



Digistat® Produkt Brugermanual

Revision 1.0

2019-06-11

ASCOM UMS s.r.l. Unipersonale

Via Amilcare Ponchielli 29, IT-50018, Scandicci (FI), Italien

Tlf. (+39) 055 0512161 – Fax (+39) 055 829030

www.ascom.com

Digistat® version 6.0

Digistat® fremstilles af Ascom UMS s.r.l. (<http://www.ascom.com>).

Digistat® produktet er  mærket i henhold til direktiv 93/42/EØF ("Medicinsk udstyr") ændret ved direktiv 2007/47/EF.

Ascom UMS er certificeret i henhold til EN ISO 13485:2016 med følgende rækkevidde: "Product and specification development, manufacturing management, marketing, sales, production, installation and servicing of information, communication and workflow software solutions for healthcare including integration with medical devices and patient related information systems".

Softwarelicens

Produktet må kun anvendes efter at have indhentet en gyldig licens fra Ascom UMS eller distributøren

Licenser og registrerede varemærker

Digistat® er et varemærke hos Ascom UMS s.r.l. Alle øvrige varemærker tilhører de respektive ejere.

Ingen del af denne udgivelse må gengives, videresendes, kopieres, registreres eller oversættes uanset form, måde eller medie uden forudgående skriftlig tilladelse fra Ascom UMS.

Indhold

1. Brug af manualen.....	6
1.1 Mål	6
1.2 Anvendte tegn og terminologi.....	6
1.3 Symboler.....	7
1.3.1 Informationsboksen DIGISTAT®:	8
2. Introduktion til DIGISTAT®	9
2.1 Modulopbygget arkitektur	9
2.2 Tilladt brug	9
2.2.1 Sikkerhedsprocedurer	Error! Bookmark not defined.
2.3 Off-label-brug af produktet.....	11
2.4 Patient Befolkning	12
2.5 CE-mærke og overensstemmelse med forordninger	Error! Bookmark not defined.
2.6 Producentens ansvar	14
2.7 Sporing af produkt.....	14
2.8 Kontrol efter markedsføringen	15
2.9 Driftslevetid	15
3. Software-/hardwarespecifikationer	16
3.1 Central & Seng	16
3.1.1 Hardware	16
3.1.2 Operativsystem.....	17
3.1.3 Systemsoftware	17
3.2 Server	17
3.2.1 Hardware	17

3.2.2 Operativsystem.....	18
3.2.3 Systemsoftware	18
3.3 DIGISTAT® "Mobile"	19
3.4 DIGISTAT® "Web"	19
3.5 Advarsler.....	20
3.6 Firewall og antivirus	21
3.6.1 Yderligere anbefalede forholdsregler for cyberbeskyttelse	22
3.7 Funktioner i lokalt netværk	23
3.7.1 Påvirkning af sundhedsinstitutionens netværk fra de Produkt.....	24
4. Inden start.....	25
4.1 Advarsler vedrørende installation og vedligeholdelse	25
4.1.1 Patientområde.....	Error! Bookmark not defined.
4.2 Rengøring	Error! Bookmark not defined.
4.3 Generelle forskrifter og advarsler	26
4.3.1 Elektrisk sikkerhed.....	Error! Bookmark not defined.
4.3.2 Elektromagnetisk kompatibilitet.....	Error! Bookmark not defined.
4.3.3 Udstyrets egnethed.....	Error! Bookmark not defined.
4.4 Beskyttelse af privatlivets fred.....	26
4.4.1 Egenskaber vedrørende adgangsinformationer og brug	29
4.4.2 Systemadministratorer	31
4.4.3 Systemlogs.....	31
4.4.4 Lægelog.....	31
4.5 Backup-politik.....	33
4.6 Fremgangsmåde ved arbejdsstation ude af drift	33
4.6.1 Genkonfiguration/erstatning af netværksudstyr.....	35

4.7 Forebyggende vedligeholdelse	36
4.8 Kompatibelt udstyr	36
4.9 Manglende adgang til Produkt	37
5. Producentens kontaktoplysninger	39
6. Resterende risici.....	40

1. Brug af manualen

Denne brugervejledning skal bruges i kombination med modulspecifikke manualer, som er angivet nedenfor. Se de gældende manualer, ifølge de Digistat-moduler, der anvendes i sundhedsorganisationen:



USR DNK Controlbar
USR DNK Smart Central
USR DNK Smart Central Mobile
USR DNK Vitals Mobile
USR DNK Voice Notes Mobile
USR DNK Identity Mobile
USR DNK Collect Mobile

1.1 Mål

De bestræbelser, som ligger til grund for udarbejdelsen af denne manual, er at give alle de nødvendige oplysninger for at garantere en sikker og korrekt brug af DIGISTAT® produktet (herefter "Produktet") og muliggøre identifikation af producenten. Endvidere har dette dokument til formål at beskrive hver enkelt del i Produktet, at udgøre en referencevejledning for den bruger, som ønsker at få oplysninger om udførelse af et bestemt indgreb, og at udgøre en vejledning vedrørende korrekt brug af Produktet, så forkert og potentielt farlig brug kan undgås.

1.2 Anvendte tegn og terminologi

Brugen af DIGISTAT® Produkter kræver et grundlæggende kendskab til de mest almindelige IT-termer og -aspekter. På tilsvarende måde forudsætter forståelsen af denne manual besiddelse af dette kendskab.

Husk, at DIGISTAT® Produkter kun må bruges af professionelt og korrekt uddannet personale.

Ved indhentning af oplysninger i online-versionen i modsætning til papirudgaven, fungerer krydshenvisninger i dokumentet som links. Dette indebærer, at du, når du støder på en henvisning til en figur (eksempelvis "Fig 8") eller et afsnit (eksempelvis "afsnit 3.1.2"), kan klikke på henvisningen for at få direkte adgang til den pågældende figur eller det pågældende afsnit.

1.2.1 Grundlag

Det følgende grundlag er blevet anvendt i dette dokument:

- Navne på knapper, menukommandoer, indstillinger, ikoner, felter og alt i brugergrænsefladen, som brugeren kan anvende (enten touch, klik eller vælg) er angivet i **fed skrift**.
- Navne/overskrifter på skærbilleder, vinduer og faner er præsenteret med "dobbelte anførselstegn".
- Programmeringskodens font er Courier.
- ➤ Punkttegnet angiver en handling, som brugeren skal udføre for at gennemføre en bestemt opgave.
- Henvisninger til eksterne dokumenter er angivet i *kursiv*.

1.3 Symboler

Manualen anvender følgende symboler:

Nyttig information



Dette symbol vises ved siden af supplerende oplysninger vedrørende karakteristika og brug af DIGISTAT®. Der kan være tale om forklarende eksempler, alternative procedurer eller enhver anden form for "ekstra" information, som skønnes at være nyttig for en forbedret forståelse af produktet.

Advarsel!



Dette symbol benyttes for at fremhæve oplysninger, der har til formål at forebygge forkert brug af softwaren eller at henlede opmærksomheden på kritiske procedurer, som kan medføre risici. Det er derfor nødvendigt at være meget opmærksom, hver gang dette symbol vises.

Følgende symboler anvendes i informationsboksen Digistat:



Fabrikantens navn og adresse



Vær opmærksom, læs ledsagende dokumenter

1.3.1 Informationsboksen Digistat:

Om-knappen, på Digistats hovedmenu, viser et vindue, der indeholder oplysninger om den installerede version af Digistat og de tilknyttede licenser (Fig. 1). Få flere oplysninger i brugervejledningens kontrolbjælke.



Fig. 1

2. Introduktion til Digistat

Programsuiten for Digistat kliniske moduler Suite er et avanceret softwaresystem til styring af patientrelaterede oplysninger. Produktet er designet specifikt til brug af læger, sygeplejersker og administratorer.

Softwarepakken omfatter en række moduler, som kan fungere særskilt eller integreres fuldstændigt for at skabe en komplet løsning til styring af patientrelaterede oplysninger.

Digistat kan benyttes i en lang række forskellige miljøer, eksempelvis intensivenheder, afdelinger, operationsstuer, administrationskontorer osv.

