

ITS: Nonconformance & Continual Improvement Policy

1. Purpose

- 1.1. This policy details how the Information Security Management System (ISMS) will be managed in order to ensure it remains aligned with the requirements of ISO 27001:2022, delivers the ISMS's intended outcomes and is improved on an ongoing basis.

2. Legislative and regulatory context

- 2.1. This policy is aligned with the ISMS Legal Register.

3. Scope

- 3.1. This policy covers actions required to monitor and manage the performance of the ISMS and to ensure it addresses the requirements of ISO 27001:2022 satisfactorily. It also covers how the ISMS will remain aligned with the University's objectives, both now and in the future.

4. Principles

- 4.1. The University's policy is that:
- its employees and contractors must adhere to the ISMS at all times
 - any nonconformances must be identified at the earliest opportunity, then logged and addressed
 - its ISMS must conform with the requirements of ISO 27001:2022
 - its ISMS must be improved on an ongoing basis in order to provide an appropriate level of protection at all times

5. Roles and responsibilities

- 5.1. It is the responsibility of internal auditors under the direction of the Head of Information Security to create an audit schedule.
- 5.2. It is the responsibility of Information Technology Leadership Team (ITLT) to ensure management reviews are conducted at least once annually and review nonconformances and opportunities for improvement.

6. Terminology

- 6.1. The following terms are used throughout the policy:
 - Must is used to state a **mandatory** requirement of this policy
 - Must not is used to state a **prohibition** of this policy
 - Should is used to state a **recommendation** of this policy
 - References to internal or external auditors refer to ISMS auditors

7. Internal Audits

- 7.1. Internal audits must be conducted to assess compliance with all aspects of the ISMS and to make sure the ISMS continues to support the University in achieving its wider objectives.
- 7.2. An audit programme must be created and maintained which sets out when each policy will be audited, how and by whom. Records of the audit programme must be retained.
- 7.3. The timing and frequency with which each policy is audited should be based on risk, organisational need and the results of previous audits.
- 7.4. The scope and criteria of each audit must be defined in advance of the audit taking place.
- 7.5. Internal audits must be conducted by people who are independent of the area they are auditing and who are competent to conduct them.
- 7.6. The findings of internal audits must be documented and retained as evidence of the implementation of the internal audit programme. Their results must be reported to IT Leadership Team.
- 7.7. Nonconformities and potential improvements must be recorded in the internal audit report and considered by the IT Leadership Team.

8. External Audits

- 8.1. The ISMS must be reviewed independently at planned intervals or when significant changes occur. The purpose of these reviews is to ensure the ISMS continues to meet all the requirements of ISO 27001:2022; to ensure the ISMS is being complied with by all those it applies to; and to identify any opportunities for improvement.
- 8.2. The independent reviews must be carried out by an external organisation which specialises in information security and whose staff have appropriate qualifications and experience.
- 8.3. The findings of external audits must be documented and retained as evidence of the implementation of the external audit programme. Their results must be reported to the IT Leadership Team.
- 8.4. Nonconformities and potential improvements must be recorded in the external audit report and considered by the IT Leadership Team.

9. Management Review

- 9.1. A management review group must be formed to assess the effectiveness of the ISMS. It must include representatives of ITS management.
- 9.2. Management reviews of the ISMS must be conducted at least once a year. The agenda for its meetings must include as a minimum all the headings mandated by ISO 27001:2022. As part of those reviews, progress in relation to ISMS objectives must be considered and opportunities for improvement and any nonconformities must be discussed.
- 9.3. Records of management reviews must be kept and retained. These records will highlight decisions and actions relating to opportunities for improvements; changes needed to the ISMS; and the resources needed to support the ISMS on an ongoing basis and to complete specific changes.

10. Nonconformances and Corrective Action

- 10.1. Nonconformances may be identified from a range of sources, including:
 - internal and external audits
 - observations made by internal or external specialists
 - observations made by employees
 - issues and incidents

- management review meetings
- 10.2. A log of nonconformances and opportunities for improvement must be created and maintained.
 - 10.3. When a nonconformance is identified, a decision must be made about whether and how to control and correct it as well as how to deal with any consequences. This must be recorded in the log of nonconformances.
 - 10.4. All nonconformances must be evaluated in order to determine whether action is needed to eliminate the cause so as to ensure it does not recur or occur elsewhere. These evaluations must:
 - review the nature of the nonconformance
 - determine its cause
 - determine whether similar nonconformities may also exist or potentially could occur
 - 10.5. Records of evaluations must be included in the log of nonconformances.
 - 10.6. Appropriate corrective actions must be determined and recorded in the log of nonconformances. Approval may be required before a corrective action is implemented. The respective process owner must ensure that senior decision-makers are aware of and accept the time, effort, cost and impact of the proposed resolution before corrective actions are taken.
 - 10.7. The impact of corrective actions must be assessed in order to determine whether they have had the intended effect. Where they have not, alternative actions must be defined, implemented and assessed.

11. Continual Improvement

- 11.1. Following the results of internal and external audits, recommendations for continual improvements must be considered.
- 11.2. Queen Mary must ensure that recommendations for continual improvement are received from a range of people and that a mechanism is in place for requesting continual improvement recommendations across ITS.
- 11.3. Recommendations for continual improvements must be logged and actions taken where appropriate.

12. Monitoring

- 12.1. Compliance with the policies and procedures laid out in this document must be monitored by the Information Security Team as directed by the Head of Information Security, along with independent reviews by both internal and external auditors on a periodic basis.
- 12.2. The Governance, Risk and Compliance Manager, in conjunction with the Head of Information Security, is responsible for the monitoring, revision and updating of this document.
- 12.3. The effectiveness of this document must be evaluated on an ongoing basis as part of the management of the ISMS and formally reviewed each year at the Management Review.

13. Exceptions

- 13.1. Any exception to this policy must be documented with business reasoning and signed off by the University's Chief Information Officer and Head of Information Security before being taken forward.

14. Associated information

- 14.1. Accompanying the ISMS is a Statement of Applicability. This lists all the requirements of ISO 27001 and states how the University will fulfil them.

15. Review

- 15.1. This policy will be reviewed annually by the ISMS operational team, with a full review by the policy owner every three years.
- 15.2. Minor updates to this policy that do not affect the rules, principles or intent of this Code may be approved by the Head of Information Security on behalf of the Information Governance Group.

Policy Information and Document Control

Policy title	ITS: Nonconformance and Continual Improvement Policy
Version number	V1.1
Related policies and procedures	Statement of Applicability
Superseded policies	n/a
Approval level	Information Governance Group
Approval date	22 nd April 2025
Last review date	8 th January, 2026
Next review due	January 2029
Policy owner	Rachel Bence – CIO
Policy contact	Ambrose Neville – Head of Information Security

Version Control

Version	Date	Reason for updates/Summary of key changes
v1.0	22/04/2025	Initial release.
v1.1	08/01/2026	Annual & Periodic review for the PSG 2026 review. Minor updates include the use of 'Must' instead of 'Shall' as per the University Policy Writing Guide.