VOP			
Operating sub Process			
Documentation and Records, Control, Creation, Storage, Retrieval, Revision Control and Online Records			
Created:	27/03/06	VOP 01	Issue 1
		See the Route Map for related ISO Standards.	Page 1 of 5

SCOPE

This procedure is established to describe the system used within the company for the control of Documentation, and that all significant documents are subject to control. That only correct issues of relevant documents are available and in use. It is used in conjunction with the individual sub procedures, which show the relevant information necessary. The purpose of this document is to describe the system in use, at the company, in order to ensure Company Operating Procedures are binding instructions, and all members of staff are required to conform to the requirements therein. The requirement for new procedures, or changes to procedures can originate from any person within the company. These requirements will be discussed and agreed by management before processing

RESPONSIBILITIES

It is the responsibility of the Managing Director, to ensure that the contents of this procedure, and related procedures, are adhered to. To ensure the origination, upkeep, revision, control and authorisation of documentation, including technical documents, work instructions, specifications, records, forms, procedures and online documents.

OBJECTIVES

It is the Objective of this VOP to demonstrate the handling of Documentation, Records, Processes and any risks associated with them within the Companies, digital internally and online externally. Including the version control, retention, sole authority for top level documents, amendments and responsibility.

GENERAL

All Company operating procedures are complementary to, but DO NOT, replace the requirements of the Quality Manual (VOPs).
Company operating procedures are binding instructions and all members of staff are required to conform to the requirements therein.

DOCUMENTATION

Any change to system documentation or process(s), if they are linked to either a VOP, ISO Standard, Sub Process, or Controlled Product Technical File, will have a Risk of Change or Impact Assessment created. This assessment will then be uploaded to the controlled documents in the Document Index and linked to Top Level Document that is to be updated.

Documents such as procedures, instructions, specifications, online records etc. are retained as Word documents, Autocad, PCB, HTML and PDF documents, and are stored electronically (Read Only) therefore making them available to all personnel, for information purposes.

All documentation including international standards and technical files are now digitally controlled. Internal documents, not designated to be used external to the system, have a computer controlled revision ID, and updated date. A warning on the user view of documentation:

"All Documents while viewed live are CURRENT. Printed internal documents should have the date written on them and the Document ID / Version Control #Number and destroyed the next day, or be destroyed immediately after use"

All documents have the relevant ISO Route map detailed in the Admin page for each document, to show the section they relate to.

DOCUMENT CHANGE / AMENDMENT

See VM3COP24.02 Document Change Performing a Risk Assessment Prior to document change / amendment.

The Managing director will decide when a company operating procedure or top level VOP requires updating.

All essential documents contain a change / revision facility. This is controlled by date revised and last date printed. Printed is either electronic or hard copy. Departmental heads are responsible for ensuring prompt removal of obsolete documents from all points of use. This is controlled by the system, any printed documents are deemed immediately out of date.

Where Significant Changes have been made to a Company Document / Management System e.g. major modifications to procedures or a reduction in quality surveillance, or to such as the Design / CE Files. Then the appropriate Notified Body(s) will be informed in writing, with copies of the changes where required. Details on what constitutes a significant change can be found on the notified bodies Terms and Conditions.

Documents that are amended, the new document will get a new document ID, and the obsolete document, will be filed away in the history of the new document only available to the admin panel of the Document Index limited to directors.
Any users who have use of the obsolete document, will be informed by the Intrastats system, that the document has been updated, or prior to the process being performed.

All documentation in the document index have a request amendment function so end users can request an amendment, this creates an internal issue to log any changes or updates potentially required. The issue can track the changes of a document until its finally approved, assessed for risk and uploaded to the system.

Once an updated or new document is submitted for approval a risk assessment will be carried out to ensure the updated or new document does not cause a change of risk or new risk, in its creation. This risk assessment will be attached to the Archived Document.

When the Document is uploaded a description of the changes / updates made and any other relevant information is added to the notes field before submission.

Control of online Documents and Data e.g. Webshop, Website, Email Templates, Price lists, Leaflets, Terms and Conditions and Terms of Sales. A log of the amendment will be kept and reviewed by the Documentation and Records Controller regularly. All updates will be reviewed by a director to ensure correct and up to date data and information is available.

