Digistat® Product

Manuale Utente

Revisione 1.0

2019-06-11

Ascom UMS s.r.l. Unipersonale

Via Amilcare Ponchielli 29, 50018, Scandicci (FI), Italy

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

www.ascom.com

Digistat® version 6.0

DIGISTAT® è prodotto da ASCOM UMS s.r.l. (http://www.ascom.com).

Il prodotto ASCOM UMS DIGISTAT® ha la marcatura CE ai sensi della Direttiva 93/42/CEE ("Dispositivi medici") emendata dalla direttiva 2007/47/CE.

ASCOM UMS è certificata conforme alla norma EN ISO 13485:2016 per la "Progettazione, sviluppo, produzione, marketing, vendite, installazione e manutenzione di soluzioni software in ambito sanitario per la gestione della comunicazione, delle informazioni e dei flussi di lavoro, incluse integrazioni con dispositivi medici e sistemi clinici".

Licenza software
Il Prodotto deve essere utilizzato solo dopo aver ottenuto una licenza valida da Ascom UMS o dal Distributore

Licenze e marchi registrati
DIGISTAT® è un Marchio Registrato di ASCOM UMS s.r.l. Tutti gli altri Marchi Registrati sono dei rispettivi possessori.

Nessuna parte di questa pubblicazione può essere riprodotta, trasmessa, trascritta, registrata su supporti di qualunque tipo o tradotta in alcuna lingua, in qualunque forma e con qualunque mezzo senza il consenso scritto di ASCOM UMS.

Sommario

1. Uso del Manuale

Questo manuale utente deve essere utilizzato in combinazione con i manuali specifici dei singoli moduli, elencati di seguito. Fare riferimento ai manuali applicabili, in base ai moduli Digistat in uso nell'Organizzazione sanitaria.

USR ITA Controlbar
USR ITA Controlbar Web
USR ITA Smart Central
USR ITA Codefinder
USR ITA Codefinder Web
USR ITA Diary
USR ITA Fluid Balance
USR ITA Forms
USR ITA Forms Web
USR ITA Image Bank
USR ITA Infusion
USR ITA Messenger
USR ITA On Line
USR ITA Nutrition
USR ITA OranJ
USR ITA Patient Explorer
USR ITA Scoring Calculator
USR ITA Smart Scheduler
USR ITA Stock Management
USR ITA Therapy
USR ITA MDI Web
USR ITA Vitals Web
USR ITA Smart Central Mobile
USR ITA Vitals Mobile
USR ITA Voice Notes Mobile
USR ITA Identity Mobile
USR ITA Collect Mobile

1.1 Intenti

Lo sforzo effettuato nel compilare il presente manuale è volto ad offrire tutte le informazioni necessarie per garantire un utilizzo sicuro del software Digistat e per consentire di identificare il fabbricante.
Il presente documento vuole inoltre essere una guida di riferimento per l'utente che desideri sapere "come fare" a compiere una determinata operazione, nonché una guida al corretto uso di Digistat affinché possano essere evitati usi impropri e potenzialmente pericolosi.

1.2 Caratteri usati e terminologia

L'uso di Digistat presuppone una conoscenza di base dei più comuni termini e concetti informatici. Allo stesso modo, la comprensione del presente manuale è subordinata a tale conoscenza.
Si ricordi comunque che l'uso di Digistat deve essere consentito soltanto a personale professionalmente qualificato ed opportunamente addestrato.

I riferimenti incrociati interni al documento funzionano, nel caso si stia consultando la versione on-line del manuale, come collegamenti ipertestuali. Ciò significa che ogni volta che si trova il riferimento a una immagine ("**Error! Reference source not found.**", ad esempio) o a un paragrafo ("paragrafo 2.2", ad esempio) è possibile cliccare sul riferimento per accedere direttamente a quella particolare figura o a quel particolare paragrafo.

1.2.1 Convenzioni

Nel documento sono utilizzate le seguenti convenzioni:

- I nomi dei pulsanti, le voci dei menu, le opzioni, le icone, i campi e qualunque cosa nell'interfaccia possa essere utilizzato dall'utente (tramite tocco o click o selezione) sono formattate in **grassetto**.
- I nomi/titoli delle schermate, delle finestre e delle "tabs" sono citate "Fra virgolette".
- Il codice di programmazione è formattato in carattere Courier.
- Il simbolo ➢ indica un'azione che l'utente può effettuare per portare a termine una certa procedura.
- I riferimenti a documenti esterni sono formattati in *corsivo*.

1.3 Simbologia

Nel manuale sono utilizzati i seguenti simboli.

Informazioni utili

Questo simbolo appare in corrispondenza di informazioni aggiuntive riguardanti le caratteristiche e l'uso del software Digistat. Si può trattare di esempi esplicativi, di procedure alternative o di qualsiasi informazione "a lato" si ritenga utile ad una più approfondita comprensione del prodotto.

Attenzione!
Il simbolo è usato per evidenziare informazioni volte a prevenire un uso improprio del software o per sottolineare procedure critiche che potrebbero portare a situazioni rischiose. È perciò necessario prestare estrema attenzione ogni volta che il simbolo appare.

I seguenti simboli sono usati nel box informativo Digistat (Fig 1):

Indica nome e indirizzo del fabbricante

Attenzione, consultare la documentazione allegata

1.3.1 Informazioni su Digistat

Il pulsante Info sul menu principale Digistat apre una finestra che riporta informazioni generali sul Prodotto (versione installata, licenze etc. - Fig 1). Si veda il manuale utente di Digistat® Control Bar per ulteriori informazioni (*USR ITA Control Bar*).

Fig 1

2. Introduzione a Digistat

Digistat è un dispositivo software per la gestione dei dati paziente, progettato specificamente per l'uso da parte di medici, infermieri o amministratori.
Il pacchetto software è composto da un insieme di moduli che possono essere utilizzati singolarmente oppure essere integrati tra di loro per fornire una soluzione completa per la gestione dei dati paziente.

Digistat può essere usato sia in Terapia Intensiva che in Corsia che in Sala Operatoria. L'architettura modulare e le estese capacità di configurazione del software consentono di adeguare il sistema di gestione dati paziente alle necessità dell'utente e di espanderlo con nuovi moduli.

Si accede a Digistat solo attraverso l'inserimento di nome utente e password. Ad ogni utente è assegnato un profilo dettagliato che permette di accedere alle sole funzioni di sua pertinenza. Un sistema automatico genera un registro di tutte le operazioni effettuate dagli utenti.

2.1 L'architettura modulare

"Architettura modulare" significa che, all'interno di uno stesso ambiente (Digistat nel caso presente), caratterizzato da una veste grafica propria, da scopi precisi e da determinate regole d'uso, possono essere integrate diverse applicazioni (o "moduli"), aventi finalità specifiche. L'integrazione può avvenire in momenti diversi, e con modalità concordate con l'organizzazione ospedaliera, in modo che Digistat si adatti alle esigenze specifiche della struttura che la usa e agli eventuali cambiamenti che, nel tempo, possono intervenire nelle esigenze dell'organizzazione in questione.

2.2 Destinazione d'uso prevista

Il software Digistat® (da qui in poi "Prodotto") acquisisce, registra, organizza, trasmette e visualizza informazioni del paziente e dati relativi al paziente, inclusi i dati e gli eventi provenienti dai sistemi e dai dispositivi medici collegati, sia informazioni inserite manualmente, allo scopo di offrire un supporto al personale clinico nella diagnosi e nel trattamento dei pazienti e di creare una cartella clinica elettronica.

- Il Prodotto produce una documentazione del paziente elettronica configurabile basata sia sui dati e le informazioni acquisite, sia sulla documentazione automatizzata e manuale dell'attività del reparto.

