Integrity Systems

red meat customer assurance

STANDARD

FOR THE NATIONAL LIVESTOCK IDENTIFICATION SYSTEM API

IMPORTANT NOTICE
This Standard is issued by Integrity Systems Company (ISC). It is the responsibility of the person using this Standard to check that they have the current version of this document.

The current version of the Standard is available on ISC's website at integritysystems.com.au

Date	Change Description	Author	Issue Number
31/01/2025	First version	Peter Quigley	1

Table of Contents

1. Scope

1.1. The roles covered by this Standard are:

a) Producer;

b) Processor;

c) Saleyard;

d) Feedlot;

e) Tag Manufacturer;

f) Livestock Agent;

A Government Agency; and

g) Any other industry or supply chain based roles added by ISC from time to time

2. Introduction

2.1. The National Livestock Identification System (NLIS) is a nationally agreed system, managed by Integrity System Company Ltd (ISC), which enables secure electronic data transfer between approved parties using standardised interfaces.

2.2. Commercial software vendors, under NLIS API System Access Agreements with ISC, to develop and maintain API integrations with NLIS (e.g., web, mobile, and system applications) for system users to input, transfer and retrieve NLIS data.

2.3. The NLIS API and NLIS Terms of Use are used to support seamless transfer of data between users of the NLIS via the central NLIS System using APIs supplied by ISC.

2.4. Data is retained in the central NLIS System to support traceability and biosecurity capability and management of the industry's integrity system.

2.5. This Standard provides minimum mandatory specifications and requirements for software vendors seeking to access the NLIS API System.

2.6. The core components of the NLIS API System are:

a) Nationally agreed API definitions and the NLIS Operational User Guide and Terms of Use for the submission and retrieval of data to the central NLIS API System;

b) Commercial software vendors providing users with NLIS API tools under NLIS API System Access Agreements.

2.7. ISC operates and administers the testing and approval of NLIS API software tools. An NLIS API System Access Agreement between the applicant and ISC allows the Approved Software Vendor to access and use the NLIS API System. End users accessing the NLIS System through approved software must comply with the NLIS Operational User Guide and Terms of Use. A copy of these agreements are available from ISC.

2.8. ISC can, at its reasonable discretion, amend this Standard at any time to further improve the operation and integrity of the NLIS API System. Approved Software Vendors will be required to comply with the requirements of the new version of the Standard within the timeframe specified by ISC – being not less than 30 days. This includes changes to the NLIS API and changes arising from changes to the NLIS Operational User Guide and Terms of Use.

3. Compliance Requirements

3.1. Software vendors must demonstrate and maintain compliance with:

a) The NLIS API and the NLIS Operational User Guide and Terms of Use as defined in the ISC Developer Portal and NLIS website

b) All requirements specified in the Application form

c) The security and data handling requirements defined in this Standard

d) The technical security requirements specified in the ISC Developer Portal, including but not limited to:

- Encryption standards for data in transit and at rest
- Authentication and authorisation mechanisms
- Key management practices
- Security logging and monitoring requirements
- Access control implementations
- Vulnerability management processes

3.2. The technical security requirements specified in the Developer Portal are considered a mandatory extension of this Standard. Changes to these requirements must be implemented within timeframes specified by ISC.

3.3. These requirements must be met at all times, including after initial approval and while the software is being offered to end-users in a live environment.

3.4. ISC maintains the right to conduct security assessments and request evidence of compliance with security requirements at any time.

4. Software Assessment

4.1. To become and remain an Approved Software Vendor for the NLIS API System, providers must:

a) Complete an Application form.

b) Submit evidence of compliance against the assessment criteria set out in the Application form, undergo testing as reasonably determined by ISC, including a live demonstration, and pass that testing.

c) Enter into an NLIS API System Access Agreement for the NLIS API System, including any NLIS roles access has been granted for.

d) Be compliant with this Standard and the NLIS API System Access Agreement terms at all times.

e) Continue to comply with updates to the NLIS API System, including further testing, as the NLIS API System is modified.