TECHNICAL DOCUMENTATION

When engineering drawings and / or specifications are created for manufacturing purposes, the documents will be authorised and Uploaded to the Document Index. Authorised by the Managing Director.

Manufacturers manuals and technical data sheets, British and International standards, together with any regulatory guidance documents are maintained in the Document Index for reference purposes.

All relevant Standards are filed and indexed in the document Index and are allocated a document ID and are maintained up to date annually by reference to the BSI guide. European Commission harmonised standards to check documentation up to date https://ec.europa.eu/commission/index_en.

Quality assurance records are electronically stored against the products barcode identifiable to the product.
A network is installed and the central File server holds a master copy of all files, which require shard access. All centrally held files are backed up routinely by the IT Controller.
All CE and Design files are maintained by the Technical Controller and are available for viewing electronically.
All documents are being entered systematically into the Intrastats system.

The Technical files documentation is available in the Document Index and in the Technical Files. Here you can view documentations grouped together per product technical files, and files sectioned of into appropriate headers. Where a document applies to more than one header it can be filed in both sections, however both section will refer to the same document ID, and if that document get updated, all documents in the section with that ID will be updated.

DOCUMENTATION FROM EXTERNAL SOURCES

There are now very few sources of paperwork, within in the company. But we do receive paper documents from the delivery companies. Those relevant to Customer orders are scanned and uploaded. Those not needed, are placed in archive and kept for the required length of time.
Bank statements and other financial documents are filed securely where needed. We endeavour to reduce the need for any paperwork to zero, where ever we can.

OUT OF DATE DOCUMENTS

When a document has an expire date, it is set in the Document Index and is flagged as out of date to the end users. A regular task to check the out of date documents register is performed by the Documentation and Records Controller, who is responsible for updating the documentation.

DUPLICATE DOCUMENTS

The system will automatically flag, if a document has been entered into the system twice. So they can be merged together and only one document becomes available to the end users. A regular task, to check the Duplicate Documents is performed by the Documentation and Records Controller.

INFORMING EXTERNAL BODIES

It is the responsibility of the Managing Director to inform the External Bodies of any Significance Changes, to either the Quality Management system or to the CE marked products. E.g. BSI, CMDCAS, MHRA.

DOCUMENTS BACKUP

Documents are backup from one building to the next building every evening into the live Backup System.
Off-Site backups are performed every day.

FILE TYPES

In most cases the file types of documents are automatically detected, however in some cases, if using less well known software, the File type and version of software should be noted in the 'Document Notes Displays on main Doc View Screen' box of the Admin Document.

EXTRA DOCUMENT OPTIONS

After a document has been uploaded to the system, the document can be linked to various sections of Intrastats, i.e.

- Type of documentation
- Host Company (Viamed / VST / Humanmed / Vandagraph / Viamed Properties)
- Security Level (Internal use only / External use approved / Manager Access only)
- Products
- Contacts
- Technical Files
- Expiry date
- Hidden search terms
- Download name if different to the stored index name
- Linked to a Training Course
- Link to BSI Route Map
- Roles, Tasks and mini Audit System

Once a document is linked it will present itself as and were appropriate. i.e. In a product search, it will be available from the Stock/Product screen.
If its updated and a user has been trained and its part of the training program, the user will be alerted the document has been updated.
Top level Documents and other key documents will trigger a Required Reading notification to appear on relevant staff Intrastats.

RETENTION OF RECORDS
Intrastats records are kept indefinitely and securely.

PRIVATE DATA
Private information will be treated as per GDPR.
Except upon a GDPR Subject Access Request where any data not legally required for ISO or Legal traceability will be removed from the system relating to the GDPR Request.

SENSITIVE DATA
Viamed / VST do not have any products which store patient data / identifiable information. Should we receive any sensitive data / health information from an outside source. The data shall not be digitised into the system but passed to the Managing Director to safely dispose of, and an Issue generated to the GDPR supervisor to decide how to proceed.
The source of the information will be informed of the breech at their end, and a report produced by the GDPR officer within Viamed/ VST.

Sensitive Data stored on staff e.g. contact details, health information, wage / pay and banking information will be restricted, used only where necessary and controlled by the GDPR Controller.

PROCESS CONTROL
All ISO processes are linked to the relevant Route Map. All documents have processes linked to them and listed on the document Admin page.
Control of the processes is by top management. Risk is assessed when the process is added or updated.