- Il Prodotto fornisce visualizzazione e informazione acustica secondaria automatica dei dati acquisiti, degli eventi, dello stato corrente e delle condizioni operative dei sistemi e dei dispositivi medici connessi su appositi dispositivi di visualizzazione. Il Prodotto può inoltre essere configurato per

inviare dati e informazioni su eventi, stato e condizioni operative al sistema di messaggistica Ascom.

- Il Prodotto supporta il miglioramento dei flussi di lavoro del personale infermieristico relativi alla gestione degli allarmi provenienti dai sistemi e dai dispositivi medici collegati.

- Il Prodotto supporta la documentazione della terapia prescritta, della sua preparazione e della sua somministrazione.

- Il Prodotto supporta la registrazione, la validazione e la visualizzazione dei grafici relativi ai parametri vitali basati sui dati e le informazioni acquisite.

- Il Prodotto fornisce reportistica, grafici e statistiche configurabili basati sui dati registrati utilizzati da professionisti del settore sanitario al fine di analizzare l'efficienza, la produttività, la capacità e l'utilizzo di risorse, e la qualità della cura.

Il Prodotto **non** sostituisce o replica la visualizzazione primaria di dati e allarmi dei sistemi e dei dispositivi collegati e **non** controlla, né monitora o altera il comportamento dei suddetti sistemi e dispositivi o la notifica di allarmi ad essi associata.

Il Prodotto **non** è destinato ad essere usato come strumento di diagnosi diretta o di monitoraggio dei parametri fisiologici vitali.

Il Prodotto è destinato ad essere usato in ambiente clinico/ospedaliero da professionisti del settore sanitario appositamente formati e si basa sull'uso appropriato ed operatività dell'infrastruttura informatica e di comunicazione esistente nella struttura sanitaria, così come sull'uso appropriato ed operatività dei dispositivi di visualizzazione esistenti, e dei sistemi e dispositivi medici collegati.

In aggiunta, il Prodotto fornisce funzionalità ed interfacce specifiche destinate ad utenti non professionisti, che possono utilizzarle da remoto per fini non clinici per la visualizzazione di informazioni, reportistica, grafici e statistiche, senza che sia data alcuna possibilità di aggiungere, modificare o cancellare alcun tipo di dato o informazione.

Il Prodotto è un software stand-alone che è installato su server e computer che devono essere conformi alle specifiche tecniche hardware e software fornite insieme al Prodotto.

2.2.1 Avvertenze per la sicurezza

L'Utente dovrà basare le decisioni e gli interventi terapeutici e diagnostici solamente a partire dalla verifica diretta della fonte primaria di informazioni. È esclusiva responsabilità dell'Utente la verifica della correttezza dell'informazione fornita dal Prodotto, nonché l'uso appropriato della stessa.

Solo le stampe firmate digitalmente o su carta da medici professionisti autorizzati devono essere considerate valide come documentazione clinica. Nel firmare le suddette stampe, l'Utente certifica di aver verificato la correttezza e la completezza dei dati presenti sul documento.

Nell'inserire dati relativi al paziente l'Utente ha la responsabilità di verificare che l'identità del paziente, il reparto/unità della Struttura Sanitaria e il letto visualizzati sul Prodotto siano corretti. Questa verifica è di importanza fondamentale in caso di operazioni critiche quali, ad esempio, la somministrazione di farmaci.

La Struttura Sanitaria ha la responsabilità di identificare e implementare procedure appropriate per assicurare che i potenziali errori che si verificano sul Prodotto e/o nell'uso del Prodotto siano rilevati e corretti velocemente e che non costituiscano un rischio per il paziente o l'operatore. Queste procedure dipendono dalla configurazione del Prodotto e dalle modalità d'uso scelte dalla Struttura Sanitaria.

Il Prodotto può fornire, a seconda della configurazione, accesso ad informazioni sui farmaci. La Struttura Sanitaria ha la responsabilità di verificare, all'inizio e poi periodicamente, che questa informazione sia corretta e aggiornata.

Il Prodotto non costituisce un sistema primario di notifica degli allarmi; esso non è progettato per essere utilizzato in sostituzione del monitoraggio diretto degli allarmi generati dai dispositivi medici. Questa limitazione è dovuta, insieme alle altre ragioni, alle specifiche e limitazioni dei protocolli di comunicazione dei dispositivi medici.

Nel caso che alcuni dei dispositivi in uso per il Prodotto si trovino all'interno dell'area paziente o siano collegati ad attrezzature che si trovano all'interno dell'area paziente, la Struttura Sanitaria ha la responsabilità di assicurarsi che tutto l'insieme sia conforme alla norma internazionale IEC 60601-1 e a qualsiasi altro requisito determinato dalla legislazione locale.

L'uso del Prodotto deve essere consentito, attraverso apposita configurazione degli account degli utenti e attraverso la sorveglianza attiva, soltanto ad Utenti 1) addestrati secondo le indicazioni del Prodotto da personale autorizzato dal produttore o dai suoi distributori, e 2) professionalmente qualificati ad interpretare correttamente le informazioni da esso fornite, ed a implementare le procedure di sicurezza opportune.

Il Prodotto è un software stand-alone che opera su comuni computer e dispositivi mobili collegati alla rete locale della Struttura Sanitaria. La Struttura Sanitaria è responsabile di proteggere adeguatamente computer, dispositivi e rete locale contro cyber-attacchi.

Il Prodotto deve essere installato solo su computer e dispositivi che soddisfano i requisiti hardware minimi e solo sui sistemi operativi supportati.

2.3 Uso “Off-label” del Prodotto

Ogni uso del Prodotto al di fuori di quanto indicato nella Destinazione d’uso (usualmente chiamato uso “off-label”) è sotto la completa discrezionalità e responsabilità dell’utente e della organizzazione responsabile. Il produttore non garantisce in nessuna forma la sicurezza e la adeguatezza allo scopo del Prodotto quando esso viene usato al di fuori di quanto indicato nella Destinazione d’uso.

Il Prodotto **non è** un sistema primario distribuito di allarme.

2.4 Popolazione dei pazienti

Il Prodotto è una applicazione software che non è in contatto col paziente.
La popolazione e le condizioni dei pazienti sono stabilite dai dispositivi medici e da sistemi con cui il prodotto è connesso.
In aggiunta, si applicano le seguenti limitazioni:

- Il peso del paziente deve essere compreso fra 0.1kg e 250kg
- L’altezza del paziente deve essere compresa fra 15cm e 250cm

2.5 Responsabilità della Struttura Sanitaria

Ascom UMS declina ogni responsabilità per le conseguenze sulla sicurezza ed efficienza del dispositivo determinate da interventi tecnici di riparazione o manutenzione non espletati da personale del proprio Servizio Tecnico o da Tecnici autorizzati da Ascom UMS.

Si richiama l'attenzione dell'utente e del responsabile legale dell’organizzazione sanitaria in cui l'apparecchio viene utilizzato sulle responsabilità di loro competenza, alla luce della legislazione vigente in materia di sicurezza nei luoghi di lavoro (ad esempio, in Italia il Decreto legislativo no. 81 del 09/04/2008) e di Vigilanza sul campo per incidenti pericolosi o potenzialmente pericolosi.

Il Service di Ascom UMS è in grado di fornire ai clienti il supporto necessario a mantenere nel tempo la sicurezza ed efficienza delle apparecchiature fornite, garantendo la competenza, dotazione strumentale e le parti di ricambio adeguate a garantire nel tempo la piena rispondenza dei dispositivi alle originarie specifiche costruttive.

