RenRøros
Digital as

Informasjonssikkerhet

Os kommune 09.06.2021

Vidar Kojan Grind – Avdelingsleder
Tølløv Tamnes – Senior Systemkonsulent

RenRøros
Digital as

Informasjonssikkerhet Ren Røros

Hva er et sikkerhetsbrudd?

- **Konfidensialitet:** Uvedkommende får innsyn i beskyttelsesverdig informasjon.
- **Integritet:** Informasjon og systemer endres, skades eller slettes på uautoriserte eller utilsiktete måter.
- **Tilgjengelighet:** Informasjon og systemer går tapt eller er utilgjengelige når behovet er der.

Eksempler på sikkerhetsbrudd som du må varsle

- feilutlevering eller -publisering
- mistet utstyr (mobil, laptop, nettbrett, notater og lignende)
- feil i tilganger, utstyr eller programvare som kan svekke sikkerheten
- rutiner som mangler, ikke fungerer eller som ikke følges
- mistanke om hacking
- passord på avveie

RenRøros
Digital as

Informasjonssikkerhet Ren Røros

En kanal for varsling av avvik!

Kundesenter:

E-post til helpdesk.digital@renroros.no

Telefon: 724 14 860

Kundesenter og driftssenter vil følge opp hendelsen sammen med virosafe.

RenRøros
Digital as

Informasjonssikkerhet Ren Røros

4 viktigste tiltaks områder:

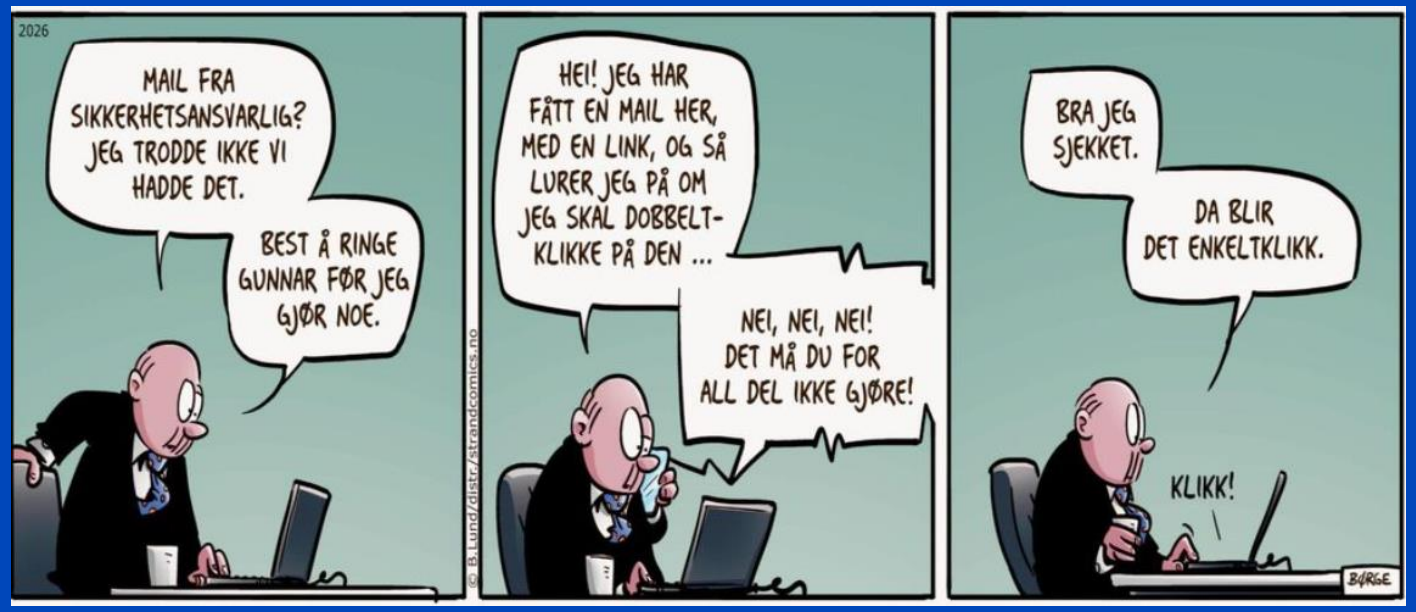
1. **Passord, tilganger og rettigheter**
2. **Ansattes sikkerhetsbevissthet/kunnskap**
3. **Nettverk og fysisk sikring**
4. **Systemsikkerhet**

+ GDPR

Alle punkt er like viktig å prioritere.

