Digistat® Product User Manual

Revision 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 is manufactured by Ascom UMS (http://www.ascom.com).
The Product is CE marked according to 93/42/EEC ("Medical Device Directive") amended by the 2007/47/EC.
Ascom UMS is certified according to EN ISO 13485:2016 with the following scope: "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".

Software License
The Product must be used only after obtaining a valid license from Ascom UMS or the Distributor

Trademarks and copyright

Contents

1. Using the manual

ℹ This User Manual shall be used in combination with module-specific manuals, listed below. Refer to the applicable manuals, according to the Digistat modules in use in the Healthcare Organization.

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

1.1 Aims

The effort which has gone into creating this manual aims to offer all the necessary information to guarantee a safe and correct use of the Digistat software and to allow the manufacturer identification. Furthermore, this document aims to describe every part of the software, it also intends to offer a reference guide to the user who wants to know how to perform a specific operation and a guide for the correct use of the software so that improper and potentially hazardous uses can be avoided.

1.2 Characters used and terminology

The use of Digistat requires a basic knowledge of the most common IT terms and concepts. In the same way, understanding of this manual is subject to such knowledge.

Remember that the use of Digistat must only be granted to professionally qualified and properly trained personnel.

When consulting the online version as opposed to the paper version, cross-references in the document work like hypertext links. This means that every time you come across the reference to a picture (e.g. “Fig 2”) or to a paragraph / section (e.g. “Paragraph 2.2.1”), you can click the reference to directly go to that particular figure or that particular paragraph / section.

1.2.1 Conventions

The following conventions are used in this document:

- Names of buttons, menu commands, options, icons, fields and anything on the user interface that the user can interact with (either touch or click or select) are formatted in **bold**.
- Names/headings of screens, windows and tabs are quoted with “Double quotation marks”.
- Programming code is formatted in Courier.
- The ➢ bullet indicates an action the user must perform to carry out a specific operation.
- References to external documents are formatted in *italic*.

1.3 Symbols

The following symbols are used in this manual.

Useful information

This symbol appears alongside additional information concerning the characteristics and use of Digistat. This may be explanatory examples, alternative procedures or any “extra” information considered useful to a better understanding of the product.

Caution!

The symbol is used to highlight information aimed at preventing improper use of the software or to draw attention to critical procedures which might cause risks. Consequently, it is necessary to pay extreme attention every time the symbol appears.

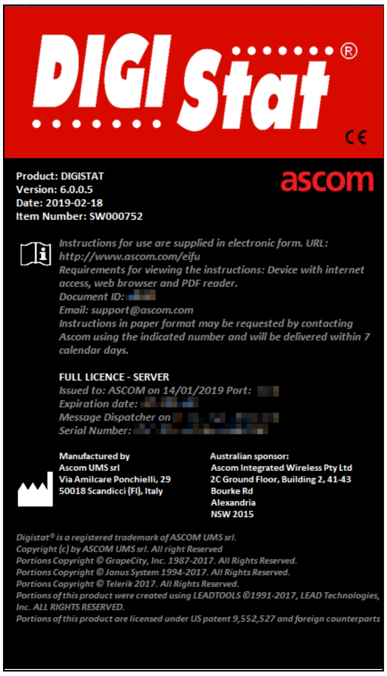
The following symbols are used in the about box (Fig 1):

Indicates the manufacturer’s name and address

Attention, consult accompanying documents

1.3.1 The Digistat About Box

The **About** button on the Digistat main menu displays a window containing information on the Digistat version installed and the related licenses (Fig 1). See Digistat Control Bar user manual for more information (*USR ENG Control Bar*).



Product: DIGISTAT
Version: 6.0.0.5
Date: 2019-02-18
Item Number: SW000752

Instructions for use are supplied in electronic form. URL: http://www.ascom.com/eifu
Requirements for viewing the instructions: Device with internet access, web browser and PDF reader.
Document ID: [redacted]
Email: support@ascom.com
Instructions in paper format may be requested by contacting Ascom using the indicated number and will be delivered within 7 calendar days.

FULL LICENCE - SERVER
Issued to: ASCOM on 14/01/2019 Port: [redacted]
Expiration date: [redacted]
Message Dispatcher on [redacted]
Serial Number: [redacted]

Manufactured by
Ascom UMS srl
Via Amilcare Ponchielli, 29
50018 Scandicci (FI), Italy

Australian sponsor:
Ascom Integrated Wireless Pty Ltd
2C Ground Floor, Building 2, 41-43
Bourke Rd
Alexandria
NSW 2015

Digistat® is a registered trademark of ASCOM UMS srl.
Copyright (c) by ASCOM UMS srl. All right Reserved
Portions Copyright © GrapeCity, Inc. 1987-2017. All Rights Reserved.
Portions Copyright © Janus System 1994-2017. All Rights Reserved.
Portions Copyright © Telerik 2017. All Rights Reserved.
Portions of this product were created using LEADTOOLS ©1991-2017, LEAD Technologies, Inc. ALL RIGHTS RESERVED.
Portions of this product are licensed under US patent 9,552,527 and foreign counterparts

Fig 1

2. Introduction to Digistat

The Digistat clinical modules suite is an advanced patient data management software system that is designed specifically for use by clinicians, nurses and administrators.

The software package consist of a set of modules that can either work alone or be fully integrated to provide a complete patient data management solution.

From the Intensive Care Unit to the Ward, from the Operating Room to the Administrative Department, Digistat can be used in a wide range of environments.