Il prodotto è stato progettato prendendo in considerazione i requisiti e le “best practices” presenti nello standard IEC 80001 e nei suoi documenti tecnici correlati. In particolare lo IEC/TR 80001-2-5:2014 ha grande rilevanza per il prodotto. Così come reso chiaro nella serie IEC 80001 parte delle attività necessarie e delle misure di controllo del rischio sono sotto il controllo e la responsabilità dell’organizzazione ospedaliera. Si faccia riferimento agli standard e ai documenti collegati al fine di identificare le attività necessarie e le misure di controllo del rischio; in particolare si faccia riferimento ai seguenti documenti:

- 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 Responsabilità del fabbricante

Ascom UMS è responsabile agli effetti della sicurezza, affidabilità e delle prestazioni del prodotto soltanto se:

- l'uso e la manutenzione siano conformi a quanto indicato nella documentazione del Prodotto (che include il presente manuale d'uso);
- l’installazione e la configurazione sono eseguite da personale appositamente formato e autorizzato da Ascom UMS
- configurazioni, modifiche e manutenzione siano effettuate da personale formato ed espressamente autorizzato da Ascom UMS;
- l'ambiente nel quale il Prodotto venga utilizzato sia conforme alle prescrizioni di sicurezza e alle normative applicabili;
- l'ambiente nel quale il Prodotto venga utilizzato (inclusi computer, collegamenti elettrici, attrezzature) sia conforme alla normativa applicabile.

Qualora a seguito della fornitura elettrica venga a costituirsi un "sistema elettromedicale", attraverso il collegamento elettrico e funzionale con i dispositivi medici, rimangono a carico dell'organizzazione ospedaliera la verifica di sicurezza elettrica e il collaudo del sistema elettromedicale risultante, anche nel caso in cui Ascom UMS abbia effettuato in tutto o in parte i collegamenti necessari.

2.7 Rintracciabilità del Prodotto

Con lo scopo di assicurare la rintracciabilità del prodotto e azioni correttive sul posto, in conformità alle direttive EN 13485 e MDD 93/42/EEC, all'acquirente è richiesto di informare ASCOM UMS o il suo Distributore riguardo qualunque trasferimento di proprietà mediante documentazione scritta attestante il Prodotto ed i dati identificativi del precedente proprietario ed il nuovo.
I dati del Prodotto possono essere trovati nell'etichetta del Prodotto (schermata "A proposito" mostrata all'interno del prodotto – si veda Pagina **Error! Bookmark not defined.**).
In caso di dubbi o domande a proposito dell'identificazione del Prodotto, per favore contatta l'assistenza tecnica d ASCOM UMS o del suo Distributore (per i contatti si veda pagina **Error! Bookmark not defined.**).

2.8 Sistema di sorveglianza post-vendita

Il dispositivo marcato CE è soggetto a sorveglianza post-vendita – che ASCOM UMS e il suo Distributore eseguono per ogni copia venduta – riguardo rischi potenziali ed attuali, sia per il paziente che per l'Utente, durante il ciclo di vita del Prodotto.
In caso di degradazione delle caratteristiche del Prodotto, prestazioni scadenti o istruzioni dell'utente inadeguate che possono o possono essere state un rischio per la salute del paziente o dell'Utente o per la sicurezza dell'ambiente, l'Utente deve immediatamente darne notifica ad ASCOM UMS o al suo Distributore.
Alla ricezione di un feedback da parte dell'Utente ASCOM UMS o il suo Distributore avvieranno immediatamente il processo di verifica e revisione ed effettueranno le azioni correttive necessarie.

2.9 Vita del Prodotto

Il ciclo di vita del Prodotto non dipende dal logoramento o altri fattori che possono compromettere la sicurezza. Esso è influenzato dall'obsolescenza dei componenti dell'ambiente software (ad esempio OS, Framework .NET) ed è pertanto fissato a cinque anni dalla data di rilascio della versione del Prodotto considerata (disponibile nella finestra "Informazioni").

3. Specifiche Software e Hardware

Il Prodotto deve essere installato esclusivamente da personale addestrato e autorizzato. Questo include il personale di Ascom UMS/Distributore e qualsiasi altra persona specificamente formata e esplicitamente autorizzata da Ascom UMS/Distributore. In mancanza di una esplicita, diretta autorizzazione da parte di Ascom UMS/Distributore, il personale della struttura clinica non è autorizzato ad eseguire procedure di installazione o a modificare la configurazione del Prodotto.

Il Prodotto deve essere utilizzato solamente da personale addestrato. Il Prodotto non può essere utilizzato in mancanza di una appropriata formazione, effettuata dal personale di Ascom UMS/Distributore.

Le informazioni fornite in questa sezione coprono gli obblighi informativi a carico del produttore identificati dalla norma IEC 80001-1:2010 (Application of risk management for IT-networks incorporating medical devices).
In base alla norma IEC 60601-1, per le stazioni di lavoro al posto letto, o che comunque sono posizionate in “Area Paziente”, è necessario l’uso di dispositivi di grado medicale. Usualmente in questi luoghi vengono utilizzati PANEL PC di grado medicale. Se richiesto Ascom UMS può suggerire alcune possibili apparecchiature di questo tipo.

Un lettore PDF supportato deve essere installato sulle postazioni di lavoro al fine di visualizzare l’help on line. Si veda il paragrafo **Error! Reference source not found.** per i requisiti Software delle postazioni centrali e al posto letto.

3.1 Posto letto e Centrale

3.1.1 Hardware

Requisiti hardware minimi:

- Processore Intel® I3 (o superiore)
- Memoria RAM 4 GB
- Hard Disk con almeno 60 GB di spazio libero
- Monitor con risoluzione 1024 x 768 o superiore (consigliato 1920 x 1080)
- Mouse o altro dispositivo compatibile. Raccomandato touch screen.
- Interfaccia Ethernet 100 Mb/s (o superiore)
- Lettore CD/DVD oppure possibilità di copiare i file di installazione

Se una workstation Centrale / Posto Letto è configurata per visualizzare flussi video (funzione supportata solo in Smart Central o OranJ con integrazione telecamera abilitata) i requisiti minimi sono i seguenti:

- Processore Intel® I3 (o superiore)
- Memoria: 4 GB di RAM + 50 MB per ogni stream video di una telecamera visualizzato contemporaneamente (ad esempio con 20 videocamere visualizzate 4 GB + 1 GB)
- Hard Disk con almeno 60 GB di spazio libero
- Monitor con risoluzione 1024 x 768 o superiore (consigliato 1920 x 1080)
- Mouse o altro dispositivo compatibile. Raccomandato touch screen.
- Interfaccia Ethernet 100 Mb/s (o superiore)

Alcuni esempi: con Intel i7 6600 2,60 Ghz, con uno streaming di 10 telecamere con un bitrate di 3138 kbps, l'utilizzo della CPU è circa del 45%. Con I3 7100t 3.4 Ghz, con uno streaming di 16 telecamere con un bitrate di 958 kbps, l'utilizzo della CPU è di circa il 30%.

3.1.2 Sistema Operativo

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

3.1.3 Software di sistema

- Microsoft .NET Framework v4.5
- Adobe Acrobat Reader versione 10

Il manuale utente del Prodotto è un file in formato PDF generato in accordo alla versione standard PDF 1.5 ed è perciò leggibile da Adobe Acrobat 6.0 o superiore. Inoltre, il manuale utente del Prodotto è stato testato con Adobe Acrobat Reader 10. L'organizzazione ospedaliera può usare una differente versione di Acrobat Reader: la verifica del

	Prodotto installato include la verifica della corretta leggibilità del manuale utente.

3.2 Server

3.2.1 Hardware

Requisiti hardware minimi (piccole installazioni, 20 letti, 4 dispositivi per letto):

- Processore Intel® I5 con quattro “core”.
- Memoria RAM 8 GB
- Hard Disk con almeno 120 GB di spazio libero
- Interfaccia Ethernet 100 Mb/s (o superiore). Raccomandato 1 GB.
- Lettore CD/DVD oppure possibilità di copiare i file di installazione

Requisiti hardware raccomandati (installazione di medie dimensioni, 100 letti, 4 dispositivi per letto, Connect e Mobile):

- Processore Intel® I7 con otto“core”.
- Memoria RAM 32 GB
- Hard Disk con almeno 120 GB di spazio libero
- Interfaccia Ethernet 100 1 GB
- Lettore CD/DVD oppure possibilità di copiare i file di installazione

3.2.2 Sistema Operativo

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

3.2.3 Software di sistema

- 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 è stato testato sul dispositivo “ASCOM Myco SH1 and SH2 Wi-Fi and Cellular Smartphone”, con versione Android 4.4.2 (Myco1) o 5.1 (Myco1 / Myco2) o 8.0 (Myco3). Quindi è compatibile con i dispositivi mobili Myco1, Myco2 e Myco3.