RenRøros
Digital as

Informasjonssikkerhet Ren Røros



Alt sikkerhetsarbeid starter med kartlegging. Spørsmål som sikkerhetsansvarlig bør (må) kunne besvare

RenRøros
Digital as

Informasjonssikkerhet Ren Røros

1. Passord, tilganger og rettigheter

- Totrinnspålogging (MFA)
- Beskyttelse av e-post (SPAM-filter, SPF, DKIM og DMARC)
- Logganalyse
- Passordrutiner (Se retningslinjer Norsis og Microsoft)

RenRøros
Digital as

Informasjonssikkerhet Ren Røros

2. Ansattes sikkerhetsbevissthet/kunnskap

- Kartlegge kunnskapsnivå.
- E-post. Hva er trygt og ikke. Behov for profesjonell kartlegging/test?
- Nettsider og linker
- Windows-tast + L
- Deling/håndtering av bedriftens data
- Bevisst bruk av skybaserte tjenester
- Datahierarki/roler/regler/tilganger

RenRøros
Digital as

Informasjonssikkerhet Ren Røros

3. Datasikkerhet fysisk og nett

- Segmentering av nett. For eksempel: Sikker, åpen, gjest, mobil, o.l.
- Datarom/patcheskap er ryddet og låst. Overspenning/UPS påkoblet?
- Brannmur
- Alder og programvare
- Konfigurasjon
- UPS/overspenningsvern
- Alder. Batteri bør (må) byttes etter 3år
    - Størrelse stor nok til utstyr den skal beskytte?
    - Praktisk test
- Passord
- Skrevet ned på tavler eller lapper?
- Tilgang til lokalet.

RenRøros
Digital as

Informasjonssikkerhet Ren Røros

4. Systemsikkerhet

- Alle enheter oppdatert med programvare og firmware.
- Automatisk varsling
- Patching - programvare oppdatering
- Antivirus
    - Aktivert?
    - Oppdatert?

RenRøros
Digital as

Informasjonssikkerhet Ren Røros

Sikkerhet er mer enn en god brannmur….

RenRøros
Digital as

Informasjonssikkerhet Ren Røros

4 viktigste tiltaks områder:

1. **Passord, tilganger og rettigheter**
2. **Ansattes sikkerhetsbevissthet/kunnskap**
3. **Nettverk og fysisk sikring**
4. **Systemsikkerhet**

+ GDPR

Alle punkt er like viktig å prioritere.

RenRøros
Digital as

Informasjonssikkerhet Ren Røros

(4) Systemsikkerhet klienter = Ren Klient

1. Kartlegging
2. Standardoppsett
3. Automatisk patching
4. Logging/overvåkning
5. Changelogg
6. Et klikk fjernhjelp
7. Rapportering
8. Oversikt over installert software på klienter
9. Utskiftingsplan/investeringsplan
10. «Antivirus»
11. «Krisevarsling» direkte mot klient.
12. Dynamisk utstyrsregister
13. Tilbys til både nye og eksisterende klienter, uansett operativsystem

*Alle funksjoner har «best practice» oppsett fra RRD, men kan tilpasses etter kundens ønske.