Digistat modular architecture and extensive configuration capabilities allows the patient data management system to be tailored to organizational needs and adaptable to meet new demands when required.

Digistat can only be accessed by entering username and password. Every user is defined by a detailed profile and can access only the allowed areas. An audit trail of every login performed is automatically generated by the system.

2.1 Modular Architecture

“Modular Architecture” means that different applications (or modules) can be implemented within the same software environment (Digistat in the present case) that is characterized by a consistent user interface, same overall goals and terms of use.

Modules can be added at different times, and in a way that is agreed with the healthcare organization. The resultant software suite fits the specific organization needs and can change in time, according to the possible changes in the organization needs.

2.2 Intended use

The Digistat® Software (hereafter “Product”) acquires records, organizes, transmits and displays patient information and patient related data, including data and events from connected clinical devices and systems as well as information entered manually, in order to support caregivers in diagnosis and treatment of patients as well as to establish electronic patient records.

- The Product produces configurable electronic patient records based on acquired data and information, as well as on manual and automated documentation of the clinical unit’s activity.
- The Product provides automated, secondary visual and audible announcing and displaying of acquired data, events, current status and operating conditions of connected clinical devices and systems on designated display device(s). The Product can also be configured to forward data and information about events, statuses and operating conditions to the ASCOM messaging system.

- The Product supports the improvement of nursing workflows related to the management of alarms from the connected clinical devices and systems.
- The Product supports the documentation of the prescribed therapy, its preparation and its delivery.
- The Product supports the recording, validation and display of vital signs charting based on the acquired data and information.
- The Product provides configurable reports, charts and statistics based on recorded data for use by healthcare professionals to analyze the unit’s efficiency, productivity, capacity and resource utilization, and the quality of care.

The Product **does not** replace or replicate the original display of data and alarms of the connected devices and systems and **does not** control, monitor or alter the behavior of these connected devices and systems, or their associated alarms.

The Product **is not** intended to be used for direct diagnosis or monitoring of vital physiological parameters.

The Product is intended for use by trained healthcare professionals within a hospital/clinical environment and relies on proper use and operation of the IT and communication infrastructure in place at the healthcare facility, the display devices used and the connected clinical devices and systems.

Additionally, the Product provides specific functions and interfaces intended to be used by non-professional users in remote locations for non-clinical purposes for display of information, reports, charts and statistics, without the ability to add, change or delete any information or data.

The Product is a stand-alone software that is installed on servers and computers, which must comply with the technical hardware and software specifications provided with the Product.

2.2.1 Safety Advisories

The User shall base therapeutic or diagnostic decisions and interventions solely on the direct examination of the original source of information. The user has sole responsibility to check that the information displayed by the Product is correct and to make appropriate use of it**.**

Only printouts that are signed with digital or ink signature by authorized medical professionals shall be considered valid clinical records. In signing the aforementioned printouts, the User certifies they have checked the correctness and completeness of the data present in the document.

When entering patient related data the User have responsibility to verify that the patient identity, Healthcare Organization department/care unit and bed information displayed in the Product are correct. This verification is of utmost importance in cases of critical interventions, for instance, drug administration.

The Healthcare Organization is responsible to identify and implement appropriate procedures to ensure that potential errors occurring in the Product and/or in the use of the Product are promptly detected and corrected and do not constitute a risk to the patient and the User. These procedures depend on the configuration of the Product and the method of use preferred by the Healthcare Organization.

The Product may provide, depending on the configuration, access to information on drugs. The Healthcare Organization is responsible to verify, initially and periodically, that this information is current and updated.

The Product does not provide ~~a~~ primary notification of alarms; it is not intended to be used in place of the direct monitoring of the alarms generated by the medical devices. This limitation is due, among the other reasons, to the specifications and limitations of the communication protocols of the medical devices.

In case some devices used with the Product are located in the patient area or are connected to equipment present in the patient area then the Healthcare Organization have responsibility to ensure that the whole combination complies with the international standard IEC 60601-1 and any additional requirement(s) established by the local regulations.

Use of the Product must be granted, by means of specific configuration of user accounts and active surveillance, only to User who are:

- trained according to Product indications by personnel authorized by the manufacturer or distributors and
- in possession of the professional qualifications to correctly interpret the information supplied and to implement the appropriate safety procedures.

The Product is a stand-alone software that runs on standard computers and/or standard mobile devices connected to the Healthcare Organization local network. The

Healthcare Organization is responsible to adequately protect computers, devices and local network against cyber-attacks.

The Product shall be installed only on computers and devices fulfilling the minimum hardware requirements and on supported operating systems.

2.3 “Off-label” use of the Product

Every use of the Product outside what explicitly stated in the “Intended use” (usually referred to as “off-label” use) is under the full discretion and responsibility of the user and of the Healthcare organization.

The manufacturer does not guarantee in any form the Product safety and suitability for any purpose where the Product is used outside the stated “Intended use”.

⚠ The Product **is not** a primary distributed alarm system.

2.4 Patient Population

The product is a software application and is not in contact with the patient.
The patient population and patient conditions are established by the medical devices and systems with which the product is connected.
In addition the following limitations apply:

- Patient weight between 0.1kg and 250kg
- Patient height between 15cm and 250cm

2.5 Healthcare organization responsibilities

Ascom UMS declines all responsibility for the consequences on the safety and efficiency of the product determined by technical repairs or maintenance not performed by its own Technical Service personnel or by Ascom UMS-authorized technicians.

