

Introduction

When a issue (or nonconformity) occurs, the Smartwatch;

- a) react to the nonconformity, and as applicable: Log the Non-Conformity using the procedure below. Understand the scope and impact of the issue.
 - 1) take action to control and correct it; On the log state any initial correction (what you did to control the issue)
 - 2) deal with the consequences; If any actions taken have consequences log this
- b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by: this should be logged for all issues using procedure below
 - 1) reviewing the nonconformity; This is done at management review
 - 2) determining the causes of the nonconformity; In the “Root Cause Sections” of the log
 - 3) determining if similar nonconformities exist, or could potentially occur; In the Correction action and comments of the log.
- c) implement any action needed; Detail in correction how the issue was contained
- d) review the effectiveness of any corrective action taken; Management Review check on the correction and corrective action of all log items since last management review.
- e) make changes to the information security management system and business continuity management system, if necessary.; Detail changes in sections for correction and corrective actions

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The Smartwatch retains documented information as evidence of:

- f) the nature of the nonconformities and any subsequent actions taken; ensure logs comments and items assigned are kept up to date
- g) the results of any corrective action; This is done at management review

Logging

Smartwatch ISMS systems have integrated preventive measures built into the respective processes, procedures and instructions.

However, sometimes due to unforeseen circumstances, things can and do go wrong, and can impact on the service we provide.

When a non-conformity, incident or event, observation or opportunity for improvement is found these should be recorded on procedure (regardless if they are event, incident etc).

Non-Conformity

A Non-Conformity is a failure of a person, process or system to follow the requirements of the international standards or Smartwatch documented procedures and standards. This is often logged at external or internal audit.

Event

An Event is a “Near miss”. Something that is wrong but no actual information loss / information breach has occurred. These should be logged using this procedure and marked as “Event” below.

Incident

An incident is when something has gone wrong which has led to an information breach

It is essential for all staff to be able to identify when and where an incident occurs within our ISMS, and take the appropriate reporting measures, whereby the incident is immediately reported to the ISMS Representative, who will record, investigate, and determine the appropriate corrective and/or preventive actions to be taken, with the departmental head / persons concerned.

As part of the promotion of the ISMS awareness around the organisation, the ISMS Representative will educate staff on what to look for in identifying actual or potential areas of non-conformity, where information security could, or is actually compromised.

Opportunity for Improvement

An “OFI” is used by auditors, staff or external interested parties to make suggestions to help Smartwatch to improve their management systems

Observation

Observations are areas of risk or concern that could lead to a future non-conformance

Collection of Evidence

When appropriate evidence must be collected in relation to nonconformity, event or incident. In these cases objective evidence must be protected and restricted to appropriate staff members. Where possible collect evidence and store along side the appropriate forms.

0. Severity Classification

Incidents and nonconformities shall be classified by severity:

- Minor: No significant impact on operations or data integrity.
- Major: Significant impact requiring immediate corrective action.
- Critical: Severe impact including data breach, legal or regulatory violation.

Severity classification must be recorded in the incident log and used to determine escalation and response timelines.

1. Defined Roles and Responsibilities

The following roles are defined for incident and issue management:

- ISMS Representative: Oversees the incident management process.
- Incident Owner: Assigned to each incident to coordinate investigation and resolution.
- Investigators: Conduct root cause analysis and recommend corrective actions.
- Approvers: Review and approve corrective actions and closure.

All roles must be documented in the incident log.

2. Integration with Business Continuity

All incidents must be assessed for potential impact on business continuity.

Where applicable, incidents shall trigger activation or review of Business Continuity Plans (BCPs).

The ISMS and BCMS teams must coordinate to ensure alignment of corrective actions and continuity measures.

Signed:

Position: Managing Director



Name: Neil Jones

Date: 31/07/2025