Den modulopbyggede arkitektur og de omfattende konfigurationsmuligheder i Digistat giver dig mulighed for at opbygge dit eget system til styring af patientrelaterede oplysninger og at udvide produktet til at opfylde dine nye behov, når det er nødvendigt.

Digistat Produktet kan kun tilgås ved indtastning af brugernavn og password. Hver bruger er defineret af en detaljeret profil og har kun adgang til de tilladte områder. Produktet genererer automatisk en audit trail for hvert login.

2.1 Modulopbygget arkitektur

“Modulopbygget arkitektur” indebærer, at forskellige programmer (eller moduler) kan implementeres i det samme softwaremiljø (i dette tilfælde Digistat), som er karakteriseret ved et særligt grafisk design, samme generelle mål og brugsbetingelser.

Det er muligt at tilføje forskellige moduler på forskellige tidspunkter og på en måde, som er aftalt med brugeren. Den endelige software suite passer til de specifikke brugerbehov og kan ændres gennem tiden på baggrund af de mulige ændringer i brugerens behov.

2.2 Tilladt brug

Digistat Software (herefter “Produktet”) udarbejder registreringer, organiserer, sender og viser patientrelaterede oplysninger, herunder oplysninger og hændelser fra tilsluttet klinisk udstyr og systemer samt manuelt indtastede informationer for at understøtte sundhedspersonalet i forbindelse med diagnosticering og behandling af patienter samt etablering af elektroniske patientregistreringer.

- Produktet opretter konfigurerbare elektroniske patientregistreringer baseret på indlæste oplysninger og information samt på manuel og automatiseret dokumentation om aktiviteterne i den kliniske enhed.
- Produktet tilvejebringer automatiseret sekundær visuel og hørbar meddelelse og visning af de indlæste oplysninger, hændelser, den aktuelle status og driftsbetingelserne i det tilsluttede medicinske udstyr og systemer

på dertil beregnet visningsudstyr. Produktet kan også konfigureres til at videresende oplysninger og information om hændelser, statusser og driftsbetingelser til Ascom meddelelsessystemet.

- Produktet understøtter forbedringen af workflow i forbindelse med sygepleje vedrørende styringen af alarmer fra det tilsluttede kliniske udstyr og systemer.
- Produktet understøtter dokumentationen af den ordinerede behandling, dens forberedelse og dens udførelse.
- Produktet understøtter registreringen, valideringen og visningen af kort med vitale tegn baseret på de indlæste oplysninger og information.
- Produktet tilvejebringer konfigurerbare rapporter, kort og statistik baseret på registrerede oplysninger til brug af sundhedspersonalet til analyse af enhedens effektivitet, produktivitet, kapacitet, ressourceudnyttelse og plejekvalitet.

Produktet erstatter eller gengiver **ikke** den originale visning af oplysninger og alarmer fra det tilsluttede udstyr og systemer og kontrollerer, overvåger og ændrer **ikke** funktionen i det tilsluttede udstyr og systemer eller de respektive alarmmeddelelser.

Produktet **er ikke** beregnet til brug til direkte diagnosticering eller monitorering af vitale fysiologiske parametre.

Produktet er beregnet til brug af uddannet sundhedspersonale på et hospital/i et klinisk miljø og forudsætter korrekt betjening af og drift i IT- og kommunikationsinfrastrukturen på hospitalet, det anvendte visningsudstyr og det tilsluttede kliniske udstyr og systemer.

Endvidere tilvejebringer produktet specifikke funktioner og interfaces, som kan betjenes af ikke-fagpersoner på andre steder til ikke-kliniske formål til visning af oplysninger, journaler, kort og statistik uden mulighed for at tilføje, ændre eller slette nogen oplysninger eller information.

Produktet er stand-alone software, som installeres på servere og computere, som skal være i overensstemmelse med de tekniske specifikationer vedrørende hard- og software, som leveres sammen med produktet.

2.2.1 Sikkerhedsprocedurer

Brugeren skal udelukkende basere de terapeutiske eller diagnostiske beslutninger og indgreb på den direkte undersøgelse af den oprindelige informationskilde. Brugeren alene bærer ansvaret for at kontrollere, at de oplysninger, som vises af produktet, er korrekte samt for korrekt brug af oplysningerne.

Kun udskrifter, som er underskrevet digitalt eller med blæk af autoriseret medicinsk personale, skal betragtes som gyldige patientregistreringer. Ved underskrivelse af de ovennævnte udskrifter attesterer brugeren at have kontrolleret, at oplysningerne på dokumentet er korrekte og fuldstændige.

Ved indtastning af patientrelaterede oplysninger har brugeren ansvar for at verificere, at patientidentitet, afdeling for sundhedsorganisationens facilitet/behandlingsenhed og sengens oplysninger, der vises i Produktet, er korrekte. Kontrollen er meget vigtig i tilfælde af kritiske indgreb såsom eksempelvis indgivelse af medicin.

Sundhedsorganisationen er ansvarlig for at identificere og gennemføre passende procedurer for at sikre, at potentielle fejl i produktet og/eller ved brugen af produktet registreres og afhjælpes med det samme og ikke udgør en risiko for patienten og operatøren. Disse procedurer afhænger af Produktets konfiguration og den anvendelsesmetode, som foretrækkes af sundhedsorganisationen.

Afhængigt af konfigurationen kan produktet tilvejebringe oplysninger om medicin. Sundhedsorganisationen er ansvarlig for at bekræfte indledende og periodisk, at disse oplysninger er aktuelle og opdaterede.

Produktet giver ikke primær notifikation af alarmer; det er ikke beregnet til at blive anvendt i stedet for den direkte overvågning af alarmerne, der genereres af de medicinske enheder. Denne begrænsning skyldes bl.a. specifikationer og indskrænkninger i kommunikationsprotokollerne i det medicinske udstyr.

Såfremt udstyr, som skal benyttes til produktet, er placeret i patientområdet eller tilsluttes udstyr i patientområdet, Sundhedsorganisationen har ansvaret for at sikre, at hele kombinationen overholder den internationale standard IEC 60601-1 og ethvert yderligere krav fastsat i de lokale bestemmelser

Brug af Produktet skal gives ved hjælp af specifik konfiguration af brugerkonti og aktiv overvågning tildeles brugere, 1) som er instrueret i overensstemmelse med produktets anvisning af personale, som er autoriseret af producenten eller distributører, og 2) er i besiddelse af professionelle kvalifikationer til korrekt at kunne fortolke de tilvejebragte oplysninger og implementere de passende sikkerhedsprocedurer.

Produktet er et stand-alone-software, der kan køre på standardcomputere og/eller standard mobile enheder, der er forbundet til Sundhedsorganisationens lokale netværk. Sundhedsorganisationen er ansvarlig for tilstrækkeligt at beskytte computere, enheder og lokalt netværk mod cyberangreb.

Produktet må kun installeres på computere og udstyr, som opfylder min. kravene til hardwaren, og på understøttede operativsystemer.

2.3 Off-label-brug af produktet

Enhver brug af produktet, som ikke er omfattet af de udtrykkelige anvisninger i "Tilladt brug" (normalt beskrevet som "off-label"-brug), sker med fuld diskretion og på brugerens og den ansvarlige organisations eget ansvar.

Producenten garanterer på ingen måde produktets sikkerhed og egnethed til et givent formål, hvis brugen af produktet ikke er omfattet af de udtrykkelige anvisninger i "Tilladt brug".



Produktet **er ikke** et primært distribueret alarmsystem.

2.4 Patient Befolkning

Produktet er et softwareprogram og er ikke i kontakt med patienten.

Patientpopulationen og patientforholdene etableres af de medicinske enheder og systemer, som produktet er forbundet med.

Derudover gælder følgende begrænsninger :

- Patientvægt mellem 0,1 kg og 250 kg
- Patienthøjde mellem 15cm og 250cm

2.5 Sundhedsvæsenets ansvar

Ascom UMS kan ikke gøres ansvarlig for konsekvenser med hensyn til udstyrets sikkerhed og effektivitet, som skyldes tekniske reparationer eller vedligeholdelse, som ikke er blevet udført af producentens eget tekniske servicepersonale eller af teknikere med autorisation fra Ascom UMS.