L’applicazione è progettata per essere compatibile con altri dispositivi Android con una dimensione minima dello schermo di 3.5’’; la compatibilità con ciascun dispositivo specifico deve quindi essere verificata prima dell’uso in ambito clinico.

Si prega di contattare ASCOM UMS o il distributore di riferimento per la lista completa dei dispositivi che supportano l'applicazione Digistat® Mobile.

3.4 Digistat Web

Le applicazioni Digistat web sono supportate dai seguenti browser:

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

Si faccia uso dei soli browser supportati.

Una postazione Digistat Web deve avere sempre il Web Browser visibile in primo piano. Oltre a questo, il browser Web non deve essere usato per altro che non sia Digistat Web (il che implica che la homepage di Digistat Web deve essere la homepage di default del browser).

Il Display Scaling del browser deve essere sempre impostato al 100%.

Se la rete locale è almeno in parte basata su connessioni Wi-Fi, data la natura intermittente di tali connessioni, possono esserci disconnessioni che attivano la modalità "Disconnesso" (un fondo grigio che copre Digistat Web). In questi casi Digistat Web non è disponibile. L'organizzazione ospedaliera deve adoperarsi per assicurare una copertura Wi-Fi ottimale e istruire lo staff clinico su come gestire queste indisponibilità temporanee.

3.5 Avvertenze generali

L’applicazione “MDI Web” presentata in questo Manuale Utente può essere utilizzata solo a scopo dimostrativo. Essa non può essere usata in un ambiente di lavoro.

Per utilizzare correttamente il Prodotto è necessario che il Display Scaling di Microsoft Windows sia impostato al 100%. Impostazioni diverse possono impedire l’esecuzione del prodotto oppure creare malfunzionamenti a livello di rappresentazione grafica. Per impostare il valore Display Scaling consultare la documentazione di Microsoft Windows.

La risoluzione verticale minima di 768 è supportata solo nei casi in cui il Prodotto sia configurato per essere eseguito a full-screen oppure quando la barra di Windows è configurata per nascondersi automaticamente (Auto-hide).

I computer e gli altri dispositivi impiegati devono essere idonei per l’ambiente in cui vengono utilizzati e devono pertanto rispettare le norme e i regolamenti rilevanti. Si raccomanda al personale competente di effettuare i dovuti controlli

È obbligatorio seguire le indicazioni del produttore per l'immagazzinamento, il trasporto, l’installazione, la manutenzione e l’eliminazione dell'hardware di terze parti. Tali operazioni dovranno essere effettuate solo da personale competente e opportunamente addestrato.

L’uso del Prodotto con un qualsiasi software che sia diverso da quelli specificati nel presente documento potrebbe compromettere la sicurezza, l’efficacia e le funzionalità del Prodotto stesso. Un uso del genere potrebbe portare un maggiore rischio per gli utenti e/o i pazienti. È obbligatorio consultare un tecnico di Ascom UMS o di un distributore autorizzato prima di usare il Prodotto con un qualsiasi software che sia diverso da quelli esplicitamente menzionati in questo documento.
Se l’hardware sul quale funziona il Prodotto è un computer di tipo stand-alone, l’utente è tenuto a non installare alcun altro software

(programmi di utilità o applicazioni) sul computer stesso. Si suggerisce di implementare una politica di permessi che impedisca agli utenti di effettuare la procedura di installazione di un nuovo software.

L'organizzazione ospedaliera è tenuta a implementare un meccanismo di sincronizzazione della data ed ora delle workstation su cui gira il Prodotto con una sorgente temporale di riferimento.

Si raccomanda di disabilitare l'accesso alla rete Internet sulle postazioni di lavoro "client" e sui dispositivi mobili sui quali è usato il Prodotto.
In alternativa la struttura clinica dovrà implementare le misure di sicurezza necessarie a garantire una protezione adeguata dagli attacchi informatici e dall'installazione di applicazioni non autorizzate.

Parti del prodotto fungono da visualizzatore di flussi video; il Prodotto non è la fonte del flusso video e non registra queste informazioni in alcun modo. È responsabilità dell'organizzazione sanitaria gestire il sistema da una prospettiva di protezione dei dati compresa l'installazione e la configurazione delle telecamere sorgente.

Parti del Prodotto trattano audio e immagini relative agli utenti e / o ai pazienti inclusa l'acquisizione, l'elaborazione e la registrazione. È responsabilità dell'organizzazione sanitaria implementare le procedure necessarie per conformarsi alla normativa locale sulla protezione dei dati, inclusi, a titolo esemplificativo ma non esaustivo, i limiti di utilizzo e formazione degli utenti.

La funzionalità di streaming video sulle workstation desktop è stata testata con i codec video H264 e H265.
Qualsiasi altro codec video presente o installato da applicazioni di terze parti (ad esempio VLC Media Player) deve essere testato prima dell'uso.

Attenzione: ogni sorgente video supporta un numero massimo di client connessi simultaneamente. È responsabilità dell'organizzazione sanitaria determinare questo numero massimo e informare gli utenti.

La funzionalità di streaming video su dispositivi mobili supporta solo flussi video RTSP con i seguenti tipi di autenticazione:

- Nessuna autenticazione;
- Autenticazione di base;
- Autenticazione Digest.

La funzionalità di streaming video su dispositivi mobili supporta solo i codec video H263, H264 e H265.

3.6 Firewall e Antivirus

Per proteggere il Prodotto da possibili attacchi informatici è necessario che:

- Il Firewall di Windows sia attivo sia sulle workstations che sul server;
- Su workstation e server sia attivo e regolarmente aggiornato un software Antivirus/Antimalware.

È carico dell'organizzazione clinica responsabile assicurarsi che queste due protezioni siano messe in atto. Ascom UMS ha testato il prodotto con l'antivirus F-SECURE. Considerate però le scelte e le politiche preesistenti nell'ospedale, l'identificazione dell'Antivirus specifico è lasciata all'organizzazione responsabile. Ascom UMS non può assicurare che il Prodotto sia compatibile con ogni antivirus o configurazione dello stesso.

Con l'uso dell'antivirus Kaspersky sono state segnalate delle incompatibilità con parti del Prodotto la cui soluzione ha richiesto la definizione di regole specifiche nell'antivirus stesso.

Si consiglia fortemente di mantenere aperte le sole porte TCP ed UDP effettivamente necessarie. Queste possono variare in base alla configurazione del Prodotto. Si raccomanda quindi di rivolgersi all'assistenza tecnica Ascom UMS per tutti i dettagli del caso.

3.6.1 Ulteriori precauzioni raccomandate per la sicurezza informatica

Allo scopo di rafforzare ulteriormente la sicurezza informatica e di proteggere il Prodotto, si raccomanda fortemente di:

- pianificare e implementare lo “Hardening” dell’infrastruttura informatica, inclusa la piattaforma informatica che rappresenta l’ambiente di lavoro del Prodotto,
- implementare un “Intrusion Detection and Prevention System (IDPS) - Sistema di rilevazione e prevenzione delle intrusion informatiche,
- eseguire un test di penetrazione (Penetration Test) e, se in seguito al test è riconosciuta una qualsiasi debolezza, eseguire tutte le azioni necesarie a mitigare il rischio di intrusione informatica,
- mettere fuori uso tutti i dispositivi che non è più possibile aggiornare,
- pianificare ed eseguire una verifica periodica dell’integrità dei file e delle configurazioni,
- implementare una soluzione DMZ (demilitarized zone - zona demilitarizzata) per i server web che devono essere esposti su internet.