The attention of the user and the legal representative of the Healthcare Organization where the device is used is drawn to their responsibilities, in view of the local legislation in force on the matter of occupational safety and health (e.g. in Italy Dlgs. no. 81/2008) and any additional local site safety.

The Ascom UMS Service is able to offer customers the support needed to maintain the long-term safety and efficiency of the devices supplied, guaranteeing the skill, instrumental equipment and spare parts required to guarantee full compliance of the devices with the original construction specifications over time.

⚠ The product is designed taking into account the requirements and best practices present in the IEC 80001 standard and its collateral technical reports. In particular the IEC/TR 80001-2-5:2014 has great relevance for the product. As clarified in the IEC 80001 series part of the necessary activities and risk control measures are under the control and responsibility of the healthcare organization. Please refer to the standard and its collaterals to identify the necessary activities and risk control measures; in particular refer to the following documents:

- 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 Manufacturer’s responsibility

Ascom UMS is responsible for the product’s safety, reliability and performance only if:

- Installation and configuration were performed by personnel trained and authorized by Ascom UMS;
- Use and maintenance comply with the instructions provided in the Product documentation (including this User Manual);
- Configurations, changes and maintenance are only performed by personnel formed and authorized by Ascom UMS ;
- The Product’s usage environment complies with applicable safety instructions and applicable regulations;
- The environment in which the Product is used (including computers, equipment, electrical connections, etc.) complies with applicable local regulations.

⚠ Should the Product be part of a “medical electrical system” through electrical and functional connection with medical devices, the healthcare organization is in charge of the required electrical safety verification and acceptance tests, even where Ascom UMS performed in whole or in part the necessary connections.

2.7 Product traceability

In order to ensure device traceability and on site corrective actions, in compliance EN 13485 and MDD 93/42/EEC, the owner is requested to inform ASCOM UMS/Distributor about any ownership transfer by giving written notice stating the Product, former owner and new owner identification data.
Device data can be found in the Product label ("About box" displayed within the Product – see page **Error! Bookmark not defined.**).
In case of doubts/questions about Product identification please contact ASCOM UMS/Distributor technical assistance (for contacts see page **Error! Bookmark not defined.**).

2.8 Post-market surveillance

The CE marked device is subject to a post-market surveillance - which ASCOM UMS and Distributor provide for each marketed copy - concerning actual and potential risks, either for the patient or for the User, during the Product's life cycle.
In case of deterioration of the device characteristics, poor performance or inadequate user instructions that have been or could be a hazard to either the patient or User' health or to environmental safety, the User must immediately give notice to either ASCOM UMS or Distributor.
On reception of a user feedback ASCOM UMS/Distributor will immediately start the review and verification process and perform the necessary corrective actions.

2.9 Product life

The life time of the Product does not depend on wearing or other factors that could compromise safety. It is influenced by the obsolescence of the software environment (e.g. OS, .NET Framework) and is therefore set to 5 years from the release date of the Product version (available in the About box).

3. Software/Hardware specifications

⚠ The Product must only be installed by trained authorized personnel. This includes Ascom UMS/Distributors staff and any other person specifically trained and explicitly authorized by Ascom UMS/Distributor. Without an explicit, direct authorization from Ascom UMS/Distributor, the healthcare organization staff are not authorized to perform installation procedures and/or to modify the Product configuration.

⚠ The Product must only be used by trained personnel. The Product cannot be used without having a proper training, performed by Ascom UMS/Distributors staff.

The information provided in this chapter covers the manufacturer's obligations identified by the IEC 80001-1:2010 standard (Application of risk management for IT-networks incorporating medical devices).

According to the IEC 60601-1 standard, in case where an electrical equipment is positioned close to the bed, the use of "Medical grade" devices is required. In these situations medical grade PANEL PCs are usually used. If explicitly requested, Ascom UMS is able to provide information on appropriate devices.

⚠ A supported PDF reader must be installed on the workstation in order to show the online help. See 3.1.3 for the Software Requirements of Central & Bedside workstations.

3.1 Central & Bedside

3.1.1 Hardware

Minimum hardware requirements:

- Intel® I3 processor (or faster)
- Memory: 4 GB RAM
- Hard Disk: at least 60 GB of available space
- Monitor: 1024 x 768 or higher (1920 x 1080 suggested)
- Mouse or other compatible device. Touch screen recommended.
- Ethernet interface 100 Mb/s (or higher)
- CD/DVD Drive or possibility to copy the installation files

In case a Central/Bedside workstation is configured to display video streams (feature supported only in Smart Central or OranJ with camera integration enabled) the minimum requirements are the following:

- Intel® I3 processor (or faster)
- Memory: 4 GB RAM + 50MB every camera stream displayed concurrently (ex. with 20 cameras displayed 4 GB + 1 GB)
- Hard Disk: at least 60 GB of available space
- Monitor: 1024 x 768 or higher (1920 x 1080 suggested)
- Mouse or other compatible device
- Ethernet interface 100 Mb/s (or higher)
- CD/DVD Drive or possibility to copy the installation files

Some examples: with Intel i7 6600 2.60 Ghz, with a streaming of 10 cameras with a bitrate of 3138 kbps, the cpu utilization is about 45%. With I3 7100t 3.4 Ghz, with a streaming of 16 cameras with a bitrate of 958 kbps, the cpu utilization is about 30%.