Brugeren og den juridiske repræsentant for den Sundhedsorganisation, hvor udstyret benyttes, skal være opmærksomme på deres respektive ansvar i henhold til den gældende lokale lovgivning angående sikkerhed og helbred på arbejdspladsen (eksempelvis italiensk lovdekret nr. 81/2008) og eventuelle stedsspecifikke sikkerhedsprocedurer.

Ascom UMS Service er i stand til at tilbyde kunder den nødvendige support for at bevare sikkerheden og effektiviteten i det leverede udstyr på langt sigt ved at sikre kvalifikationer, det instrumentelle udstyr og de reservedele, som er nødvendige for at garantere, at udstyret fortsat opfylder de originale konstruktionsspecifikationer.



Produktet er designet under hensyntagen til de krav og de bedste praksisser, der findes i IEC 80001-standarden og dens tekniske sikkerhedsrapporter. Især IEC/TR 80001-2-5: 2014 har stor relevans for produktet. Som forklaret i IEC 80001-serien, er en del af de nødvendige aktiviteter og risikokontrolforanstaltninger under sundhedsorganisationens kontrol og ansvar. Se venligst standarden og dens sikkerhedsstillelser for at identificere de nødvendige aktiviteter og risikokontrolforanstaltninger. Der henvises især til nuværende gyldige version af følgende dokumenter:

- IEC 80001-1:2010
 - IEC/TR 80001-2-1:2012
 - IEC/TR 80001-2-2:2012
 - IEC/TR 80001-2-3:2012
 - IEC/TR 80001-2-4:2012
 - IEC/TR 80001-2-5:2014
-

2.6 Producentens ansvar

Ascom UMS er kun ansvarlig for produktets sikkerhed, pålidelighed og ydelse, hvis:

- Installation og konfiguration er blevet udført af personale, der er uddannet og godkendt af Ascom UMS;
- Brug og vedligeholdelse overholder instruktionerne i produktdokumentationen (herunder denne brugsanvisning);
- Indstillinger, ændringer og reparationer kun udføres af personale, som er uddannet og autoriseret af Ascom UMS;
- Produktets brugsmiljø overholder de gældende sikkerhedsforskrifter og gældende regler;
- Miljøet, som produktet anvendes i (herunder computere, udstyr, elektriske forbindelser osv.) overholder de gældende lokale bestemmelser.



Hvis produktet er en del af et "medicinsk elektrisk system" gennem en elektrisk og funktionel forbindelse med medicinsk udstyr, har sundhedsorganisationen ansvaret for de nødvendige elektriske sikkerhedsgodkendelser og godkendelsestests, også selvom Ascom UMS helt eller delvis har implementeret de nødvendige forbindelser.

2.7 Spring af produkt

For at sikre sporbarhed og korrigerende handlinger på stedet, i overensstemmelse med EN 13485 og MDD 93/42/EØF, anmodes ejeren om at underrette Ascom UMS/distributør skriftligt om enhver overdragelse af ejerskab med angivelse af identifikationsdata for produktet, tidligere ejer og ny ejer.

Enhedsdata kan findes på produktmærket ("Om boks", der vises i produktet – se side **Error! Bookmark not defined.**).

I tilfælde af tvivl/spørgsmål om produktidentifikation, kontakt teknisk assistance hos Ascom UMS/distributør (for kontaktoplysninger se side **Error! Bookmark not defined.**).

2.8 Kontrol efter markedsføringen

Gennem  hele produktets livscyklus er den markerede enhed underlagt eftermarkedsovervågning – som Ascom UMS og distributøren står for i forhold til hver markedsført enhed – i forhold til aktuelle og potentielle risici for patient eller bruger.

I tilfælde af forringelse af enhedens egenskaber, dårlige præstationer eller utilstrækkelige brugerinstruktioner, der har været eller kunne være til fare for patienten eller brugerens sundhed eller miljø sikkerheden, skal brugeren straks varsle enten Ascom UMS eller distributør.

Ved modtagelse af brugerfeedback begynder Ascom UMS/distributør omgående en gennemgangs- og verifikationsproces, og udfører de nødvendige rettelser.

2.9 Driftslevetid

Produktets levetid afhænger ikke af slid og andre faktorer, som kunne compromittere sikkerheden. Den påvirkes af softwaremiljøets forældelse (f.eks. OS, .NET Framework) og er derfor sat til 5 år fra produktversionens udgivelsesdato (kan ses i feltet Om).

3. Software-/hardwarespecifikationer



Digistat må kun installeres af uddannet autoriseret personale. Dette omfatter Ascom UMS-/forhandlerpersonale og enhver anden person, der er specielt uddannet og udtrykkeligt autoriseret af Ascom UMS-/forhandler. Uden en udtrykkelig, direkte tilladelse fra Ascom UMS-/forhandler, er sundhedsorganisationens medarbejdere ikke autoriseret til at udføre installationsprocedurer og/eller ændre Digistat-indstillingerne.



Digistat må kun bruges af uddannet personale. Digistat må ikke bruges uden at have fået en ordentlig oplæring, udført af Ascom UMS-/forhandlerpersonale.

Oplysningerne i dette kapitel beskriver producentens forpligtelser i henhold til standard IEC 80001-1:2010 (Anvendelse af risikostyring inden for it-netværk indbefattende medicinsk udstyr).

I henhold til standard IEC 60601-1 skal der benyttes "medicinsk godkendt" udstyr, hvis et elektrisk udstyr skal placeres tæt på sengen. I disse situationer benyttes normalt medicinsk godkendte PANEL PC'er. Ved udtrykkelig forespørgsel herom kan Ascom UMS give oplysninger om passende udstyr af denne type.



En understøttet PDF-læser skal installeres på arbejdsstationen for at vise onlinehjælpen. Se 3.1.3 efter softwarekravene til centrale - og sengearbejdsstationer.

3.1 Central & Seng

3.1.1 Hardware

Min. hardwarekrav:

- Intel® I3 processor (eller hurtigere)
- Hukommelse: 4 GB RAM
- Harddisk: min. 60 GB ledig plads
- Monitor: 1.024 x 768 eller højere (1920 x 1280 anbefales)
- Mus eller andet kompatibelt udstyr
- Ethernet interface 100 Mb/s (eller højere)
- CD/DVD drev eller mulighed for kopiering af installationsfilerne

Hvis en central/side-arbejdsstation er konfigureret til at vise videostrømme (funktionen understøttes kun i Smart Central eller OranJ med kameraintegration aktiveret), er minimumskravene følgende:

- Intel® I3-processor (eller hurtigere)
- Hukommelse: 4 GB RAM + 50 MB for hver kamerastrøm der vises samtidigt (f.eks. med 20 kameraer vist 4 GB + 1 GB)

- Harddisk: Mindst 60 GB ledig plads
- Overvågning: 1024 x 768 eller højere (1920 x 1080 foreslået)
- Mus eller anden kompatibel enhed
- Ethernet interface 100 Mb / s (eller højere)
- CD / DVD-drev eller mulighed for at kopiere installationsfilerne

Nogle eksempler: med Intel i7 6600 2.60 Ghz, med en streaming af 10 kameraer med en bitrate på 3138 kbps, er cpu-forbruget omkring 45%. Med I3 7100t 3,4 Ghz, med en streaming af 16 kameraer med en bitrate på 958 kbps, er cpu-udnyttelsen ca. 30%.

3.1.2 Operativsystem

- Microsoft Corporation Windows 7 SP1 x86/x64 Professional
- Microsoft Corporation Windows 8.1 x86/x64 Professional
- Microsoft Corporation Windows 10

3.1.3 Systemsoftware

- Microsoft Framework .NET 4.5
- Adobe Acrobat Reader 10

Produktbrugermanualen er en PDF-fil, der er produceret i henhold til PDF-standardversion 1.5, og den er dermed læsbar af Adobe Acrobat 6.0 eller nyere. Desuden blev produktbrugermanualen testet med Adobe Acrobat Reader 10. Sygehusorganisationen kan bruge en anden version af Acrobat Reader: Verifikationen af det installerede produkt inkluderer en kontrol af, at brugervejledningen er korrekt læsbar.

