschaft.

**Hoe wordt gecontroleerd of er data op de harde schijf van werkpleksystemen staat?**

Het beheer en de controle van de gegevensopslag op werkpleksystemen is de verantwoordelijkheid van de gebruiker, niet van LISA. Gebruikers moeten ervoor zorgen dat cruciale data veilig is opgeslagen op een netwerkschijf of in de cloud, om risico's bij vervanging, herinstallatie, verlies of diefstal te minimaliseren.

**Wat zijn de gevolgen als blijkt dat data niet correct is opgeslagen?**

LISA controleert hier niet op. Bij vervanging, herinstallatie, verlies of diefstal is LISA niet aansprakelijk voor de schade.

**Wat gebeurt er als een medewerker een oud systeem niet inlevert bij de uitlevering van een nieuw systeem?**

Het niet inleveren van een oud systeem kan leiden tot vertragingen bij het ontvangen van een nieuw systeem. Er zal contact worden opgenomen met de medewerker om het apparaat alsnog in te leveren. Als de medewerker niet reageert, kan dit worden geëscaleerd naar het management.

**Hoe wordt omgegaan met gegevens die nog op een ingeleverd apparaat staan?**

Oude systemen worden volledig gewist volgens de beveiligingsrichtlijnen. Medewerkers worden geadviseerd belangrijke gegevens tijdig te verplaatsen naar een netwerkschijf of cloudopslag voordat ze het systeem inleveren.

**Welke tools worden gebruikt voor het centrale beheer van werkpleksystemen?**

Alle door LISA beheerder werkpleksystemen worden beheerd via een centraal beheersysteem (zoals Defender ATP, SCCM of Intune) dat door LISA wordt gemonitord. Dit systeem zorgt voor automatische software-updates, beveiligingspatches, bescherming tegen malware en inventarisatie van hardware.

**Wat gebeurt er met systemen die tijdelijk offline zijn en daardoor niet centraal beheerd kunnen worden?**

Systemen die langere tijd offline zijn, worden als een potentieel beveiligingsrisico beschouwd. Als een systeem langer dan drie maanden offline is geweest, kan het niet meer goed functioneren wanneer het opnieuw wordt ingeschakeld. Het is daarom belangrijk dat systemen niet langer dan drie maanden uit staan, anders kan LISA actie ondernemen om het systeem onbruikbaar te maken, op afstand te wissen of te vervangen.

**Hoe wordt bepaald of een systeem een beveiligingsrisico vormt en wordt geïsoleerd?**

Systemen worden als een risico beschouwd als ze niet voldoen aan de minimale beveiligingseisen, zoals verouderde software, ontbrekende beveiligingspatches of verdachte netwerkactiviteiten. Deze systemen worden direct geïsoleerd van het netwerk totdat ze worden geüpdatet of vervangen.

**Hoe snel kunnen geïsoleerde systemen weer op het netwerk worden aangesloten?**

Zodra een geïsoleerd systeem voldoet aan de beveiligingseisen, kan het direct weer worden aangesloten. Dit gebeurt soms na een grondige controle en het toepassen van de nodige updates door LISA.

**Hoe wordt ervoor gezorgd dat uitdiensttredende medewerkers alle apparatuur inleveren?**

Er is een formeel (off-boarding)nproces waarbij medewerkers verplicht zijn om alle UT-apparatuur in te leveren bij het beëindigen van hun dienstverband. Dit wordt gecontroleerd door de leidinggevende. Medewerkers die apparatuur niet inleveren, kunnen worden geconfronteerd met administratieve stappen of kosten.

**Wat gebeurt er als apparatuur verloren gaat of niet kan worden ingeleverd?**

In het geval van verlies of diefstal wordt er verwacht dat de medewerker dit onmiddellijk bij CERT-UT meldt. Er kan een onderzoek worden gestart, en er kunnen kosten in rekening worden gebracht als blijkt dat de medewerker nalatig is geweest.

**Wat houdt de "regelmatige bewustwordingscampagne" precies in?**

Dit zijn campagnes gericht op het vergroten van het bewustzijn onder medewerkers over IT-beveiliging, het belang van tijdige inlevering van apparatuur, opslag van bestanden, en het naleven van beveiligingsrichtlijnen. Deze campagnes worden via e-mails, workshops en online trainingen uitgevoerd.

**Hoe vaak vinden deze bewustwordingscampagnes plaats?**

De bewustwordingscampagnes worden minimaal eens per twee jaar georganiseerd, maar kunnen vaker plaatsvinden afhankelijk van de noodzaak, zoals na een beveiligingsincident of de introductie van nieuwe richtlijnen.

**Hoe wordt de effectiviteit van bewustwordingscampagnes gemeten?**

De effectiviteit wordt gemeten via phishingtests en het monitoren van naleving van IT-beleid. Incidenten met betrekking tot niet-beheerde systemen of niet-ingeleverde apparatuur worden gerapporteerd en geanalyseerd om verbeteringen door te voeren. Het beleid is er op gericht om alle computer apparatuur door LISA te laten beheren.

**Hoe wordt de inventarisatie van werkpleksystemen uitgevoerd?**

De inventarisatie wordt periodiek uitgevoerd door LISA via een centraal beheersysteem dat automatisch alle werkpleksystemen controleert op beveiligingseisen en hardware-status. Eventuele afwijkingen worden gerapporteerd aan de CISO.

**Wat gebeurt er als een systeem niet voldoet aan de security-eisen?**

Als een systeem niet voldoet, wordt het ofwel direct geüpdatet, geïsoleerd, of vervangen. Gebruikers worden hierover geïnformeerd en moeten actie ondernemen om aan de eisen te voldoen. In het geval van hardnekkige weigeren kan het systeem permanent worden verwijderd uit het netwerk.

**Welke actiepunten volgen uit de rapportages van LISA aan de CISO?**

De CISO ontvangt regelmatig rapportages over de status van werkpleksystemen en kan daarop actie ondernemen, zoals het aanscherpen van beveiligingsbeleid, het organiseren van extra bewustwordingssessies, of het prioriteren van specifieke risicogebieden binnen de UT.