3.1.2 Operating System

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

3.1.3 System Software

- Microsoft Framework .NET 4.5
- Adobe Acrobat Reader version 10

NOTE: the User Manual is a PDF file, version 1.5, compatible with Acrobat 6.x or higher. Digistat was tested with Adobe Acrobat Reader 10.
The hospital organization may use a different version of Acrobat Reader, it is part of the Verification of the installed product to assure that the help system is working correctly.

3.2 Server

3.2.1 Hardware

Minimum hardware requirements (small installation, 20 beds, 4 devices each):

- Intel® I5 processor with 4 cores.
- Memory: 8 GB RAM.
- Hard Disk: 120 GB of available space.
- Ethernet interface 100 Mb/s.
- CD/DVD Drive or possibility to copy the installation files

Recommended hardware requirements (medium size installation, 100 beds, 4 devices each, Connect and Mobile):

- Intel® I7 processor with 8 cores.
- Memory: 32 GB RAM.
- Hard Disk: 120 GB of available space.
- Ethernet interface: 1 Gb/s.
- CD/DVD Drive or possibility to copy the installation files

3.2.2 Operating System

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

3.2.3 System Software

- 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 has been verified on the Ascom Myco SH1 and SH2 Wi-Fi and Cellular Smartphone devices, with Android version 4.4.2 (Myco1) or 5.1 (Myco1/Myco2) or 8.0 (Myco3). It is therefore compatible with Myco1, Myco2 and Myco3 mobile devices.

The application is designed to be compatible with other Android devices with a minimum screen size of 3.5'', and compatibility with a specific device must be verified before clinical use.

Please contact Ascom UMS/Distributor for the full list of devices that support Digistat Mobile.

3.4 Digistat Web

The following browsers are supported for use with DIGISTAT® Web (hereafter Digistat Web) applications:

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

⚠ Only supported Web Browsers shall be used for Digistat Web.

⚠ A Digistat Web workstation shall always have the Web Browser in foreground. Besides, the Web Browser shall never be used for anything else but Digistat Web (which also implies that the Digistat Web homepage shall be the default homepage of the Web Browser).

⚠ The Browser's Display Scaling shall always be set to 100%.

⚠ When the local network is at least partially based on WiFi connections, given the intermittent nature of WiFi connections, disconnects could occur which activate the Disconnected Mode (grey carpet covering Digistat Web) and thus the system may not be available. The healthcare organization must work to ensure optimal WiFi coverage and instruct the staff on how to handle these temporary system outages

---

3.5 General Warnings

⚠ ***IMPORTANT!***

The “MDI Web” application presented in this User Manual can only be used for demo purposes. It cannot be used in a production environment

⚠ To correctly use the Product, the Microsoft Windows Display Scaling must be set to 100%. Different settings may prevent the product from starting or cause malfunctions in the way the Product is visually displayed. Please refer to the Microsoft Windows documentation for instructions on the Display Scaling settings.

⚠ The minimum vertical resolution of 768 is supported only if the Product is configured to run in full-screen mode or if the Windows tray bar is in Auto-hide mode.

⚠ The computers and the other connected devices must be suitable for the environment in which they are used and must, therefore, comply with the relevant regulations.

⚠ It is mandatory to follow the manufacturer instructions for storage, transport, installation, maintenance and waste of third parties hardware. These procedures must be performed only by qualified and authorized personnel.

⚠ The use the Product together with any software other than those specified in this document may compromise the safety, effectiveness and design controls of the Product. Such use may result in an increased risk to users and patients. It is mandatory to consult an authorized Ascom UMS or Distributor technician before using together with the Product any software other than those specified in this document.

If the hardware on which the Product runs is a stand-alone computer, the user shall not install any other software (utilities or applications programs) on the computer. It is suggested to apply a permission policy that prevents users from performing procedures such as the installation of new software.

⚠ The Healthcare Organization shall implement for the workstations on which the Product runs a date/time synchronization mechanism to a reference source.

⚠

It is recommended to disable the access to Internet on the client workstations and the handheld devices on which the Product is used.
Alternatively the healthcare organization shall implement the necessary security measures in order to guarantee adequate protection from cyber-attacks and installation of unauthorized applications.

⚠

Parts of the Product act as viewer of video streams; the Product is not the source of the video stream and it does not record this information in any way. It is responsibility of the healthcare organization to manage the system from a data protection perspective including the installation and configuration of source cameras.

⚠

Parts of the Product handle audio and images related to the users and/or patients including acquisition, elaboration and recording. It is responsibility of the healthcare organization to implement the necessary procedures to comply with the local data protection regulation. Including but not limited to definition of boundaries of usage and training of users.

⚠

The video streaming functionality on desktop workstations has been tested with H264 and H265 video codecs.
Any other video codec natively present or installed by third party applications (e.g. VLC Media Player) has to be tested before use.

⚠

Beware: each video source supports a maximum number of simultaneously connected clients. It is responsibility of the healthcare organization to determine this maximum number and to inform the users.

⚠

The video streaming functionality on mobile devices only supports RTSP video streams with the following authentication types:

- No authentication;
- Basic authentication;
- Digest authentication.

⚠

The video streaming functionality on mobile devices only supports H263, H264 and H265 video codecs.

3.6 Firewall and Antivirus

To protect the the Product from possible cyber-attacks, it is necessary that:

- the Windows© Firewall is active both on the client PCs and the server;
- antivirus/antimalware software is installed and regularly updated both on the client PCs and the server.