3.2 Server

3.2.1 Hardware

Minimum hardwarekrav (lille installation, 20 beds, 4 enheder hver):

- Intel® I5 processor med 4 kerner.
- Hukommelse: 4 GB RAM (8 GB anbefales)
- Harddisk: min. 120 GB ledig plads
- Ethernet interface 100 Mb/s (eller højere). 1 Gb/s anbefales.
- CD/DVD drev eller mulighed for kopiering af installationsfilerne

Anbefalede hardwarekrav (mellemstore installationer, 100 beds, 4 enheder hver, Connect og Mobile):

- Intel® I7 processor med 8 kerner.
- Hukommelse: 32 GB RAM.
- Harddisk: min. 120 GB ledig plads
- Ethernet interface: 1 Gb/s.

- CD/DVD drev eller mulighed for kopiering af installationsfilerne

3.2.2 Operativsystem

- Microsoft Corporation Windows Server 2012 R2
- Microsoft Corporation Windows Server 2016

3.2.3 Systemsoftware

- Microsoft SQL Server 2008R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft Framework.NET 4.5

3.3 Digistat "Mobile"

Digistat Mobile applikationen er blevet testet på Ascom Myco SH1 og SH2 Wi-Fi og Smartphone mobiltelefon med Android version 4.4.2 (Myco1) eller 5.1 (Myco1/Myco2) eller 8.0 (Myco3). Ansøgningen er derfor kompatibel med Myco1, Myco2 og Myco3.

Applikationen er designet til at være kompatibel med andre Android-enheder med en mindste skærmstørrelse på 3,5"; kompatibilitet med en bestemt enhed skal verificeres inden klinisk brug.

Kontakt venligst Ascom UMS/distributøren vedrørende listen over tilgængelige drev. Generelle advarsler

3.4 Digistat "Web"

Følgende browsere understøttes til brug med Digistat webapplikationer:

- Chrome 63
- Firefox 56
- Edge 41
- Internet Explorer 11



Kun understøttede webbrowserne skal bruges til Digistat Web.



En Digistat Web-arbejdsstation vil altid have webbrowseren i forgrunden. Desuden skal webbrowser aldrig bruges til andet end Digistat Web (hvilket også indebærer, at Digistats webside skal være standardwebsted for webbrowseren).



Browserens skærm skal altid indstilles til 100%.



Når det lokale netværk i det mindste delvist er baseret på WiFi-forbindelser, er der muligvis afbrydelser, der aktiverer afbrydelsesfunktionen (grå tæppe, der dækker Digistat Web), da WiFi-forbindelserne er intermitterende. Derfor er Produktet muligvis ikke tilgængeligt. Sundhedsorganisation skal arbejde for at sikre optimal WiFi-dækning og instruere personalet om, hvordan man håndterer disse midlertidige produktbrud.

3.5 Advarsler



Programmet "MDI Web", der præsenteres i den relevante brugervejledning, kan kun bruges til demoformål. Det kan ikke bruges i et produktionsmiljø.



For at benytte de Produkt korrekt skal Microsoft Windows skalering indstilles til 100 %. Andre indstillinger kan hindre produktet i at starte eller medføre driftsforstyrrelser i den visuelle visning af de Produkt. Vedrørende oplysninger om skaleringsindstillinger henvises til dokumentationen fra Microsoft Windows.



Den minimale vertikale opløsning på 768 understøttes kun, hvis de Produkt er konfigureret til at køre i fuldskærm modus, eller hvis Windows proceslinjen er i Auto-hide modus.



Computere og andet tilsluttet udstyr skal være egnet til det miljø, hvor de benyttes, og skal derfor opfylde den gældende lovgivning.



Det er obligatorisk at følge producentens anvisninger vedrørende opbevaring, transport, installation, vedligeholdelse og bortskaffelse af hardware fra tredjemænd. Disse procedurer må kun udføres af kvalificeret og autoriseret personale.



Brugen af produktet sammen med anden software end den, som er specificeret i dette dokument, kan øve negativ indflydelse på produktets sikkerhed, effektivitet og udformningen af kontroller. Sådan brug kan udgøre en øget risiko for brugere og patienter. Det er obligatorisk at kontakte en autoriseret tekniker hos Ascom UMS eller forhandleren inden brug af produktet sammen med anden software end den, som er specificeret i dette dokument.

Hvis hardwaren, som produktet kører på, er en stand-alone computer, må brugeren ikke installere andre former for software (hjælpe- eller applikationsprogrammer) på computeren. Det anbefales at anvende en politik om tilladelse, som hindrer brugere i at udføre procedurer såsom installation af ny software.



Den ansvarlige organisation skal implementere en mekanisme til synkronisering af dato og klokkeslæt til en referencekilde for de Produkt arbejdsstationerne.



Det anbefales at deaktivere adgangen til internettet på klientarbejdsstationerne og de håndholdte enheder, som produktet

	bruges på. Alternativt skal sundhedsorganisationen iværksætte de nødvendige sikkerhedsforanstaltninger for at sikre tilstrækkelig beskyttelse mod cyberangreb og installation af uautoriserede applikationer.
	Dele af produktet fungerer som visere af videostrømme; Produktet er ikke kilden til videostrømmen, og den optager ikke disse oplysninger på nogen måde. Det er sundhedsorganisationens ansvar at styre systemet ud fra et databeskyttelsesperspektiv, herunder installation og konfiguration af kildekameraer.
	Dele af produktet håndterer lyd og billeder relateret til brugerne og/eller patienterne herunder erhvervelse, udarbejdelse og optagelse. Det er sundhedsvæsenets ansvar at gennemføre de nødvendige procedurer for at overholde den lokale databeskyttelsesforordning. Inklusive, men ikke begrænset til, definitionen af brugerbegrænsning og uddannelse.
	Video streaming funktionaliteten på stationære arbejdsstationer er blevet testet med H264 og H265 video codecs. Ethvert andet video codec, der er indbygget eller installeret af tredjeparts applikationer (f.eks. VLC Media Player) skal testes før brug.
	Pas på: hver videokilde understøtter et maksimalt antal samtidige forbundne klienter. Det er sundhedsorganisationens ansvar at bestemme dette maksimale antal og informere brugerne.
	Videostreamings-funktionaliteten på mobile enheder understøtter kun RTSP-videostrømme med følgende godkendelses typer: • Ingen godkendelse; • Grundlæggende godkendelse; • Digest-godkendelse.
	Video streaming funktionaliteten på mobile enheder understøtter kun H263, H264 og H265 video codecs.

3.6 Firewall og antivirus

For at beskytte de Produktet mod mulige hackerangreb er det nødvendigt at gøre følgende:

- Windows® Firewall er aktiv både på klient pc'erne og serveren.
- Antivirus/Antimalware software er installeret og blevet opdateret regelmæssigt, både på klient pc'erne og serveren.

Den sundhedsorganisation skal sikre, at disse to beskyttelser er aktiveret. Ascom UMS testede produktet med F-SECURE Antivirus men henset til sundhedsinstitutionens allerede eksisterende strategier og politikker overlades det faktiske valg af antivirusprogram til den ansvarlige organisation. Ascom UMS kan ikke sikre, at de Produktet er kompatibelt med ethvert antivirusprogram eller antiviruskonfiguration.



Der er blevet rapporteret om visse tilfælde af manglende kompatibilitet mellem dele af Digistat og Kaspersky antivirusprogrammet. Løsningen af disse problemer med manglende kompatibilitet krævede fastlæggelse af specifikke regler i selve antivirusprogrammet.



Det anbefales det at begrænse åbningen til blot de TCP og UDP porte, som reelt er nødvendige. Dette kan ændre sig afhængigt af konfigurationen af Produktet. Vedrørende yderligere oplysninger henvises til Ascom UMS teknisk servicecenter.

3.6.1 Yderligere anbefalede forholdsregler for cyberbeskyttelse

For yderligere at beskytte de Product fra mulige cyberangreb, anbefales det stærkt at:

- planlægge og implementere "styrkning" af IT-infrastrukturen, herunder IT-plattformen, der repræsenterer runtime-miljøet for produktet,
- implementere et system til registrering og forebyggelse af indtrængen (IDPS),
- udføre en penetrationsmåling og, hvis der opdages en svaghed, udføre alle de nødvendige tiltag for at forebygge risikoen for cyberindbrud,
- smide enhederne ud, når de ikke længere kan opdateres,
- planlægge og udføre en regelmæssig verifikation af integriteten af filerne og konfigurationerne,
- implementere en DMZ-løsning (demilitariseret zone) til webservere, der skal eksponeres på internettet.