3.7 Caratteristiche della rete locale

In questo paragrafo sono elencate le caratteristiche richieste alla la rete locale sulla quale è installato il Prodotto affinché funzioni correttamente.

- il Prodotto utilizza traffico di tipo TCP/IP standard.
- La rete LAN deve essere priva di congestioni e/o saturazioni.
- il Prodotto richiede una LAN di almeno 100 Mbps alle postazioni utente. È auspicabile la presenza di dorsali Ethernet da 1Gbps.
- Non devono essere presenti filtri sul traffico TCP/IP tra workstations, server e dispositivi secondari.
- Se i dispositivi (server, workstation e dispositivi secondari) sono collegati a sottoreti diverse ci deve essere routing tra tali sottoreti.
- Si suggerisce l’adozione di tecniche di ridondanza al fine di assicurare il servizio di rete anche in caso di malfunzionamento.
- Si suggerisce una programmazione condivisa degli interventi di manutenzione programmata in modo che Ascom UMS o il distributore autorizzato possa supportare la struttura sanitaria nel gestire in modo ottimale i disservizi.

Se la rete non rispetta le caratteristiche richieste si ha un rallentamento progressivo nel prodotto fino ad arrivare ad errori di timeout sull’accesso ai dati; ciò fino ad entrare in modalità “Recovery”.

Nel caso si utilizzi una rete WiFi, a causa della possibile intermittenza del collegamento WiFi, si potrebbero avere disconnessioni di rete con conseguente attivazione del “Recovery Mode” e indisponibilità del Prodotto. L’organizzazione responsabile deve attivarsi per garantire una ottimale copertura e stabilità della rete WiFi e istruire il personale coinvolto sulla gestione delle possibili temporanee disconnessioni.

Al fine di cifrare i dati trasmessi tramite reti wireless, si raccomanda di adottare il più alto protocollo di sicurezza disponibile; in ogni caso non inferiore al WPA2.

3.7.1 Impatto del Prodotto sulla rete ospedaliera

L’introduzione del Prodotto ha un impatto sulla rete locale della struttura ospedaliera. Questo paragrafo contiene informazioni riguardo al traffico generato dal Prodotto sulla rete, in modo che l’organizzazione responsabile possa valutare i rischi dell’introduzione del dispositivo nella rete ospedaliera. La banda utilizzata dal Prodotto dipende da molti fattori. Fra questi, i principali sono:

- il numero di postazioni,
- il numero di postazioni configurate come centrali,
- il numero e il tipo di dispositivi adibiti all’acquisizione dei dati,
- le interfacce con sistemi esterni,
- la configurazione e le modalità di uso del Prodotto.

La banda utilizzata dal Prodotto dipende principalmente dall’acquisizione dei dati dai dispositivi medici. In una configurazione con acquisizione da 100 posti letto dove ogni posto letto raccoglie dati da 1 ventilatore, 1 monitor paziente e 3 pompe a infusione e con 10 postazioni di lavoro che mostrano 10 posti letto ciascuna, si possono considerare i seguenti valori di occupazione di banda (i valori sono indicativi):

Media: 0.8 – 6 Mbit/s

Picco: 5 – 25 Mbit/s

Per configurazioni nelle quali non ci sia acquisizione dati dai dispositivi medici, i valori di occupazione di banda sono inferiori a quelli specificati sopra.

4. Prima di iniziare

4.1 Avvertenze per la manutenzione e l'installazione

Le seguenti avvertenze riguardanti la corretta installazione e la manutenzione del Prodotto devono essere rispettate scrupolosamente.

L'installazione, la manutenzione e le procedure di riparazione devono essere effettuate in accordo alle direttive e linee guida fornite da Ascom UMS/Distributore e solo da tecnici e personale formato e autorizzato da Ascom UMS/Distributore.

Si raccomanda all'organizzazione ospedaliera che fa uso del Prodotto di stipulare un contratto di manutenzione con Ascom UMS o un Distributore autorizzato in modo da assicurare che la versione installata del prodotto sia sempre la più recente e aggiornata.

Si ricorda che il Prodotto può essere installato e configurato solo da personale addestrato ed autorizzato. Questo include il personale Ascom UMS o dei Distributori autorizzati e ogni altra persona specificamente addestrata e autorizzata da Ascom UMS o dal Distributore.
Analogamente, gli interventi di manutenzione e riparazione sul Prodotto possono essere effettuati solo da personale addestrato ed autorizzato e devono rispettare le procedure e linee guida aziendali. Questo include il personale Ascom UMS/Distributore e ogni altra persona specificamente addestrata e autorizzata da Ascom UMS/Distributore.

Il Prodotto può essere installato e configurato solo da personale addestrato ed autorizzato. Questo include il personale Ascom UMS o del Distributore autorizzato e ogni altra persona specificamente addestrata e autorizzata da Ascom UMS o dal Distributore.

- Usare solo dispositivi di terze parti raccomandati da Ascom UMS o distributore.
- Solo personale addestrato e autorizzato può installare dispositivi di terze parti. La scorretta installazione di dispositivi di terze parti può creare il rischio di lesioni al paziente e agli operatori.
- Rispettare scrupolosamente le indicazioni del costruttore per l'installazione dell'hardware di terze parti.
- Effettuare una regolare manutenzione in accordo alle istruzioni contenute in questo manuale e in quelli forniti dai produttori di terze parti.

- La Struttura Sanitaria è responsabile per la selezione delle apparecchiature adatte all'ambiente in cui sono installate ed utilizzate. La Struttura Sanitaria deve tra gli altri obblighi considerare la sicurezza elettrica, le emissioni EMC, interferenze dei segnali radio, disinfezione e pulizia. Attenzione dovrà inoltre essere posta ai dispositivi installati nell'area paziente.

4.2 Precauzioni e avvertimenti

Per garantire affidabilità e sicurezza del software durante l'uso attenersi scrupolosamente a quanto indicato in questa sezione del manuale.

L'organizzazione ospedaliera deve assicurare che la manutenzione del Prodotto e di qualsiasi dispositivo di terze parti sia implementata come richiesto al fine di garantirne sicurezza ed efficienza e ridurre il rischio di malfunzionamenti e possibili situazioni di pericolo per il paziente e l'utente.

Il Prodotto deve essere utilizzato soltanto da personale addestrato e autorizzato.

4.3 Gestione della Privacy

Precauzioni appropriate devono essere prese al fine di proteggere la privacy di utenti e pazienti, e di assicurare che i dati personali siano elaborati nel rispetto dei diritti dei soggetti coinvolti, delle libertà fondamentali, della dignità personale, con particolare riguardo per la confidenzialità, l'identità personale e il diritto alla protezione dei dati personali

---

Per 'Dati personali' si intende qualsiasi informazione riguardante una persona naturale identificata o identificabile ('soggetto dei dati'); una persona naturale identificabile è un individuo che possa essere identificato, direttamente o indirettamente, in particolare in riferimento a un identificatore quale un nome, un numero identificativo, dati relativi a luoghi, un identificativo telematico o a uno o più fattori specifici dell'identità fisica, fisiologica, genetica, mentale, economica, culturale o sociale di quella persona naturale.

Attenzione particolare deve essere dedicata ai dati definiti nel "EU general data protection regulation 2016/679 (GDPR)" come "Categorie Speciali di dati personali".

Categorie speciali di dati personali:
(...) Dati personali che rivelino origini razziali o etniche, opinion politiche, convinzioni religiose o filosofiche, appartenenza a sindacati, e (...) dati genetici, dati biometrici che abbiano il solo scopo di identificare una persona naturale, data riguardanti lo stato di salute o riguardanti la vita sessuale o l'orientamento sessuale di una persona naturale.