The Healthcare Organization shall ensure that these two protections are activated. Ascom UMS tested the Product with F-SECURE Antivirus but, considering the strategies and policies already existing in the healthcare organization, the actual choice of the antivirus is left to the Healthcare Organization. Ascom UMS cannot ensure that the Product is compatible with any antivirus or antivirus configuration.

⚠ Some incompatibilities have been reported between parts of the Product and Kaspersky antivirus. The solution to these incompatibilities required the definition of specific rules in the antivirus itself.

⚠ It is suggested to only keep open the TCP and UDP ports actually needed. These may change according to the system configuration. Please refer to the Ascom UMS technical assistance for more information.

3.6.1 Further recommended precautions for cyber-protection

In order to further protect the Product from possible cyber-attacks, it is highly recommended to:

- plan and implement the “Hardening” of the IT infrastructure including the IT platform that represent the runtime environment for the Product,
- implement an Intrusion Detection and Prevention System (IDPS),
- perform a Penetration Test and, if any weakness is detected, perform all the required actions to mitigate the risk of cyber-intrusion,
- dismiss the devices when they are no longer updatable,
- plan and perform a periodic verification of the integrity of files and configurations,
- Implement a DMZ (demilitarized zone) solution for web servers that need to be exposed on the internet.

3.7 Local network features

This section lists the features of the local network on which the Product is installed in order to guarantee the Product's full functionality.

- The Product uses a TCP/IP traffic protocol.
- The LAN must not be congested and/or full loaded.
- The Product requires at least a 100 Megabit LAN available to the client workstation. 1 Gigabit Ethernet backbone~~s~~ would be worthwhile.
- There must not be filters in the TCP/IP traffic between workstations, server and secondary devices.
- If the devices (server, workstations and secondary devices) are connected to different subnets there must be routing in these subnets.
- It is recommended to adopt redundancy strategies to ensure network service availability in case of malfunction.
- It is recommended to schedule, together with Ascom/Distributors, the maintenance calendar in order to let Ascom or the authorized Distributor efficiently support the healthcare organization in managing the possible disservices caused by maintenance activities.

⚠ If the network does not match the requested features, the Product performance gradually deteriorates until timeout errors occur. The system may finally switch to "Recovery" mode.

⚠ In case a WiFi network is in use, given the possible intermittency of the WiFi connection, network disconnections are possible, that cause the activation of the "Recovery Mode" and the consequent system unavailability. The Healthcare Organisation shall ensure an optimal network coverage and stability, and train the personnel in the management of these temporary disconnections.

⚠ In order to encrypt the data transmitted over wireless networks it is recommended to adopt the highest security protocol available; in any case no less than WPA2.

3.7.1 Impact of the Product on the healthcare organization network

The Product impacts the local network of the healthcare organization. This section provides information on the traffic generated by the Product on the network in order to make it possible for the structure to evaluate and analyze the risks related to the introduction of the Product.
The bandwidth used by the Product depends on many different factors. The most important are:

- Number of workstations,
- Number of workstations configured as central stations,
- Number and type of devices dedicated to data acquisition
- Interfaces with external systems,
- Product configuration and mode of use.

The Product bandwidth occupation depends mainly on data acquisition from medical devices. In a configuration with acquisition on 100 beds where every bed collects data from 1 ventilator, 1 patient monitor and 3 infusion pumps, and with 10 workstations covering 10 beds each, the following bandwidth occupation values can be indicatively predicted:

Average: 0.8 – 6 Mbit/s
Pitch: 5 – 25 Mbit/s

In case of configurations with no acquisition from medical devices, bandwidth occupation values are lower than those specified above.

4. Before starting

4.1 Installation and maintenance warnings

The following warnings provide important information on the correct installation and maintenance procedures of the Product. They must be strictly respected.

⚠ Installation, maintenance and repairs shall be performed in compliance with Ascom UMS procedures and guidelines only by Ascom UMS/Distributor technicians or personnel trained and authorized by Ascom UMS/Distributor.

⚠ It is recommended for the healthcare organization using the Product to stipulate a maintenance contract with Ascom UMS or an authorized Distributor. Part of the maintenance shall include the upgrade to the latest version available of the Product.

The Product must be installed and configured by specifically trained and authorized personnel. This includes Ascom UMS (or authorized Distributor) staff and any other person specifically trained and authorized by Ascom UMS/Distributor. Similarly, maintenance interventions and repairs on the Product must be performed according to Ascom UMS guidelines only by Ascom UMS/Distributor personnel or another person specifically trained and authorized by Ascom UMS/Distributor.

⚠ The Product must be installed and configured by specifically trained and authorized personnel. This includes Ascom UMS (or authorized Distributor) staff and any other person specifically trained and authorized by Ascom UMS/Distributor.

- Use third party devices recommended by Ascom UMS/Distributors.
- Only trained and authorized people can install third party devices.
- Incorrect installation of the third party devices can create a risk of injury to the patient and/or operators.
- Meticulously observe the manufacturer’s instructions for the installation of third party hardware.
- Make provision for regular maintenance of the system according to the instructions present in this manual and those provided with the third party devices.

- The healthcare organization is responsible to select equipment that are suitable for the environment in which they are installed and used. The healthcare organization among the other should consider electrical safety, EMC emissions, radio signal interferences, disinfection and cleaning. Attention shall be payed to devices installed in the patient area.

4.2 General precautions and warnings

⚠	To guarantee the reliability and security of the software during use, strictly observe the instructions given in this section of the manual.

⚠	The Healthcare Organization shall ensure that the maintenance for the product and any third party device is implemented as requested to guarantee safety and efficiency and reduce the risk of malfunctioning and the occurrence of possible hazards to the patient and user.