3.7 Funktioner i lokalt netværk

Dette afsnit beskriver funktionerne i det lokale netværk, hvor de Produkt installeres, for at sikre fuld effektivitet i Produktet.

- Produktet bruger en TCP/IP trafikprotokol
- LAN må ikke overbelastes og/eller fyldes fuldstændigt.
- Produktet kræver, at en LAN på min. 100 Megabit er tilgængelig for klientarbejdsstationen. 1 Gigabit Ethernet backbone vil være værdifuld.
- Der må ikke være filtre i TCP/IP trafikken mellem arbejdsstationer, servere og sekundært udstyr.
- Hvis udstyr (server, arbejdsstationer og sekundært udstyr) er sluttet til forskellige subnetværk, skal der være routing i disse subnetværk.
- Det anbefales at fastlægge redundansstrategier for at sikre serviceadgang til netværket i tilfælde af driftsforstyrrelser.
- Det anbefales at planlægge vedligeholdelsen i samarbejde med Ascom UMS/distributører, så Ascom UMS eller den autoriserede distributør effektivt kan understøtte sundhedsinstitutionen i styring af de mulige gener i forbindelse med vedligeholdelsesaktiviteterne.



Hvis netværket ikke passer sammen med de ønskede funktioner, forringes Produktets ydelse gradvist, indtil der opstår timeout fejl. Produktet skifter til slut til "Afhjælpning" modus.



Hvis et WiFi netværk er i brug, kan der ske netværksfrakoblinger som følge af en mulig intermittens i WiFi forbindelsen. Dette kan medføre aktivering af "Afhjælpning" modus og efterfølgende manglende adgang til Produktet. Den ansvarlige organisation skal sikre en optimal netværksdækning og stabilitet og uddanne personalet i håndteringen af disse midlertidige frakoblinger.



For at kryptere de data, der overføres via trådløse netværk, anbefales det at vedtage den højeste tilgængelige sikkerhedsprotokol; under alle omstændigheder ikke mindre end WPA2.

3.7.1 Påvirkning af sundhedsinstitutionens netværk fra de Produkt

De Produkt påvirker sundhedsinstitutionens lokale netværk. Dette afsnit indeholder oplysninger om den trafik, som genereres af de Produkt på netværket, for at gøre det muligt for institutionen at evaluere og analysere risiciene i forbindelse med introduktion af Produktet.

Båndbredden, som benyttes af et de Produkt afhænger af en lang række faktorer. De vigtigste er følgende:

- antallet af arbejdsstationer;
- antallet af arbejdsstationer, der er konfigureret som centrale stationer;
- antallet og typen af udstyr til indlæsning af oplysninger (enten stand-alone eller integreret);
- interfaces med eksterne systemer;
- Produktets konfiguration og anvendelsesmodus.

De Produkt båndbredde besættelse afhænger hovedsageligt af dataopsamling fra medicinsk udstyr. Som vejledning kan følgende værdier i en konfiguration med opkøb på 100 senge hvor hver seng samler data fra 1 ventilator, 1 patientmonitor og 3 infusionspumper og med 10 Digistat Smart Central arbejdsstationer, der viser 10 senge hver:

Gennemsnit: 0,8-6 Mbit/s

Maks.: 5-25 Mbit/s

I tilfælde af de Produkt konfigurationer uden erhvervelse af medicinsk udstyr, båndbredde besættelse værdier er lavere end de ovenfor angivne.

4. Inden start

4.1 Advarsler vedrørende installation og vedligeholdelse

De følgende advarsler indeholder vigtige oplysninger om de korrekte procedurer ved installation og vedligeholdelse af de Produkt. De skal overholdes nøje.



Installation, vedligeholdelse og reparationer skal udføres i overensstemmelse med procedurerne og retningslinjerne for Ascom UMS, kun af Ascom UMS-/forhandlerteknikere eller personale, der er uddannet og autoriseret af Ascom UMS/forhandlere.



Det anbefales, at sundhedsorganisationen anvender produktet til at fastsætte en vedligeholdelseskontrakt med Ascom UMS eller en autoriseret distributør. En del af vedligeholdelsen skal omfatte opgradering til den seneste version, der er tilgængelig for produktet.

De Produkt skal installeres og konfigureres af specialuddannet og autoriseret personale. Dette inkluderer personale fra Ascom UMS (eller autoriseret distributør) eller enhver anden specialuddannet person, som er autoriseret af Ascom UMS/distributøren. På tilsvarende måde skal vedligeholdelse og reparationer på de Produkt under alle omstændigheder udføres med overholdelse af retningslinjerne fra Ascom UMS. Indgrebene må kun udføres af personale fra Ascom UMS/distributøren eller enhver anden specialuddannet person, som er autoriseret af Ascom UMS/distributøren.



De Produkt skal installeres og konfigureres af specialuddannet og autoriseret personale. Dette inkluderer personale fra Ascom UMS (eller autoriseret distributør) eller enhver anden specialuddannet person, som er autoriseret af Ascom UMS/distributøren.

- Anvend tredjepartsudstyr, som anbefales af Ascom UMS/distributører.
- Kun uddannet og autoriseret personale må installere tredjepartsudstyr.
- Forkert installation af tredjepartsudstyr kan føre til risiko for kvæstelse af patient og/eller operatører.
- Overhold producentens anvisninger vedrørende installation af tredjepartshardware nøje.
- Sørg for regelmæssig vedligeholdelse af Produktet i henhold til anvisningerne i denne manual og de anvisninger, der medfølger tredjepartsudstyr.
- Sundhedsorganisationen er ansvarlig for at vælge udstyr, der er egnet til det miljø, hvor de installeres og bruges. Sundhedsorganisationen og andre

bør overveje elektrisk sikkerhed, EMC-emissioner, radiosignalforstyrrelser, desinfektion og rengøring. Opmærksomhed skal henledes til enheder installeret i patientområdet.

4.2 Generelle forskrifter og advarsler



For at sikre softwarens pålidelighed og sikkerhed i forbindelse med brug er det nødvendigt at overholde oplysningerne i dette afsnit omhyggeligt.



Den sundhedsorganisation skal sikre, at produktet og tredjepartsudstyret vedligeholdes som påkrævet for at garantere sikkerhed og effektivitet samt reducere risikoen for funktionsforstyrrelser samt opståen af mulige farer for patienten og brugeren



Produktet må kun benyttes af uddannede og autoriserede læger.

4.3 Beskyttelse af privatlivets fred

Der skal træffes passende forholdsregler for at beskytte brugerne og patienternes privatliv og for at sikre, at personoplysninger behandles ved at respektere de registreredes rettigheder, grundlæggende frihedsrettigheder og værdighed, især med hensyn til fortrolighed, personlig identitet og ret til beskyttelse af personoplysninger.



'Personoplysninger' betyder oplysninger vedrørende en identificeret eller identificerbar fysisk person ('registreret person'); en identificerbar fysisk person er en, der direkte eller indirekte kan identificeres ved henvisning til en identifikator som et navn, et identifikationsnummer, lokaliseringsdata, en online identifikator eller en eller flere faktorer, der er specifikke for den fysiske, fysiologiske, genetiske, mentale, økonomiske, kulturelle eller sociale identitet af den pågældende fysiske person"

Der lægges særlig vægt på de oplysninger, der er defineret i "EU's generelle databeskyttelsesforordning 2016/679 (GDPR)" som "Særlige kategorier af personoplysninger".

Særlige kategorier af personoplysninger:

(...) Personoplysninger, der afslører race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger eller fagforening, og (...) genetiske oplysninger, biometriske oplysninger, der har til formål at identificere en fysisk

person unikt, oplysninger vedrørende sundhed eller oplysninger vedrørende en fysisk persons sexliv eller seksuelle orientering.

Sundhedsorganisationen skal sikre sig, at brugen af produktet er i overensstemmelse med kravene i den gældende forordning om privatliv og beskyttelse af personoplysninger, og specifikt respekterer forvaltningen af ovennævnte oplysninger.

