

POLICY

Investigation Policy

Document Control: -

Document Control Information	Details
Policy Name	Investigation
Policy Number	OGPO228
Status	Approved
Date Approved by Board	18 th October 2024
Next Review Date	October 2025

Date	Description	By	Version
Oct 2024	Created	H Walker	V1

Investigation Policy

- 1) A request for an incident investigation can only be made by an Ortus customer whereby the device in question was sold directly by the Ortus Group.
- 2) Ortus require that all customer name a designated Medical Device Safety Officer to coordinate all Investigations and reporting.
- 3) Ortus categorise reported incidents as
 - a) Technical Support: a request for support has been submitted from a customer – who generally undertakes their own servicing/ repairs – where more advanced technical investigation is required.
 - i) Ortus would require the Incident Investigation Form and/or Mission File as a minimum
 - b) Incident Support: a request for detailed support has been submitted whereby a customer requires more technical information (i.e. detailed overview of what happened according to the mission file) when an incident has been reported internally to them.
 - i) Ortus would require the Device, Mission File, Datix and SBARDR, but understand one or more of these are normally not available.
 - c) Clinical Incident: a request for support where there has been material impact
 - i) in relation to a patient, no matter how minimal (i.e. delay in diagnosis/ treatment etc).
- 4) Where an approved Service Partner requests Technical Support, Incident Support or Clinical Incident, the request must be submitted with a full device STK and Mission File with a clear description of the specific event(s) requiring investigating
 - a) Ortus require the Incident be reported by the designated MDSO, with generic Fault Category listed and relevant IMDRF codes applied
 - b) Where an STK and specific reference to Mission File is not present, Ortus will return the device in question.
 - c) In the event that Ortus undertake a Full STK in the event of Technical Support, Incident Support and/or Clinical Incident, we reserve the right to charge for a full Service.
- 5) Ortus require the Device in question and all associated accessories and consumables, Mission Files for the full shift, Datix, SBARDR, and complaint Form completing.
- 6) If a staff member is informed of an incident whilst in discussion with customers, they are duty bound to report it, in writing, to md-vigilance@ortus.co.uk within 24 hours.

- 7) A review of any complaint, using the Vigilance Decision Tree (see Process OGPO22a), will happen within 2 working days from the initial date this issue was reported to the MD Vigilance mailbox.
- 8) If an incident is reportable, the timeframes in which it becomes reportable will be determined via the Vigilance Decision Tree process (see Process OGPO22a).
- 9) Where the reportable score is >01, the first notification will be sent to the manufacturer, and a manufacturer-specific Complaints Form will be issued to the relevant customer.
- 10) All requests for investigations will be logged on our investigation pipeline (HubSpot) for tracking purposes.
- 11) All investigation requests raised in HubSpot will include the output score from the Vigilance Decision Tree.
- 12) All investigation requests will have a generic Fault Category attributed to it.
 - a) Fault Categories are:
 - i) Defibrillation,
 - ii) ECG,
 - iii) Capnography,
 - iv) Oximetry,
 - v) NIBP,
 - vi) IBP,
 - vii) Temperature,
 - viii) CPR Feedback,
 - ix) Configuration,
 - x) Modularity/Functional,
 - xi) Other
- 13) All investigation requests raised in HubSpot will include the relevant IMDRF Adverse Event Terminology as per: <https://www.imdrf.org/working-groups/adverse-event-terminology>
 - a) Shortcut Coding can be seen here: Active IMDRF codes.xlsx
- 14) All investigations will be recorded on our Medical Device Database (Microsoft Business Central) by raising a ticket and linking all relevant Equipment Files.
- 15) The Service Order Number will be attached to the HubSpot Ticket in the relevant field.
- 16) A SharePoint Folder will be created within the Ortus Quality Management System.
- 17) All files will be stored here (Mission Files, completed SBARDR, Incident Reports etc.)
- 18) Where the outcome score of the Vigilance Decision Tree (see Point 4) is >01, Ortus will request to undertake an SBARDR for the incident in question.

- a) Ortus will allow 2 weeks for this. In the event no information is forthcoming that will enable the SBARDR, or the customer refuses this, which is ever sooner, an investigation report will be undertaken on the Device and Mission File/Data only.
 - b) All Technical Incident Reports whereby an SBARDR is not possible will reference this fact. Where it was possible to undertake the SBARDR, the evidence will be taken into consideration, and attached as evidence in the Technical Incident Report.
- 19) Investigations that involve accessories and consumables that are not provided with the device will not provide a definitive root cause analysis.
- 20) Investigations where only Mission Files are provided will not provide root cause analysis, rather just a descriptive prose on key events recorded on the Mission File.
- 21) Where an investigation is requested and only the Device is provided, it will be held in quarantine until the Mission File is provided.
- 22) Investigation Reports will not be written in the absence of a Mission File.
- a) If no Mission File is sent, the Device will only be released back into service at the written request of the customer. A full functional test will be undertaken, and any remedial actions taken. No report will be provided.
- 23) Ortus will endeavour to provide a Technical Incident Report 20 working days after the Device and Mission File (as a minimum) are received.
- 24) Where it is deemed relevant for the Device to be sent back to the Manufacturer, then the Official Complaint Form must be completed by the customer requesting the investigation. The Generated Vigilance number generated by the manufacturer will be added to the HubSpot Ticket.
- 25) Where required, all reportable incidents will be reported directly to the Manufacturer on the same day the Vigilance Decision Tree outcome is determined. In collaboration with the Manufacturer, relevant MIR reports will be submitted via the MHRA MORE System.
- 26) In March, June, September and December of each calendar year, the MDSG Group will undertake a Vigilance Analysis to investigate all Incident Categories, IMDRF Codes and RMA Fault Codes in that Quarter, Year, and 3 Year Period (or as long as reporting allows).
- 27) All Vigilance Data/Analysis will be shared with the Manufacturer to incorporate in to Global Trend Analysis.

Approved by: Peter Benson

Date: 18.10.2024