⚠	The Product shall be used only by trained and authorized clinicians.

4.3 Privacy Policy

Appropriate precautions shall be taken in order to protect the privacy of users and patients, and to ensure that personal data is processed by respecting data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection.

> 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Special attention shall be dedicated to the data defined in "EU general data protection regulation 2016/679 (GDPR)" as "Special categories of personal data".

Special categories of personal data:
(…) Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and (…) genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The healthcare organization needs to assure that the use of the Product is in line with the requirements of the applicable regulation on privacy and personal data protection, specifically respect the management of aforementioned information.

The Product manages the following personal data:

- First name and surname
- Birthdate
- Sex
- Patient code
- Admission date
- Discharge date
- Patient weight
- Patient height

The Product can be configured to automatically hide this data on every application screen.
To do that, on the "Digistat Configuration Application", set the system option named "Privacy Mode" to "true" (see the Digistat configuration and installation manual for the detailed procedure). Its default value is "true".
If the "Privacy Mode" option is set to true, the following cases are possible:

- with no user logged in, no patient information is displayed.

- with a user logged in, and the user does not have a specific permission, no patient information is displayed.
- with a user logged in, and the user does have a specific permission, patient information is displayed.

The option can be applied to a single workstation (i.e. different workstations can be configured differently)

⚠ Please read the following precautions carefully and strictly observe them.

- The workstations must not be left unattended and accessible during work sessions. It is recommended to log out when leaving a workstation.

- Personal data saved in the system, such as passwords or users' and patients' personal data, must be protected from possible unauthorized access attempts through adequate protection software (antivirus and firewall). The healthcare organization is responsible for implementing this software and keep them updated.

- The user is advised against the frequent use of the lock function. Automatic log out protects the system from unauthorized accesses.

⚠ Personal data can be present inside some reports produced by the Product. The healthcare organization needs to manage these documents according to the current standards on privacy and personal data protection.

⚠ Client workstations (both desktop and mobile) do not store patient data on disk. Patient data is stored only inside database and database storage depends on the healthcare organization's procedures and choices (examples: physical machine, SAN, virtualization environment). Patient data shall be treated according all the current standards on privacy and personal data protection.

⚠ Patient data is not stored in proprietary files. The only place in which patient data is stored is database.

⚠ In some circumstances, personal data are transmitted in non-encrypted format and using a connection which is not physically secure. An example of this kind of transmission are the HL7 communications. The healthcare organization is responsible for providing adequate security measures to comply with the local privacy laws and regulations.

⚠ It is suggested to configure the database server so that the Product database is encrypted on the disk. To enable this option it is required SQL Server Enterprise Edition and during its installation it is necessary to enable the TDE (Transparent Data Encryption) option.

⚠ The healthcare organization is in charge to provide basic training regarding privacy issues: i.e. basic principles, rules, regulations, responsibilities and sanctions in the specific work environment.
Ascom UMS/Distributor shall provide specialized training on the best use of the Product relating to privacy issues (i.e. database anonymization, privacy mode, user permissions etc.).

⚠ The healthcare organization shall produce and keep the following documentation:

1) the updated list of the system administrators and maintenance personnel;
2) the signed forms of assignment and the certifications of attendance at the training courses;
3) a register of credentials, permissions and privileges granted to the users;
4) an updated list of the Product users.

⚠ The healthcare organization shall implement, test and certify a procedure of automatic deactivation of no-more-active users after a certain period.

⚠ The healthcare organization shall codify, implement and document a procedure for the periodic verification of belonging to the role of system administrator and technical maintenance personnel.

⚠ The healthcare organization shall carry out audits and checks on the correct behavior of the operators.

⚠ Databases containing patient data/sensible information cannot leave the healthcare organization without being encrypted/obfuscated.

4.3.1 User credentials features and use

This section explains the user credentials (username and password) features, their use and recommended policy.

- Every precaution must be taken in order to keep personal username and password secret.

- Username and password must be kept private. Do not let anybody know your username and password.

- Each user can own one or more credentials to access the system (username and password). The same username and password must not be used by more than one user.

- Authorization profiles must be checked and renewed at least once a year.

- It is possible to group different authorization profiles considering the similarity of the users' tasks.

- Each user account shall be linked with a specific person. The use of generic (for instance, "ADMIN" or "NURSE") must be avoided. In other words, for traceability reasons it is necessary that every user account is used by only one user.

- Each user has an assigned authorization profile enabling them to access only the functionalities that are relevant to their working tasks. The system administrator must assign an appropriate user profile when creating the user account. The profile must be reviewed at least once a year. This revision can also be performed for classes of users. The user profile definition procedures are described in the Digistat installation and configuration manual.

- Password must be at least 8 characters.

- The password must not refer directly to the user (containing, for instance, user’s first name, family name, date of birth etc.).

- The password is given by the system administrator at user account creation time. It must be changed by the user at first access in case this procedure is defined by configuration.

- After that, the password must be changed at least every three months.

- If username and password are left unused for more than 6 months they must be disabled. Specific user credentials, used for technical maintenance purposes, are an exception. See technical manual for the configuration of this feature.

- User credentials must also be disabled if the user is not qualified anymore for those credentials (it is the case, for instance, of a user who is transferred to another department or structure). A system administrator can manually enable/disable a user. The procedure is described in the Digistat installation and configuration manual.