Digistat forvalter følgende personoplysninger:

- Fornavn og efternavn
- Fødselsdag
- Køn
- Patientkode
- Indlæggelsesdato
- Udskrivelsesdato
- Patientens vægt
- Patientens højde

Produkt kan indstilles til automatisk at skjule disse oplysninger på alle applikationsskærme.

For at gøre det skal du i Produkt Configuration Application indstille systemvalget "Privacy Mode" til "true" (se Produkt -indstillings- og installationsvejledningen for en detaljeret beskrivelse af procedure). Standardværdien er "true".

Hvis indstillingen "Privacy Mode" er sat til "true", er følgende tilfælde mulige:

- hvis ingen bruger er logget ind, vises ingen patientoplysninger.
- hvis en bruger er logget ind, og brugeren ikke har en særlig tilladelse, vises ingen patientoplysninger.
- hvis en bruger er logget ind, og brugeren har en særlig tilladelse, vises patientoplysninger.

Indstillingen kan anvendes på en enkelt arbejdsstation (dvs. forskellige arbejdsstationer kan indstilles forskelligt).



Læs venligst de følgende forholdsregler omhyggeligt og overhold dem nøje.

- Arbejdsstationerne må ikke efterlades tilgængeligt og uden opsyn under arbejds-sessionerne. Det anbefales at logge ud, når en arbejdsstation forlades.
- Personlige oplysninger gemt i Produktet (såsom password eller brugernes og patienternes personoplysninger) skal beskyttes mod mulige forsøg på uautoriseret adgang gennem passende softwarebeskyttelse (antivirusprogram og firewall). Hospitalet har ansvaret for at implementere denne software og holde den opdateret.



Der kan være personoplysninger til stede i nogle rapporter, der er udarbejdet af Produkt. Sundhedsorganisationen skal håndtere disse dokumenter i henhold til de gældende standarder for privatliv og beskyttelse af personoplysninger.



Klient arbejdsstationer (både stationære og mobile) gemmer ikke patientdata på disken. Patientdata lagres kun inde i databasen, og databaselagring afhænger af sundhedsstrukturens procedurer og valg (eksempler: fysisk maskine, SAN, virtualiseringsmiljø). Patientdata skal behandles efter alle de nuværende standarder for beskyttelse af privatlivets fred og beskyttelse af personoplysninger.



Patient data gemmes ikke i proprietære filer. Det eneste sted, hvor patientdata lagres, er databasen.



I nogle tilfælde transmitteres personlige og/eller følsomme oplysninger i ikke-krypteret format og ved brug af en fysisk usikker forbindelse. HL7 kommunikationer er et eksempel på denne type transmissioner. Den ansvarlige organisation har ansvaret for at iværksætte passende sikkerhedsforanstaltninger for at overholde den gældende lovgivning om privatlivets fred.



Det foreslås at indstille databaseserveren, så Produkt -databasen krypteres på disken. For at aktivere denne indstilling kræves SQL Server Enterprise Edition, og under installationen er det nødvendigt at aktivere indstillingen TDE (Transparent Data Encryption).



Sundhedsorganisationen har ansvaret for at yde grundlæggende uddannelse vedrørende privatlivets fred: dvs. grundlæggende principper, regler, bestemmelser, ansvar og sanktioner i det specifikke arbejdsmiljø. Ascom UMS/forhandleren skal levere specialuddannelse om den bedste måde at bruge produktets på i forhold til beskyttelse af privatlivets fred (dvs. databaseanonymisering, fortrolig tilstand, brugerrettigheder mv.).



Sundhedsorganisationen skal udarbejde og opbevare følgende dokumentation:

- 1) den opdaterede liste over systemadministratorer og vedligeholdelsespersonale;
 - 2) de underskrevne tildelingsformularer og certificering af deltagelse i
-

oplæringskurserne;
3) et register over legitimationsoplysninger, tilladelser og privilegier, der er tildelt brugerne
4) en opdateret liste over produktbrugerne.



Sundhedsorganisationen skal gennemføre, afprøve og certificere en procedure til automatisk deaktivering af brugere, der ikke længere er aktive, efter en vis periode.



Sundhedsorganisationen skal kodificere, implementere og dokumentere en procedure til periodisk verifikation af, at de, der har rollerne som systemadministrator og teknisk vedligeholdelsespersonale.



Sundhedsorganisationen skal foretage revisioner og kontroller vedrørende operatørernes korrekte adfærd.



Databaser, der indeholder patientdata/følsom information, må ikke forlade sundhedsplejefaciliteten uden at blive krypteret/utydeliggørelse.

4.3.1 Egenskaber vedrørende adgangsinformationer og brug

Dette afsnit forklarer Produkt adgangsinformationerne (brugernavn og password) samt brug og opdateringspolitik.

- Iværksæt enhver foranstaltning for at hemmeligholde det personlige brugernavn og password.
- Brugernavn og password skal være private. Sørg for, at ingen kender dit brugernavn og password.
- Hver brugerkonto skal være knyttet til en specifik person. Undgå generelle brugerbetegnelser såsom "ADMIN" eller "SYGEPLEJERSKE". Med andre ord er det af hensyn til sporbarhed nødvendigt, at hver brugerkonto kun benyttes af en eneste bruger.
- Autorisationsprofiler skal kontrolleres og fornys min. en gang om året.
- Det er muligt at gruppere forskellige autorisationsprofiler med hensyntagen til ensartetheden i brugernes opgaver.

- Ved oprettelse af brugerkonti anbefales det altid at benytte en nominal identifikation. Undgå generelle brugerbetegnelser såsom "ADMIN" eller "SYGEPLEJERSKE". Hver konto må kun benyttes af en eneste bruger.
- Hver bruger er tilknyttet en autorisationsprofil, som giver brugerne mulighed for kun at tilgå de funktioner, som har relevans for vedkommendes arbejdsopgaver. Systemadministratoren skal tildele en passende brugerprofil i forbindelse med oprettelse af brugerkontoen. Profilen skal kontrolleres min. en gang om året. Denne revision kan også udføres for klasser af brugere. Procedurerne i forbindelse med definition af brugerprofilen er beskrevet i manualen vedrørende konfiguration af Produkt.
- Passwordet skal bestå af min. 8 tegn.
- Passwordet må ikke referere direkte til brugeren (ved eksempelvis at indeholde brugerens fornavn, efternavn, fødselsdato osv.).
- Passwordet tildeles af systemadministratoren på tidspunktet for oprettelse af brugerkontoen. Det skal ændres af brugeren, når det tages i brug første gang, hvis denne fremgangsmåde er fastlagt i konfigurationen.
- Herefter skal passwordet ændres min. hver 3. måned.
- Hvis brugernavnet og passwordet ikke benyttes i mere end 6 måneder, skal de deaktiveres. Specifikke adgangsinformationer for en bruger, som benyttes til teknisk vedligeholdelse, er en undtagelse. Se den tekniske manual vedrørende konfiguration af denne funktion.
- Brugerens adgangsinformationer skal også deaktiveres, såfremt brugeren ikke længere er kvalificeret til disse adgangsinformationer (hvis brugeren eksempelvis er blevet flyttet til en anden afdeling eller institution). En systemadministrator kan aktivere/deaktivere en bruger manuelt. Fremgangsmåden er beskrevet i manualen vedrørende konfiguration af Produkt.

Følgende oplysninger er forbeholdt systemadministratorer:

Passwordet skal passe til et regulært udtryk i Produkt konfigurationen (default er ^.....* dvs. 8 tegn). Passwordet tildeles af systemadministratoren, når der oprettes en ny konto til en bruger. Systemadministratoren kan stille krav om, at brugeren ændrer passwordet til et personligt password, når det tages i brug første gang. Passwordet udløber efter en vis (konfigurerbar) periode. Herefter skal brugeren ændre passwordet. Det er også muligt (ved hjælp af konfiguration) at hindre udløb af passwordet.

Vedrørende detaljerede oplysninger om fremgangsmåderne i forbindelse med oprettelse af brugerkonti og konfiguration af password henvises til manualen vedrørende konfiguration af Produkt.