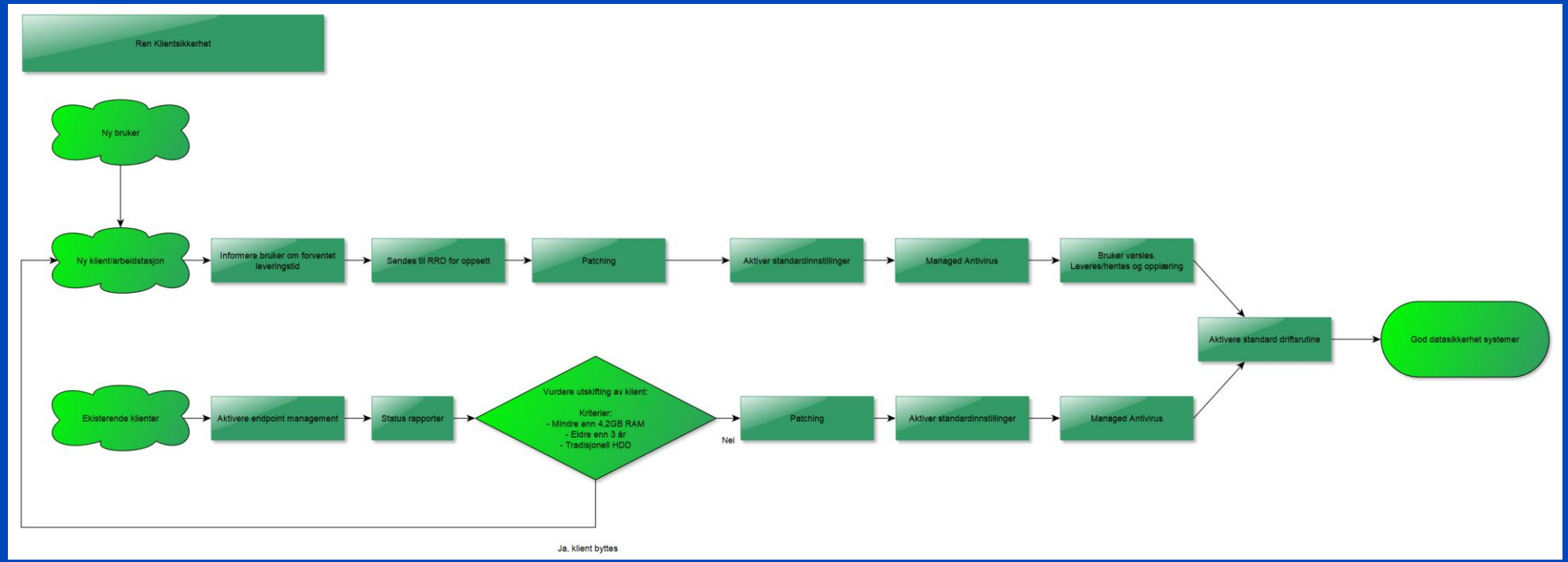
RenRøros
Digital as

Informasjonssikkerhet Ren Røros

(4) Systemsikkerhet server og klient = Ren Klient «Antivirus»

RenRøros
Digital as

Ren Klient (CaaS)