The following information is reserved to system administrators:

The password must match a regular expression defined in the Product configuration (default is ^........* i.e. 8 characters). The password is assigned by the system administrator when a new account for a user is created. The system administrator can force the user to change the password at first access to the system. The password expires after a certain (configurable) period, after that period, the user must change the password. It is also possible (by configuration) to avoid password expiration.

See “Digistat installation and configuration manual” for detailed information on user account creation procedures and password configuration.

4.3.2 System administrators

Ascom UMS/Distributor technical staff, when performing installation, updates and/or technical assistance may have access to and deal with personal/sensitive data stored in the database and act as “System Administrator” for the Product.

Ascom UMS/Distributor adopts procedures and working instructions complying with the current privacy regulation (“General Data Protection Regulation - EU 2016/679”).

The Healthcare Organization should evaluate, among the others, the following technical measures:

- define nominal accesses;
- activate the operating system access logs both at client and at server level;
- activate the access logs on the Microsoft SQL Server database server (Audit Level);
- configure and manage all these logs to keep track of the accesses for at least one year.

4.3.3 System logs

The Product records the system logs on the database. These logs are kept for a configurable period of time. Also, logs are kept for different times depending on their nature. Default times are:

- information logs are kept for 10 days;
- logs of warning messages are kept for 20 days;
- logs of alarm messages are kept for 30 days.

These times are configurable. See “Digistat installation and configuration manual” for the configuration procedures.

4.3.4 Forensic log

A subset of the before mentioned system logs, defined according to the policy of each specific healthcare structure using the Product as “clinically relevant” or “clinically useful”, can be sent to an external system (either SQL database or Syslog) to be stored according to the healthcare structure needs and rules.

4.4 Backup policy

⚠ It is recommended to regularly backup the Product database.

The Healthcare Organization using the Product must define a backup policy that best suits its data safety requirements.

Ascom UMS/Distributor is available to help and support in implementing the chosen policy.

The Healthcare Organization must ensure that backup files are stored in a way that makes them immediately available in case of need.

If data is stored on removable memory devices, the Healthcare Organization must protect these devices from unauthorized access. When these devices are not used anymore, they must be either securely deleted or destroyed.

4.5 Out of order procedure

⚠ It is recommended to perform the backup of the image of the hard drive of the workstations, so in case of replacement of the hardware it is possible to restore quickly the operating environment.

⚠ Maintenance procedures and repairs shall be performed in compliance with Ascom UMS/Distributor procedures and guidelines and only by Ascom UMS/Distributor technicians or personnel specifically trained and explicitly authorized by Ascom UMS/Distributor.

This section describes the policy suggested by Ascom UMS in case a Digistat workstation gets out of order. The goal of the procedure is to minimize the time required to successfully replace the out of order workstation.

Ascom UMS suggests the healthcare organization has substitute equipment and an additional PC on which Digistat is already installed.

In case of a Digistat workstation is out of order, the substitute equipment can promptly replace the Digistat workstation.

Always remember that the Product Digistat must only be installed by trained authorized personnel. This includes Ascom UMS/Distributors staff and any other person specifically trained and explicitly authorized by Ascom UMS/Distributor. Without an explicit, direct authorization from Ascom UMS/Distributor, the healthcare organization staff are not authorized to perform installation procedures and/or to modify the Product Digistat configuration.

The risk related to the Digistat workstation deactivation or substitution is that to associate the workstation with a wrong bed or room. This could lead to a "patient switch", which is an extremely hazardous condition.

The risk related to the substitution and/or reconfiguration of network equipment involved in the data acquisition (i.e. port server, docking station, etc…) is that of assigning the acquired data to a wrong patient. The patient-acquired data relation is based on the IP address of the Digistat workstation. Changing it could lead either to data flow interruption or, in severe cases, to assigning data to the wrong patient.

⚠

The out of order and replacement of a workstation is potentially hazardous. This is the reason why it must only be performed only by authorized and trained personnel.

The risk related to this procedure is that of associating a wrong bed/room/domain to the workstation, and therefore display data belonging to the wrong patients/beds.

In case a Digistat workstation needs to be deactivated and replaced, the Healthcare organization staff must promptly call Ascom UMS (or authorized Distributors) and request the execution of this task.

Ascom UMS suggests the healthcare organization defines a clear, univocal operating procedure and to share this procedure with all the staff members involved.

In order to speed up replacement times, Ascom UMS suggests the healthcare organization has one or more substitution equipment with all the necessary applications already installed (OS, firewall, antivirus, RDP, …) and with Digistat already installed, but disabled (i.e. not executable by a user without the assistance of an Ascom UMS technician). In case of out of order of a Digistat workstation, the substitution equipment availability assures the minimization of restoration times (hardware substitution) and reduces the risk of associating patient data incorrectly.

In case of out of order of a Digistat workstation we suggest to adopt the following procedure if a "substitution equipment" is available:

1) The healthcare organization's authorized staff replaces the out of order PC with the "substitution equipment"
2) The healthcare organization staff calls Ascom UMS/Distributor and requests the "substitution equipment" activation

3) The Ascom UMS/Distributor staff disables the out of order workstation and correctly configure the “substitution equipment”
4) The out of order PC is repaired and prepared as “substitution equipment”

The instruction on how to enable/disable and replace a Digistat workstation, reserved to system administrators, is in the Digistat installation and configuration manual.