4.3.2 Systemadministratorer

Ascom UMS/distributørens teknikere kan i forbindelse med installation, opdateringer og/eller teknisk service få adgang til og håndtere følsomme personoplysninger, som er gemt i Produkt databasen.

Med hensyn til aspekter vedrørende håndtering af følsomme personoplysninger fastsætter Ascom UMS s.r.l. eller distributøren fremgangsmåder og arbejdsinstruktioner i overensstemmelse med den gældende lovgivning om privatlivets fred ("General Data Protection Regulation - EU 2016/679").

I forbindelse med udførelse af de ovenfor anførte aktiviteter konfigureres Ascom UMS/distributørens teknikere som "Systemadministrator" for Produktet (se forordningen af 25.11.2008 fra garanten for privatlivets fred på "Systemadministratorer"). Ascom UMS/distributørens personale, som udfører disse aktiviteter, uddannes på passende måde med hensyn til aspekter vedrørende privatlivets fred og særligt om aspekter vedrørende behandlingen af følsomme oplysninger.

For at opfylde kravene i den gældende lovgivning med hensyn til "Systemadministratorer" skal den ansvarlige institution gøre følgende:

- definere nominel adgang;
- aktivere adgangsloggen både på operativsystemet samt på klient- og serverniveau;
- aktivere adgangsloggen til databaseserveren Microsoft SQL Server (revisionsniveau);
- konfigurere og håndtere alle disse logs for at overvåge adgangen i min. 1 år.

4.3.3 Systemlogs

Produkt registrerer systemlogsene på databasen. Disse logs gemmes i et konfigurerbart tidsrum. Tidsrummet for opbevaring af logs afhænger af deres natur. Default tidsrummene er følgende:

- informationslogs gemmes i 10 dage;
- logs vedrørende advarselsmeddelelser gemmes i 20 dage;
- logs vedrørende alarmmeddelelser gemmes i 30 dage.

Disse tidsrum kan konfigureres. Se manualen vedrørende konfiguration af Produkt for at få oplysninger om fremgangsmåderne i forbindelse med konfiguration.

4.3.4 Lægelog

En delmængde af de tidligere nævnte systemlogfiler, der er defineret i henhold til politikken for hver specifik sundhedsstruktur, der anvender Produktet som "klinisk

relevant" eller "klinisk nyttig", kan sendes til et eksternt system (enten SQL-database eller Syslog) til opbevaring i henhold til sundhedsplejestructurens behov og regler.

4.4 Backup-politik



Det anbefales at sikkerhedskopiere produkt databasen regelmæssigt.

Den Sundhedsorganisation, som benytter Produktet, skal fastlægge en backup-politik, som er optimal i forhold til kravene for datasikkerhed.

Ascom UMS/distributøren er til rådighed med hjælp og støtte i forbindelse med implementering af den valgte politik.

Den Sundhedsorganisation skal sikre, at backup-filerne gemmes på en måde, så der straks kan opnås adgang til dem ved behov for dette.

Hvis oplysningerne gemmes på flytbare hukommelsesindretninger, skal den Sundhedsorganisation beskytte disse indretninger mod uautoriseret adgang. Når disse indretninger ikke længere skal benyttes, skal de enten slettes på en forsvarlig måde eller tilintetgøres.

4.5 Fremgangsmåde ved arbejdsstation ude af drift



Det anbefales at sikkerhedskopiere billedet af harddisken på arbejdsstationerne, så det i tilfælde af udskiftning af hardware er muligt at genoprette driftsmiljøet hurtigt.



Vedligeholdelsesprocedurer og reparationer skal udføres i overensstemmelse med Ascom UMS (eller dets Distributør) procedurer og retningslinjer og kun af Ascom UMS (eller dets Distributør) teknikere eller personale, der er specielt uddannet og udtrykkeligt autoriseret af Ascom UMS (eller dets Distributør).

Den ansvarlige institution, som benytter Produktet, skal fastlægge en backup-politik, som er optimal i forhold til kravene for datasikkerhed. Målet med denne fremgangsmåde er at minimere den tid, som kræves i forbindelse med erstatning af den arbejdsstation, der er ude af drift, med en velfungerende arbejdsstation.

Ascom UMS anbefaler, at sundhedsinstitutionen har et ekstra udstyr og en ekstra pc, hvor Produkt allerede er installeret.

Hvis en Produkt arbejdsstation er ude af drift, kan det ekstra udstyr med det samme erstatte Produkt arbejdsstationen.

Husk altid, at Produkt kun må installeres af uddannet autoriseret personale.

Dette inkluderer personale fra Ascom UMS/distributører og enhver anden specialuddannet person, som er udtrykkeligt autoriseret af Ascom UMS/distributøren. I tilfælde af manglende udtrykkelig, direkte autorisation fra Ascom UMS/distributøren

har hospitalets personale ikke tilladelse til at udføre installation og/eller ændre konfigurationen af Produkt.

Risikoen i forbindelse med deaktivering og erstatning af Produkt arbejdsstationen består i, at arbejdsstationen knyttes sammen med en forkert seng eller stue. Dette kan medføre en "patientombytning", hvilket er en ekstremt farlig situation.

Risikoen i forbindelse med erstatning og/eller genkonfiguration af netværkets udstyr, som er omfattet af Produkt dataindlæsningen (eksempelvis serverport, dockingstation osv.), består i tildeling af de indlæste oplysninger til en forkert patient.

Oplysninger, som indlæses fra patienten, er baseret på Produkt arbejdsstationens IP-adresse. Ændringer kan medføre enten afbrydelser i dataflowet eller i alvorlige tilfælde tildeling af oplysninger til den forkerte patient.



En arbejdsstation, der er ude af drift, og erstatning heraf udgør en potentiel fare. Derfor må indgrebet kun udføres af autoriseret og uddannet personale.

Risikoen i forbindelse med denne fremgangsmåde er tilknytningen af en forkert seng/stue/domæne til arbejdsstationen og herved visning af oplysninger, som vedrører forkerte patienter/senge.

Hvis en Produkt arbejdsstation skal deaktiveres og udskiftes, skal hospitalets personale straks kontakte Ascom UMS anbefaler, at sundhedsinstitutionen definerer en klar og utvetydig fremgangsmåde, og at alt personalet informeres om denne fremgangsmåde.

Vi anbefaler, at hospitalets direktion (eller den som har ledelsen) i den forbindelse definerer en klar og utvetydig fremgangsmåde, og at alt personalet informeres om denne fremgangsmåde.

For at afkorte tidsrummene i forbindelse med erstatning anbefaler Ascom UMS, at sundhedsinstitutionen har et eller flere ekstra udstyr, hvor alle de nødvendige applikationer (OS, firewall, antivirus, RDP osv.) allerede er installeret, og hvor Produktet allerede er installeret men deaktiveret (dvs. ikke kan eksekveres af en bruger uden assistance fra en Ascom UMS tekniker). Hvis en Produkt arbejdsstation er ude af drift, sikrer den ekstra station minimering af tidsrummet for genskabelse (erstatning af hardware) og begrænser samtidig risikoen for tilknytning til forkerte patienter.

Hvis en Produkt arbejdsstation er ude af drift, anbefaler vi at følge denne fremgangsmåde, hvis der er adgang til "ekstra udstyr":

- 1) Sundhedsinstitutionens autoriserede personale erstatter den pc, som er ude af drift, med det "ekstra udstyr".
- 2) Sundhedsinstitutionens personale kontakter Ascom UMS/distributøren og anmoder om aktivering af det "ekstra udstyr".
- 3) Personalet hos Ascom UMS/distributøren deaktiverer den arbejdsstation, som er ude af drift, og konfigurerer det "ekstra udstyr" korrekt.
- 4) Pc'en, som er ude af drift, repareres og klargøres til at blive "ekstra udstyr".

Instruktionerne vedrørende aktivering/deaktivering og erstatning af en Produkt arbejdsstation er forbeholdt systemadministratorer og findes i manualen vedrørende konfiguration af Produkt.