La struttura clinica deve assicurare che l'utilizzo del Prodotto è in linea con i requisiti definiti dalla legislatura applicabile sulla privacy e sulla protezione dei dati personali, in particolare rispetto alla gestione dell'informazione menzionata sopra.

Il Prodotto gestisce i seguenti dati personali:

- Nome e cognome
- Data di nascita
- Sesso
- Codice paziente
- Data di ammissione
- Data di dimissione
- Peso del paziente
- Altezza del paziente

Il Prodotto può essere configurato in modo da occultare questo tipo di informazioni su ogni schermata dell'applicativo.
Per fare ciò, sull'applicazione di configurazione del Prodotto (Digistat Configurator), si imposti la "System Option" denominata "Privacy Mode" a "true" (si veda il manuale di configurazione e installazione del prodotto) per la procedura dettagliata). Il valore impostato di default è "true".

Se l'opzione "Privacy Mode" è impostata su "true", sono possibili i seguenti casi:

- se non c'è un utente loggato, non è visualizzata alcuna informazione relativa al paziente.
- se c'è un utente loggato, e l'utente non ha un permesso specifico, non è visualizzata alcuna informazione relativa al paziente.
- se c'è un utente loggato, e l'utente ha il permesso specifico, sono visualizzate le informazioni relative al paziente.

L'opzione può essere applicata a una singola postazione di lavoro (cioè, diverse postazioni possono essere configurate in modo differente).

Leggere attentamente le precauzioni esposte nel presente paragrafo ed osservarle scrupolosamente.

- I PC in uso non devono rimanere incustoditi e accessibili durante le sessioni di lavoro con il Prodotto. Si raccomanda di eseguire il log out dal Prodotto quando ci si allontana dalla postazione di lavoro.

- I dati sensibili immessi nel Prodotto, quali password o dati personali degli utenti e dei pazienti devono essere protetti da qualsiasi tentativo di accesso non autorizzato attraverso software adeguati (antivirus e firewall). L'implementazione di tali software è di competenza della struttura ospedaliera. Tali software devono essere regolarmente aggiornati.

- L'utente è avvisato che l'uso frequente della funzione "blocca utente" è potenzialmente pericoloso. Il "Log out" automatico protegge il Prodotto dagli accessi non autorizzati.

Dati personali possono essere presenti in alcune delle stampe generate dal Prodotto. La struttura clinica deve gestire questi documenti in accordo alla legislatura corrente sulla privacy e sulla protezione dei dati personali.

Le postazioni di lavoro client (sia desktop sia mobili) non salvano su disco i dati-paziente. I dati del paziente sono salvati solo su database e il tipo di salvataggio su database dipende dalle scelte e dalle procedure adottate dalla struttura clinica che usa il Prodotto (esempi: macchine fisiche, SAN - Storage Area Network -, ambienti virtuali). I dati del paziente dovranno essere gestiti secondo le normative vigenti sulla privacy e sulla protezione dei dati personali.

I dati del paziente non sono salvati su file proprietari. I dati del paziente sono salvati solo su database.

In alcune circostanze dati personali sono trasmessi in formato non criptato e utilizzando una connessione non intrinsecamente sicura. Un esempio di questa situazione sono le comunicazioni HL7. È responsabilità dell'organizzazione responsabile prevedere, all'interno della rete ospedaliera, adeguati meccanismi di sicurezza in modo da assicurare la conformità con le leggi e i regolamenti concernenti la privacy.

Si suggerisce di configurare il server sul quale si trova il database in modo che esso sia criptato sul disco. Per abilitare questa opzione è necessario installare SQL Server Enterprise Edition e abilitare nel corso dell'installazione l'opzione TDE (Transparent Data Encryption).

La struttura ospedaliera deve provvedere ad un addestramento del personale riguardo alle nozioni fondamentali riguardanti la privacy: ad esempio i principi base, le regole da seguire, i regolamenti in vigore, le responsabilità e le sanzioni relativamente all'ambiente di lavoro specifico di ognuno.

Ascom UMS o il Distributore dovranno provvedere ad un addestramento dettagliato riguardo al miglior uso del Prodotto relativamente alla privacy (ad esempio: anonimizzazione dei database, modalità "private", permessi degli utenti etc.).

La struttura ospedaliera dovrà produrre e conservare la seguente documentazione:

1) la lista aggiornata degli amministratori di sistema e del personale addetto alla manutenzione del Prodotto;
2) i moduli di assegnazione dei ruoli firmati e le certificazioni di presenza ai corsi di addestramento;
3) un registro delle credenziali, dei permessi e delle prerogative degli utenti;
4) una lista aggiornata degli Utenti del prodotto.

La struttura ospedaliera dovrà implementare, verificare e certificare un meccanismo di disattivazione automatica degli utenti non più attivi per un determinato periodo di tempo.

La struttura ospedaliera dovrà codificare, implementare e documentare una procedura per la verifica periodica della corrispondenza al ruolo di amministratore di sistema e di tecnico addetto alla manutenzione del Prodotto.

La struttura ospedaliera dovrà eseguire verifiche formali e controlli sul corretto comportamento degli utenti del prodotto.

I database contenenti dati personali dei pazienti o informazioni sensibili non possono lasciare la struttura ospedaliera senza che siano stati prima offuscati o criptati

4.3.1 Caratteristiche e uso delle credenziali di accesso

Questo paragrafo fornisce indicazioni sulle caratteristiche che devono avere le credenziali di accesso al Prodotto (nome utente e password) e sulle loro modalità di utilizzo e mantenimento.

- Ogni utente deve prendere tutte le precauzioni possibili per mantenere segreti il proprio nome utente e la propria password.
- Nome utente e password sono private e personali. Non comunicare mai a nessuno il proprio nome utente e la propria password.
- Ogni incaricato può avere una o più credenziali per l'autentificazione (nome utente e password). Gli stessi nome utente e password non devono essere utilizzati da più incaricati.
- I profili di autorizzazione devono essere controllati e rinnovati almeno una volta all'anno.
- È possible raggruppare diversi profili di autorizzazione in base all'omogeneità dei compiti degli utenti.

- Ogni account utente deve essere collegato con una persona specifica. L'uso di utenti generici (come, ad esempio, "ADMIN" o "INFERMIERE") deve essere evitato. In altre parole, per ragioni di tracciabilità è necessario che ogni account sia utilizzato da un solo utente.

- Ogni utente è caratterizzato da un profilo che gli permette di utilizzare soltanto le funzionalità del Prodotto che sono pertinenti ai suoi compiti. L'amministratore di sistema deve assegnare il profilo adeguato contestualmente alla creazione dell'account utente. Tale profilo deve essere rivisto almeno una volta all'anno. Tale revisione può avvenire anche per classi di utenti. Le procedure relative alla definizione del profilo dell'utente sono descritte nel manuale di configurazione di Digistat.

- La password deve essere composta da almeno otto caratteri.

- La password non deve contenere riferimenti agevolmente riconducibili all'incaricato (ad esempio nome, cognome, data di nascita etc.).

- La password è assegnata dall'amministratore di sistema e deve essere modificata dall'utente al primo utilizzo del Prodotto, se ciò è espressamente stabilito da configurazione (si veda il paragrafo **Error! Reference source not found.** per la procedura di modifica della parola chiave).

- Successivamente, la password deve essere modificata almeno ogni tre mesi.

- Se le credenziali di accesso (nome utente e password) rimangono inutilizzate per più di sei mesi devono essere disattivate. Fanno eccezione credenziali specifiche da utilizzare per scopi di manutenzione tecnica. Si veda il manuale di configurazione di Digistat per la procedura di configurazione di questa caratteristica.

- Le credenziali di accesso sono disattivate anche in caso di perdita da parte dell'utente della qualifica corrispondente a tali credenziali (è il caso, ad esempio, in cui un utente si trasferisca ad un altra struttura). L'amministratore di sistema può abilitare/disabilitare manualmente un utente. La procedura è descritta nel manuale di configurazione di Digistat.