4.5.1 Reconfiguration/substitution of network equipment

In case it is necessary to either reconfigure or substitute a network device involved in the data acquisition, the healthcare organization staff must promptly call Ascom UMS/Distributor and schedule the substitution/reconfiguration procedure to allow Ascom UMS staff to either reconfigure the Product or provide all the necessary information to the healthcare organization. It is recommended, for this purpose, to define a clear procedure and share it with all the involved personnel. Some general indications about this are in the Product installation and configuration manual.

4.6 Preventive maintenance

⚠ Maintenance procedures and repairs shall be performed in compliance with Ascom UMS/Distributor procedures and guidelines and only by Ascom UMS/Distributor technicians or personnel specifically trained and explicitly authorized by Ascom UMS/Distributor.

It is suggested to perform the maintenance of the Product at least once a year. Maintenance frequency is a function of system complexity. In case of high complexity, it is suggested to perform maintenance more often, typically up to twice a year.

See the Product installation and configuration manual for the maintenance checklist.

4.7 Compatible devices

Please contact Ascom UMS/Distributor for the list of available drivers.

⚠ Digistat is not designed to verify that connected devices are working correctly but rather to acquire and catalog clinical data.

⚠ Disconnecting a device while it is running causes the interruption of data acquisition on Digistat. Device data that is lost during the disconnection period are not recovered by Digistat after reconnection.

⚠ Never disable the alarm notification on the medical devices unless explicitly allowed by the medical device manufacturer documentation and the procedure of the healthcare organization.

⚠ The correctness of parameters currently displayed by Digistat must always be double-checked on the original medical device that generated them.

⚠ Never disable the audio on the workstations on which Digistat is running.

⚠ For reasons that are outside the control of the software, for instance, the way the actual physical devices are installed/cabled, delays are possible between the alarm generation and the actual alarm display.

⚠ If the generic Alaris® Driver is in use it is necessary to wait at least ten seconds after disconnecting an infusion pump before connecting another.

⚠ The update of data displayed on screen caused by device connection, power off, disconnection and change of status depends on the time required by the device itself to communicate the changes. This time depends on various factors. Among them is the device type and type of connection. For some devices, there are conditions in which the delay in communicating changes might be important. Since they might change depending on devices configuration and operational conditions, it is not possible to provide an indication of the delays for all the possible devices.

⚠

The drivers used to read the data from the connected medical devices have a reading-cycle of less than 3 seconds (i.e. all the data from the devices is read every 3 seconds at maximum). However, there are devices that communicate the information less frequently (5-10 seconds interval). Refer to the specific driver documentation for details on the reading-cycle.
In a test environment installed and configured as indicated in the installation and configuration manual, as soon as a driver detects an alarm, it takes maximum 1 second to display on the user interface.

⚠

In case of electrical black-out, it takes a few minutes for the system to be fully operative again and therefore generate alarm notifications (usually this time is less than 3 minutes, however it depends on the configuration of the used computers).

4.8 Product unavailability

If during start up there are problems connecting to the server the system provides a specific information message.

The connection problem is often automatically solved in a short time. If it does not happen, it is necessary to contact the technical assistance (see section 5 for the contacts list).

In rare, often extreme cases, it may be physically impossible to use the Product.

It is responsibility of the healthcare organization using the Product to define an emergency procedure to put into effect in those cases. This is necessary to

1) Make it possible for the departments to keep on working
2) Restore as soon as possible the system to full availability (back-up policy is part of this management. See paragraph 0).

⚠

It is responsibility of the healthcare organization using the Product to define an emergency procedure to put into effect in case of system unavailability.

Ascom UMS/Distributor offers full support for the definition of such procedure.
See section 5 for the contacts list.

5. Manufacturer Contacts

For any issue, please refer first to the Distributor who installed the Product.

Here are the manufacturer contacts:

Ascom UMS s.r.l unipersonale

Via Amilcare Ponchielli 29, 50018, Scandicci (FI), Italy
Tel. (+39) 055 0512161
Fax (+39) 055 8290392

Technical assistance

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

Sales and products information

it.sales@ascom.com

General info

it.info@ascom.com

6. Residual risks

A risk management process has been implemented in the life cycle of the Digistat Product adopting the relevant technical standards. Risk control measures have been identified and implemented in order to reduce the risks to the minimum level and make them acceptable compared to the benefits brought in by the product. The overall residual risk is also acceptable if compared to the same benefits.
The residual risks listed below have been taken into consideration and reduced to the minimum level possible. Given the inherent nature of the "risk" concept, it is not possible to completely remove them; these residual risks shall be disclosed to the users.

- Inability to use the Product or some of its functionalities as expected, which could cause delays and/or errors in the therapeutic/diagnostic actions.
- Unauthorized actions carried out by users, which could cause errors in the therapeutic/diagnostic actions and in the allocation of responsibilities of these actions.
- Attribution of information to the wrong patient (accidental patient exchange), which could cause delays and/or errors in the therapeutic/diagnostic actions.
- Wrong handling of patient data, including errors in visualizing, adding, modifying and deleting data that could cause delays and/or errors in the therapeutic / diagnostic actions.
- Off label use of DIGISTAT® (e.g. Product used as a primary alarm notification system, therapeutic or diagnostic decisions and interventions based solely on the information provided by the Product).
- Unauthorized disclosure of users and/or patient's personal data.

RISKS RELATING TO THE HARDWARE PLATFORM IN USE (NOT PART OF THE PRODUCT)

- Electric shock for the patient and/or the user, which could cause injury and/or death for the patient/user.
- Hardware components overheating, that could cause injury for the patient/user.
- Risk of infection for the patient/user.