NetGain systems	No of Pages	**1** of **5**
	Document Classification:	Internal
	Effective Date	1 Aug 2025
CONTROL OF NONCONFORMITY AND CORRECTIVE ACTION	Doc No	ISMS-PR-05
	Revision	1.0

AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE

This document describes the way in which nonconformities will be identified, logged and managed to resolution.

SCOPE

This procedure applies to any nonconformity requiring corrective action due to the impact it has on the Information Security Management System (ISMS).

REFERENCE

ISO/IEC 27001 Standard	10.2 Nonconformity and Corrective Action

DEFINITION

Nonconformity — A nonfulfillment or failure to meet a requirement.

Correction — Any action that is taken to eliminate a nonconformity but does not address root causes to prevent recurrence of a nonconformity.

Corrective Action — Steps that are taken to eliminate the root causes of existing nonconformities in order to prevent recurrence.

RESPONSIBILITIES & AUTHORITIES

The Top Management has the prime responsibility and approval authority for this procedure.

The person-in-charge of the nonconformity is responsible for dealing with the consequences, and to determine effective corrective action.

All employees are expected to comply with established procedures to avoid nonconformities. Any employee discovering a potential or actual nonconformity in their work area is responsible to notify his / her immediate superior immediately.

PROCEDURE

The procedure for identifying and managing nonconformities is summarised below.

1. Nonconformities may be identified from any source and the Management Representative (MR) shall encourage staff, users, customers and suppliers to propose ways in which they can be addressed.

2. Such nonconformities may be identified from, however the below is not an exhaustive list:

   - Information security reviews
   - Day-to-day operations
   - Team meetings
   - Supplier / client meetings, where applicable
   - Information security risk assessments
   - Internal and external audits

3. Once identified, the nonconformity will be documented within the *Nonconformity and Corrective Action Log* with “Open” status*.* At this stage the action to correct the nonconformity has not necessarily been determined. As much detail as possible should be specified as to the exact nature of the nonconformity.

4. If action needs to be taken to address the nonconformity immediately then this should be done without delay. This may be to fix it, stop it from getting worse or to reduce its effects until further action may be taken. Appropriate resources should be allocated to addressing the nonconformity depending on the current assessment of its seriousness. The plan to address any identified nonconformity should be presented no later than 5 business days or sooner depending on the severity. Corrections taken should be recorded in the action log.

5. The nonconformity will be evaluated no later than 5 business days or sooner depending on the severity to assess its underlying cause i.e., why it has arisen in the first place, and the further “whys” in succession, as applies (Why-Why Analysis). Other parties may be consulted during this stage to understand the mechanism and events leading to the nonconformity.

6. The identified cause should be recorded in the action log with as much description as appropriate.

7. Once the cause is understood, a review should be undertaken to assess whether similar nonconformities already exist elsewhere within the ISMS and whether they could potentially arise in the future.

8. Once the cause and real or potential impact has been established, appropriate corrective action should be identified to address both the current situation and potential future impact of the nonconformity. The expected benefits of correcting the nonconformity should be sufficient to justify the resources required to achieve the corrective action.

9. The details of the corrective action to be taken should be recorded in the action log, along with the person responsible and the target date of completion which should be within a reasonable period of time depending on the required resources and its availability to implement the corrective action taken. In general, target date of completion for corrective action to address a nonconformity must be within a month. If longer timeframe is required, justifiable reasons must be provided in the *ISMS-PR-05-F1 Nonconformity and Corrective Action Log.*

10. Once corrective action has been completed the status of the nonconformity in the log should be updated to “Review Pending” and the date of closure recorded.

11. The effectiveness of the corrective action should be reviewed by the MR to assess whether it has fixed the issue, including its actual and potential impacts.

12. If the benefits expected are not achieved, the reasons for this will be investigated as part of the regular management review meeting.

13. If successful, the date and results of the review will be recorded and the status of the nonconformity will be updated to “Closed”.

14. If the nonconformity is judged to have occurred due to a fault in the ISMS, it may be necessary to review and amend the relevant policies, procedures, information security risk assessments and controls. This should be done through a joint review by the process owner, the MR and the top management.

FORMS

ISMS-PR-05-F1 Nonconformity and Corrective Action Log