	Name & Position	Effective Date
Approved by:	**Dr Damien Bennett, Director**	**24/07/2024**

Information Security Policy Statement

The Northern Ireland Cancer Registry (NICR) have established and maintain an Information Security Management System which is accredited to ISO27001.

1. **Information Security Management System (ISMS) overview:**
   - ISMS provides structured processes for the achievement of Information Security objectives and commits to protecting the confidentiality, integrity, and availability of all our data assets.
   - NICR has implemented documented policies and procedures in accordance with the requirements of the ISMS which apply to all employees, contractors, and third parties who interact with our systems.

2. **Scope of ISMS:**
   - NICR, based in Mulhouse Building, Queen's University Belfast, is responsible for the collection, processing, storing, and sharing of information regarding instances of cancer and premalignant disease in Northern Ireland in line with all legal, regulatory, and ethical obligations.

3. **Key Principles:**
   - ISMS is designed to work alongside the existing legal, statutory, regulatory, and contractual requirements that the NICR abides by, which include the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018.
   - Management is committed to and actively support information security.
   - NICR assess and mitigates risks to prevent security incidents.
   - Regular training ensures staff understand their security responsibilities.

4. **Roles and Responsibilities:**
   - Responsibility for implementation and ongoing effectiveness of the ISMS ultimately rests with the NICR Director.
   - NICR Director has delegated responsibility to the ISO Lead to oversee implementation and maintenance of the ISMS.
   - All employees play a role in maintaining the confidentiality, integrity and availability of information held within the NICR.

5. **Continuous Improvement:**
   - As Information Security Objectives are achieved, new objectives will be set to ensure the organisation continues to improve all areas of Information Security.
   - Internal audits are completed by trained members of staff on a regular basis to ensure requirements of the standard are met and risks are effectively addressed within the organisation.
   - Feedback from audits and incidents are reported to Senior Management to drive improvements.
   - The policy statement is reviewed annually.