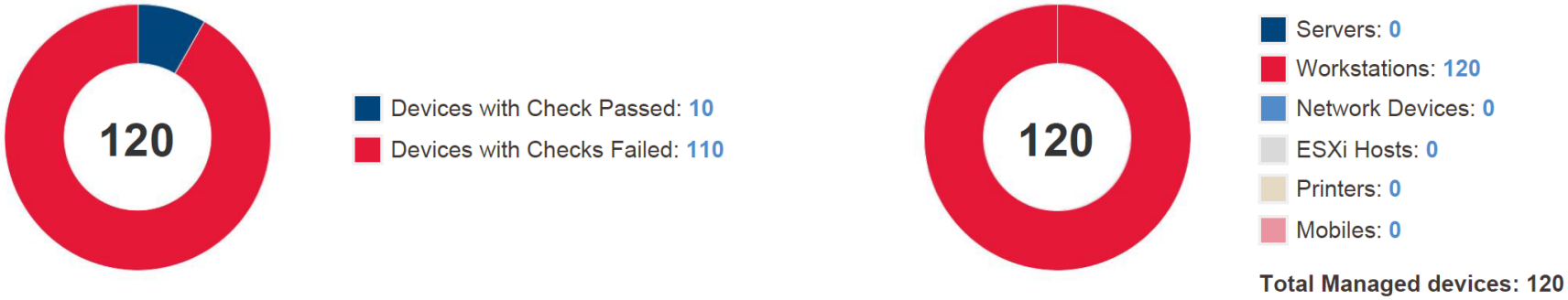
* Støtter nye og gamle klienter

RenRøros
Digital as

Automatisk rapportering

Device Health Summary Report

SUMMARY



WORKSTATIONS

Device Name	Device Description	Operating System	Disk Space	RAM Quantity	Software Compliant	Fully Patched	Antivirus Up to Date	Under Warranty	Online Within Last 30 Days	No Open Alerts

* Tilpasses etter eget ønske

RenRøros

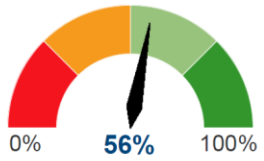
RenRøros
Digital as

Sikkerhetsstatus

Executive Summary Report

SUMMARY

The Overall score represents the overall health of the network. The score is influenced by the results of different services that are delivered below.



Services Delivered	Score
Asset Management	96%
Monitoring	100%
Patch Management	5%
Software Management	0%
Antivirus	83%
Average Score	56%

Asset Management
The Asset Management score represents the capability of the network to function as is required by today's standards. Compliancy checks are made against the device to ensure devices meet the set criteria. Included in the checks are Warranty Status, Disk Capacity, Memory Capacity and if the Operating system is still supported.

Monitoring
The Monitoring score is influenced by the open monitoring alerts for the network. The total number of open alerts influence the score, a higher priority is reflected by a increased weight in the calculation. A lower score means that issues are seen but have not yet been resolved.

Patch Management
Regularly installing Microsoft Updates is essential for keeping the network secure. The Patch Management score represents the current state of Microsoft Updates in the network.

Software Management
Keeping commonly used 3rd party software applications updated significantly helps keeping the network secure. Attackers often try to exploit security vulnerabilities in these applications. This score indicates the compliance level of the managed devices.

Antivirus
An Antivirus product on all devices is essential for keeping the network protected against malware and other threats. The Antivirus Score represents if the Antivirus solution is installed, running and up to date on all devices.

Proactive Maintenance
Any network requires proactive maintenance to ensure its availability, security and performance. The report contains a list of regularly scheduled automated activities. No score is calculated based on these activities.

RenRøros
Digital as

1-2-3 Investeringsplan/behov

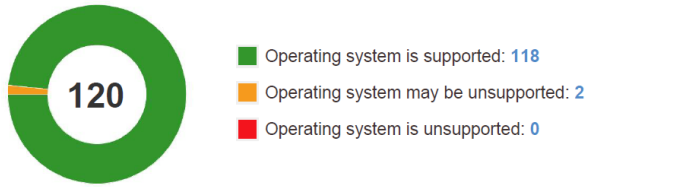
Hardware Lifecycle Report

SUMMARY

Hardware Replacement Recommendations

Period	Age	Quantity
Replacement recommended within 12 months	4 years+	13
Replacement recommended within 12-24 months	3-4 years	11
Suitable for 24 months+	< 3 years	95
Unknown		1
Total Devices		120