4.5.1 Genkonfiguration/erstatning af netværksudstyr

Hvis det er nødvendigt enten at genkonfigurere eller erstatte netværksudstyr, som er omfattet af Produkt dataindlæsningen, skal sundhedsinstitutionens personale med det samme kontakte Ascom UMS/distributøren og planlægge erstatningen/genkonfigurationen, så Ascom UMS personalet enten kan genkonfigurere Produkt eller give sundhedsinstitutionen alle de nødvendige oplysninger. I den forbindelse anbefales det at fastlægge en klar fremgangsmåde og dele den med det pågældende personale. Manualen vedrørende konfiguration af Produkt indeholder en række generelle anvisninger om dette.

4.6 Forebyggende vedligeholdelse



Vedligeholdelsesprocedurer og reparationer skal udføres i overensstemmelse med Ascom UMS (eller dets Distributør) procedurer og retningslinjer og kun af Ascom UMS (eller dets Distributør) teknikere eller personale, der er specielt uddannet og udtrykkeligt autoriseret af Ascom UMS (eller dets Distributør).

Det anbefales at vedligeholde Produktet min. en gang om året. Endvidere skal det bemærkes, at vedligeholdelsesintervallet skal fastlægges på baggrund af systemets kompleksitet. Hvis systemet er meget komplekst, anbefales det at udføre vedligeholdelsen oftere (eksempelvis to gange om året).

- Se produktinstallations- og konfigurationsvejledningen for vedligeholdelseskонтролlisten.

4.7 Kompatibelt udstyr

Kontakt venligst Ascom UMS/distributøren vedrørende listen over tilgængelige drev.



Den Produkt er ikke designet til at kontrollere, om udstyret fungerer korrekt men snarere til at indlæse og kategorisere kliniske oplysninger.



Frakobling af udstyr, mens det er i gang, medfører afbrydelse af dataindlæsningen på den Produkt. Oplysninger fra udstyret, som mistes under afbrydelsen, genskabes ikke af den Produkt ved den efterfølgende tilslutning.



Deaktiver aldrig alarmmeddelelsen på det medicinske udstyr, medmindre det udtrykkeligt er tilladt af dokumentationen fra producenten af det medicinske udstyr og sundhedsorganisationens procedure.



Korrektheden af de parametre, der vises af den Produkt, skal altid dobbeltcheckes på den originale medicinske enhed, der genererede dem.



Deaktiver aldrig lyden på de arbejdsstationer, hvor den Product er i gang.



Der kan være forsinkelser mellem tidspunktet for generering af alarmer og den faktiske visning af alarmer som følge af forhold, der ikke ligger inden for softwarens kontrol (eksempelvis den måde, hvorpå det faktiske fysiske udstyr er installeret/kablet).

	Af grunde, som ligger uden for kontrol af softwaren, for eksempel, den måde de faktiske fysiske enheder er installeret / kabelslået, forsinkelser er mulig mellem alarm generation og den faktiske alarm display.
	Hvis det almindelige Alaris® drev benyttes, er det nødvendigt at vente mindst 10 sekunder fra frakobling af en infusionspumpe, før en anden tilsluttes.
	Opdatering af data på skærmen i forbindelse med tilslutning, slukning, frakobling og ændring af udstyrets status afhænger af det tidsrum, som det tager udstyret selv at meddele ændringerne. Dette tidsrum afhænger af flere faktorer, herunder udstyrstype og tilslutningstype. For visse former for udstyr kan der være forhold, hvor forsinkelsen i meddelelser om ændringer kan være markant. Det er ikke muligt at oplyse forsinkelsesværdier for alle mulige udstyr, idet disse kan afhænge af forskellige udstyrskonfigurationer og driftsbetingelser
	Drevene, som benyttes til læsning af dataene fra det tilsluttede medicinske udstyr, har en aflæsningscyklus på mindre end 3 sekunder (dvs. alle data fra udstyret læses maks. hvert 3. sekund). Der findes dog udstyr, som meddeler informationerne mindre hyppigt (intervaller på 5-10 sekunder). Se dokumentationen for det specifikke drev vedrørende detaljer om aflæsningscyklussen. I et testmiljø, der er installeret og konfigureret som angivet i "Digistat-serverinstallations- og konfigurationsmanualen", tager det maksimalt 1 sekund at overføre det til Smart Central, så snart et drev registrerer en alarm.
	I tilfælde af strømsvigt er Produktet fuldt funktionsdygtigt igen efter et par minutter og udsender derfor alarmmeddelelser (normalt er dette tidsrum kortere end 3 minutter, men det afhænger af konfigurationen af de anvendte computere).

4.8 Manglende adgang til Produkt

Hvis der er problemer med serverforbindelsen i forbindelse med opstart, viser Produktet en specifik informationsmeddelelse.

Ofte løses problemet med forbindelse automatisk efter et kort tidsrum. Hvis dette ikke er tilfældet, er det nødvendigt at kontakte det tekniske servicecenter (se listen med kontaktoplysninger i afsnit 5).

I sjældne ekstreme tilfælde er det fysisk umuligt at benytte Produktet (i tilfælde af force majeure eller langvarige strømafbrydelser osv.).

Sundhedsinstitutionen, som benytter Produkt, har ansvaret for at definere en nødprocedure, som træder i kraft i sådanne tilfælde. Dette er nødvendigt for at

- 1) muliggøre opretholdelse af arbejdet på afdelingerne.
- 2) Genopret adgangen til Produktet så hurtigt som muligt (backup-politikken er en del af denne styring. Se afsnit 4.3.4).



Sundhedsinstitutionen, som benytter Produkt, har ansvaret for at definere en nødprocedure, som træder i kraft i tilfælde af manglende adgang til Produktet.

Ascom UMS/distributøren tilbyder fuld support ved fastlæggelse af den ovennævnte procedure.

Se listen med kontaktoplysninger i afsnit 5.

5. Producentens kontaktoplysninger

Kontakt venligst først distributøren, som installerede produktet, ved enhver henvendelse.

Her er producentens kontaktoplysninger:

Ascom UMS s.r.l. Unipersonale

Via Amilcare Ponchielli 29, IT-50018, Scandicci (FI), Italien

Tlf. (+39) 055 0512161

Fax (+39) 055 8290392

Teknisk service

support.it@ascom.com

800999715 (gratis, kun Italien)

Info om salg og produkter

it.sales@ascom.com

Generelle oplysninger

it.info@ascom.com

6. Resterende risici

En risikostyringsproces er implementeret i Digistats livscyklus ved at anvende de relevante tekniske standarder. Risikokontrolforanstaltninger er blevet identificeret og implementeret for at reducere risiciene til minimumsniveauet og gøre dem acceptable i forhold til de fordele, produktet medfører. Den samlede restrisiko er også acceptabel, hvis der er tilsvarende fordele.

De restrisici, der er anført nedenfor, er blevet taget i betragtning og er reduceret til det mindste mulige niveau. I lyset af begrebet "risiko" er det ikke muligt at fjerne dem fuldstændigt. Disse restrisici skal meddeles brugerne.

- Manglende evne til at anvende Digistat eller nogle af dets funktionaliteter som forventet, hvilket kan forårsage forsinkelser og/eller fejl i terapeutiske/diagnostiske handlinger
- Uautoriserede handlinger udført af brugere, hvilket kan forårsage fejl i terapeutiske/diagnostiske handlinger og i tildeling af ansvar for disse handlinger
- Tildeling af information til den forkerte patient (utilsigtet patientforveksling), hvilket kan forårsage forsinkelser og/eller fejl i de terapeutiske/diagnostiske handlinger.
- Forkert håndtering af patientoplysninger, herunder fejl ved visualisering, tilføjelse, ændring og sletning af oplysninger, der kan forårsage forsinkelser og/eller fejl i terapeutiske/diagnostiske handlinger.
- Off-label brug af Digistat (f.eks. Produkt anvendt som primær alarmnotifikationssystem, terapeutiske eller diagnostiske beslutninger og interventioner udelukkende baseret på oplysningerne fra Produktet).
- Uautoriseret offentliggørelse af brugere og/eller patienters personlige oplysninger.

RISICI VEDRØRENDE AKTUEL HARDWAREPLATFORM

- Elektrisk stød for patienten og/eller brugeren, som kan medføre kvæstelser og/eller dødsfald for patienten/brugeren.
- Overophedning af hardwarens komponenter, som kan medføre kvæstelser for patienten/brugeren.
- Infektionsrisiko for patient/bruger.