Le seguenti informazioni sono di pertinenza dei tecnici amministratori di sistema:

La parola chiave deve rispettare una regular expression definita nella configurazione di Digistat (Il default è ^.....* cioè 8 caratteri).
La password è assegnata dall'amministratore di sistema nel momento in cui è creato un nuovo account per un utente. L'amministratore può obbligare l'utente a modificare tale password e sostituirla con una personale la prima volta che accede al Prodotto. La password scade dopo un periodo di tempo configurabile, l'utente è tenuto a cambiare la password allo scadere di tale periodo. È possibile fare in modo che la password di un utente non scada.

Si veda il manuale di configurazione di Digistat per informazioni dettagliate sulla definizione degli account utente e sulla configurazione delle password.

4.3.2 Amministratori di sistema

Nello svolgere le normali attività di installazione, aggiornamento ed assistenza tecnica del Prodotto il personale Ascom UMS o dei Distributori autorizzati potrà aver accesso e trattare dati personali e sensibili memorizzati nel database e agire da Amministratori di Sistema per il Prodotto.
Ascom UMS adotta procedure ed istruzioni di lavoro che sono conformi alle prescrizioni della vigente normativa sulla privacy ("General Data Protection Regulation - EU 2016/679").

Si consiglia all'organizzazione ospedaliera di prendere in considerazione, fra le altre, le seguenti misure:

- definire gli accessi in modo nominativo;
- attivi il log degli accessi a livello di sistema operativo sia sul server che sui client;
- attivi il log degli accessi al database server Microsoft SQL Server (Audit Level);
- configuri e gestisca entrambi questi log in modo da mantenere traccia degli accessi per un periodo di almeno un anno.

4.3.3 Log di sistema

Il Prodotto registra i log di sistema sul database. Tali log sono mantenuti per un periodo di tempo che è configurabile. I log sono mantenuti per periodi di tempo differenti a seconda della loro natura. Di default le tempistiche sono le seguenti:

- i log informativi sono mantenuti per 10 giorni;
- i log corrispondenti a warning sono mantenuti per 20 giorni;
- i log corrispondenti a errori sono mantenuti per 30 giorni.

Queste tempistiche sono configurabili. Si veda il manuale di configurazione di Digistat per la procedura di definizione delle tempistiche di mantenimento dei log.

4.3.3.1 Log Forensi

Un sottoinsime dei suddetti log di sistema, definiti come "clinicamente rilevanti" o "clinicamente utili" in base alle politiche adottate da ogni specifica organizzazione ospedaliera che utilizzi il Prodotto, possono essere inviati a sistemi esterni (o SQL o Syslog) per essere qui immagazzinati in base ai regolamenti e alle necessità dell'organizzazione ospedaliera stessa.

4.4 Politica di Back up

Si raccomanda di eseguire regolarmente il back up del database del Prodotto.

L'organizzazione ospedaliera che utilizza il Prodotto deve identificare la politica di back up che meglio risponde alle sue esigenze dal punto di vista della sicurezza dei dati.
Ascom UMS o il Distributore autorizzato è disponibile a fornire il supporto necessario all'implementazione della politica identificata.

L'organizzazione ospedaliera responsabile deve assicurarsi che i file generati dal back up siano archiviati in modo da essere immediatamente disponibili in caso di necessità.

Se i dati vengono archiviati su supporti rimovibili, l'organizzazione ospedaliera deve custodire tali supporti in modo da evitare accessi non autorizzati. Quando tali supporti non sono più utilizzati devono essere distrutti o cancellati definitivamente.

4.5 Fuori uso di una postazione

Si raccomanda di eseguire il backup dell'immagine del disco rigido delle postazioni di lavoro, in modo che la sostituzione dell'hardware permetta di ripristinare velocemente l'ambiente di lavoro.

Gli interventi di manutenzione e le riparazioni devono essere eseguite in accordo alle procedure e line guida proprie di
UMS/Distributore, ed eseguite esclusivamente da personale tecnico specificamente formato ed autorizzato da Ascom UMS/Distributore.

Questo paragrafo descrive la politica suggerita da Ascom UMS in caso una postazione sia fuori uso. Lo scopo di questa procedura è quello di minimizzare i tempi di sostituzione della postazione fuori uso con una funzionante.
A tale scopo Ascom UMS consiglia di avere sempre a disposizione un PC aggiuntivo ("Muletto") su cui è pre-installato il Prodotto.
In caso di "fuori uso" di una postazione, il "muletto" può essere usato per sostituire velocemente la postazione fuori uso.

Si deve sempre ricordare che il Prodotto deve essere installato e configurato solo da personale addestrato ed autorizzato. Questo include il personale di Ascom UMS, dei Distrubutori autorizzati e ogni altra persona specificamente addestrata e autorizzatra

da Ascom UMS o dal Distributore. Pertanto, in assenza di una diretta autorizzazione da parte di Ascom UMS/Distributore, il personale ospedaliero non è autorizzato ad effettuare installazione e/o modificare la configurazione del Prodotto.
Il rischio associato alla procedura di disattivazione e/o sostituzione di una workstation è la possibilità di sbagliare nel correlare la workstation con il posto letto/sala. Ciò potrebbe portare a uno scambio di pazienti. Il rischio associato alla procedura di riconfigurazione o sostituzione di un apparato di rete coinvolto nell'acquisizione dati (port server, docking station, ...) è la possibilità di assegnare i dati acquisiti ad un paziente errato. L'associazione tra dati acquisiti e paziente si basa sull'indirizzo IP del dispositivo e una sua alterazione può portare all'interruzione dell'acquisizione e, nei casi più gravi, all'attribuzione dei dati al paziente sbagliato.

La procedura di fuori uso e sostituzione di una workstation è potenzialmente rischiosa, questo è il motivo per cui, tassativamente, deve essere effettuata solo da personale espressamente addestrato e autorizzato. Il rischio associato alla disattivazione e/o sostituzione di workstation è la possibilità di una erronea associazione al posto letto/ sala con conseguente potenziale scambio di pazienti.

Nel caso si voglia disattivare o sostituire una workstation il personale ospedaliero deve prontamente avvertire Ascom UMS o il Distributore di riferimento e richiedere l'esecuzione di tale operazione. A tal fine Ascom UMS consiglia all'organizzazione responsabile di definire una chiara procedura operativa e di condividere tale procedura con tutto il personale coinvolto.

Al fine di accelerare i tempi di sostituzione nel caso di guasto di una workstation Ascom UMS suggerisce di avere a disposizione uno o più "muletti" con tutte le applicazioni necessarie pre-installate (OS, firewall, antivirus, RDP, ...) e con il Prodotto pre-installato ma disabilitato (cioè non eseguibile da utente senza intervento di tecnico Ascom UMS/Distributore).
In caso di guasto di una workstation la disponibilità del muletto garantisce la minimizzazione dei tempi di ripristino (sostituzione hardware) limitando, al contempo, il rischio di associazione dei dati al paziente errato.

In caso di guasto di un PC su cui è eseguito il Prodotto la procedura consigliata in presenza di "muletti" è la seguente:

1) Il personale ospedaliero autorizzato sostituisce il PC guasto con un "muletto"
2) Il personale ospedaliero contatta Ascom UMS/Distributore richiedendo l'attivazione del "muletto"
3) Il personale Ascom UMS/Distributore disattiva la workstation guasta e configura opportunamente il muletto
4) Il computer guasto viene riparato e preparato come "muletto"

Le istruzioni per la messa fuori servizio e la sostituzione di una workstation, riservate agli amministratori di sistema, si trovano sul manuale di configurazione del Prodotto.