Operating System Support



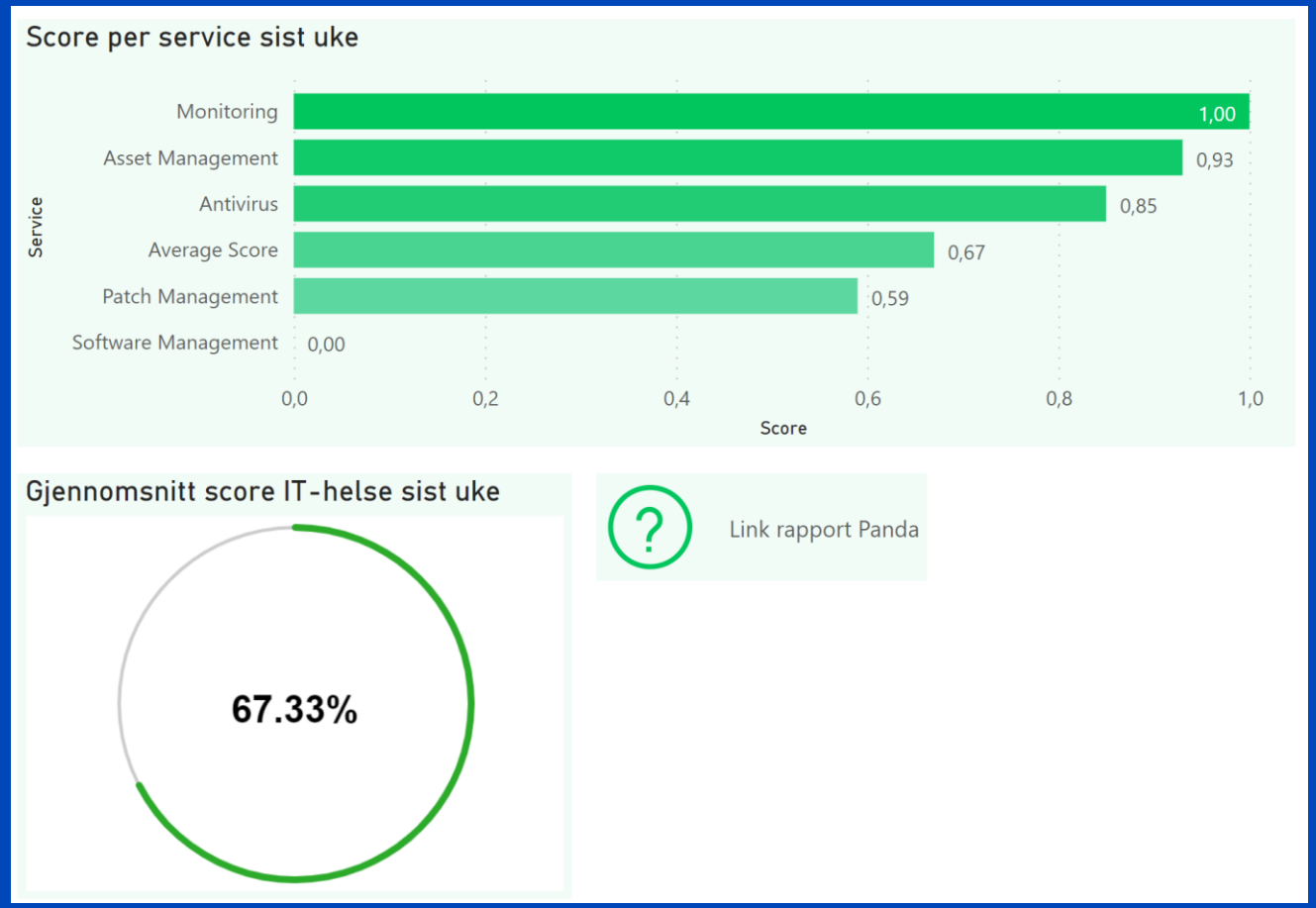
Operating System Support*	Quantity
Operating system is supported	118
Operating system is unsupported unless manufacturer extended support has been arranged	2
Operating system is unsupported	0
Total Devices	120

Windows operating system support only. Non-Windows OS are counted as supported.

RenRøros

RenRøros
Digital as

Integrasjon PowerBI



<25 = rødt Gult >62,5 = grønt

RenRøros
Digital as

Sikkerhetssamarbeid:

26.04.2021:
Presentasjon mest effektive Informasjonssikkerhet tiltak.

8.03.2021:
Arbeid anbud kommunikasjon

24.02.2021:
Gjennomgang anbefalte sikkerhetstiltak fra blant annet KS, Norsk helsenett og NorSIS

14.01.2021:
Gjennomgang generell informasjonssikkerhet i lys av «Østre toten» hendelsen

RenRøros Digital as

Informasjonssikkerhet Ren Røros

Takk for oppmerksomheten!