4.5.1 Riconfigurazione o sostituzione di apparato di rete

Nel caso si voglia riconfigurare o sostituire un apparato di rete coinvolto nella acquisizione dati il personale ospedaliero deve prontamente avvertire Ascom UMS o il Distributore autorizzato e concordare l'esecuzione di tale operazione in modo che il personale di Ascom UMS o del Distributore possa contestualmente riconfigurare il Prodotto o fornire le informazioni necessarie per effettuare l'operazione. A tal fine si consiglia all'organizzazione responsabile di definire una chiara procedura operativa e di condividere tale procedura con tutto il personale coinvolto. Sul manuale di configurazione del Prodotto si trovano le indicazioni per tale operazione.

4.6 Manutenzione preventiva

Le procedure di manutenzione e gli interventi tecnici devono essere effettuati in accordo alle procedure e alle linee guida di Ascom UMS/Distributore ed essere effettuate solamente da tecnici di Ascom UMS/Distributore o da personale specificamente formato ed esplicitamente autorizzato da Ascom UMS/Distributore.

Si consiglia di effettuare la manutenzione del Prodotto come minimo una volta l'anno. Si valuti comunque che la periodicità della manutenzione deve essere funzione della complessità del sistema. In caso di elevata complessità si consiglia di effettuare la manutenzione più di frequente, fino a due volte l'anno.

Si veda il manuale di configurazione del Prodotto per la check list contenente l'elenco dei controlli da effettuare nel corso della manutenzione:

4.7 Dispositivi compatibili

Contattare Ascom UMS o il Distributore di riferimento per la lista dei driver disponibili.

Digistat non è stato progettato per verificare il corretto funzionamento dei dispositivi, ma per acquisire e catalogare dati clinici.

La disconnessione di un dispositivo durante il suo funzionamento causa l'interruzione dell'acquisizione dei dati da parte di Digistat. I dati del dispositivo che sono persi nel periodo di disconnessione non sono recuperati da Digistat dopo che il dispositivo è di nuovo connesso.

Non disabilitare mai i sistemi di allarme sui dispositivi medici al di fuori dei casi indicati dalla documentazione fornita dal produttore del dispositivo stesso e dalle procedure in uso nella struttura clinica.

La correttezza dei parametri mostrati da Digistat deve essere sempre verificata sul dispositivo che li ha generati.

Mai disabilitare l'audio delle postazioni sulle quali è installato Digistat.

Per ragioni che non sono sotto il controllo del software (come, ad esempio, il modo in cui gli effettivi dispositivi fisici sono installati o cablati) potrebbero esserci dei ritardi fra il momento in cui l'allarme è generato e il momento in cui è visualizzato.

Se il driver generico Alaris® è in uso, dopo aver scollegato una pompa di infusione, è necessario attendere almeno dieci secondi prima di collegarne un'altra.

L'aggiornamento dei dati visualizzati sullo schermo dovuto alla connessione di un nuovo dispositivo, a spegnimento, a disconnessione e modifica di stato, dipende dal tempo necessario al dispositivo stesso per comunicare le modifiche. Questa arco temporale dipende da vari fattori, fra i quali il tipo di dispositivo e il tipo di connessione. Per alcuni dispositivi esistono condizioni nelle quali il ritardo nella comunicazione delle modifiche può essere significativo. Non è possibile indicare i ritardi per tutti i dispositivi possibili perché tali ritardi variano a seconda delle configurazioni e delle condizioni operative.

I drivers usati per leggere i dati dai dispositivi medici collegati hanno un ciclo di lettura inferiore ai tre secondi (cioè: tutti i dati dai dispositivi sono letti ogni tre secondi al massimo). Esistono dispositivi che comunicano informazioni meno di frequente (ad esempio ad intervalli di 5-10 secondi). Si faccia riferimento alla documentazione specifica del driver per dettagli riguardo al ciclo di lettura.

	In un ambiente di test installato e configurato come indicato nel manuale di installazione e configurazione di Digistat, appena un driver riconosce un allarme, è necessario un secondo al massimo per trasferirlo a Digistat.

	In caso di black-out elettrico, sono necessari alcuni minuti perché il Prodotto sia di nuovo del tutto operativo e perché generi notifiche di allarme (di solito questo tempo è inferiore a tre minuti, ma dipende dalla configurazione dei dispositivi in uso).

4.8 Indisponibilità del Prodotto

Se durante la fase di avvio si riscontrano problemi di connessione col server il Prodotto avvisa tramite una apposita schermata.

Il problema di connessione può risolversi da solo entro breve tempo. Se ciò non avviene è necessario contattare l'assistenza tecnica. Si veda il paragrafo 9 per l'elenco di contatti Ascom UMS.

Esistono casi estremi, rari ma possibili, nei quali sia fisicamente impossibile usare il Prodotto.

L'organizzazione ospedaliera che usa il Prodotto è tenuta a definire una procedura di emergenza da attuare in tali casi. Ciò al fine di

1) Permettere ai reparti di continuare a svolgere le proprie attività
2) Ripristinare al più presto la disponibilità del Prodotto.

L'organizzazione ospedaliera che usa il Prodotto è tenuta a definire una procedura di emergenza da attuare in caso di indisponibilità del Prodotto.

Ascom UMS o il Distributore di riferimento sono disponibili per fornire pieno supporto nella definizione di tale procedura. Si veda il paragrafo 5 per l'elenco dei contatti.

5. Contatti del fabbricante

Si faccia riferimento, per qualsiasi comunicazione, al distributore che ha installato il Prodotto. Qui di seguito sono riportati i contatti del fabbricante.

Ascom UMS srl unipersonale

Via Amilcare Ponchielli 29, 50018, Scandicci (FI), Italia

Tel. (+39) 055 0512161

Fax (+39) 055 8290392

Assistenza tecnica

support.it@ascom.com
800999715 (toll free, Italy only)

Informazioni commerciali

it.sales@ascom.com

Informazioni generali

it.info@ascom.com

6. Rischi residui

Un processo di gestione dei rischi è stato implementato nel ciclo di vita di Digistat, così come prescritto dalle norme tecniche di rifermento. Per ogni rischio sono state individuate e implementate tutte le opportune misure di controllo che permettono di ridurre ogni rischio residuo a livello minimo che risulta accettabile considerando i vantaggi forniti dal prodotto. Anche il rischio residuo totale risulta accettabile se confrontato con i medesimi vantaggi.

I rischi sotto elencati sono stati affrontati e ridotti a livelli minimi. Tuttavia, per la natura stessa del concetto di rischio, non è possibile ridurli a zero ed è quindi necessario, secondo la normativa, portarne a gli utenti conoscenza.

- Impossibilità di utilizzare il Prodotto o alcune sue funzionalità come atteso, che può portare a ritardo o errore nelle azioni terapeutico/diagnostiche.
- Azioni non autorizzate operate dagli utenti, che possono portare ad errori nelle azioni terapeutico/diagnostiche.
- Attribuzione dell'informazione ad un paziente sbagliato (scambio di pazienti), che può portare ad errori nelle azioni terapeutico/diagnostiche.
- Errata gestione dei dati del paziente, incluso errori di visualizzazione, aggiunta, modifica e cancellazione dei dati che possono causare ritardi e/o errori nelle azioni terapeutiche/diagnostiche.
- Uso off label di DIGISTAT® (ad esempio utilizzo del Prodotto come sistema primario di notifica di allarme, decisioni terapeutiche o diagnostiche e interventi basati esclusivamente sulle informazioni fornite dal Prodotto).
- Divulgazione non autorizzata di dati personali degli utenti e/o del paziente.

RISCHI RELATIVI ALLA PIATTAFORMA HARDWARE UTILIZZATA PER IL DISPOSITIVO MEDICO

- Shock elettrico per paziente e/o operatore, che può portare a lesioni o morte del paziente e/o dell'operatore.
- Surriscaldamento di componenti hardware, che possono portare a lesioni non gravi per il paziente e/o l'operatore.
- Contrazione di infezioni per paziente e/o operatore.