4.2. Applicants seeking NLIS API software access must provide ISC with a completed Application form along with the supporting documentation required by the form. Copies of the Application form are available from integritysystems.com.au

4.3. ISC will assess the Application and determine whether the software will be granted approval or if additional assessments are required, based on the information provided.

4.4. The scope of the software to be assessed includes:

a) Security controls implementation

b) Authentication mechanisms

c) Data handling processes

d) Review of applied encryption processes defined in the Security and Quality Assurance information specified in the Application

e) Environment separation and management processes

f) Service account control implementation

g) Business continuity procedures and documentation

h) Technical support capabilities and processes

4.5. The assessment will address those roles within the scope of the Application. They may include the roles as specified in 1.1 of the Standard. The extent of the assessment will be subject to the scope of the approval sought.

4.6. Individuals and organisations seeking approval of their software must supply evidence to demonstrate that their software complies with the Standard. Only software that has been approved by ISC under this Standard can be used to access the NLIS API System and be supplied for use under the NLIS API System.

4.7. Consideration of software submitted for approval will be limited to the scope of the Application.

4.8. Where the application indicates an intention to use the NLIS API within a number of Software Product(s), ISC will nominate the Software Product(s) to be assessed.

4.9. The Approved Software Vendor must provide ISC with the ability to access the approved software as a test user within their User Acceptance Testing and Production environments, as requested.

4.10. Approval will be granted when:

a) The software has been assessed by ISC and has complied with the NLIS API and the NLIS Operational User Guide and Terms of Use provided by ISC;

b) Software complies with this Standard; and

c) The applicant enters into an NLIS API System Access Agreement with ISC.

4.11. To maintain approval, Approved Software Vendors must maintain:

a) Compliance with NLIS API and the NLIS Operational User Guide and Terms of Use;

b) Compliance with this Standard; and

c) Compliance with the Application.

5. Supply of Approved Software

5.1. The Approved Software Vendor must have a Quality Assurance (QA) system and process, which, as far as is practical, eliminates the possibility of errors associated with the supply of the software service, and provides timely responses to clients.

5.2. The Approved Software Vendor is responsible for supporting their clients with NLIS API-related software queries and issues.

5.3. The Approved Software Vendor must have procedures that comply with the nominated response times for changes to the Standard within the timeframe specified by ISC.

5.4. The Approved Software Vendor must have a procedure for addressing software errors, system outages, and managing software changes and to notify clients of such changes.

5.5. The Approved Software Vendor must, upon request from ISC, provide system logs, screenshots, diagnostic information and any other supplementary data required to support the investigation and resolution of API-related system issues.

5.6. All complaints received by the Approved Software Vendor in respect of the approved software must be logged, and a copy of such complaints log forwarded to ISC quarterly, or as otherwise requested.

5.7. The Approved Software Vendor must have procedures to maintain required encryption protocols and security access when accessing any NLIS Confidential Information at all times while in transit or at rest.

6. Technical Documentation Requirements

6.1. The Approved Software Vendor must maintain comprehensive documentation covering integration patterns and best practices for the NLIS API System. Environment management procedures and deployment checklists must be documented and kept current. Security control implementation details must be fully documented with regular reviews and updates.

6.2. All encryption configurations must be documented with specific details of the implementation. Access control matrices must be maintained and regularly reviewed to ensure accuracy. Audit log formats must be clearly defined and retention procedures documented in line with compliance requirements.

7. Environment Management Requirements

7.1. Software vendors must maintain separate development, testing, and production environments for The Product API System. Each environment must have distinct access controls implemented and transition procedures between environments must be clearly documented and followed for all deployments. Test and production data must be clearly separated and managed according to their classification.

7.2. Software vendors must demonstrate appropriate use of sandbox environments for all testing activities. All new features and changes must be fully tested in the sandbox environment before proceeding to production deployment. Test scenarios must comprehensively cover both normal operations and error conditions, including edge cases. No testing activities are permitted to occur in production environments under any circumstances.

8. Service Account Requirements

8.1. Software vendors must implement comprehensive service account management controls. All service accounts must be configured following the principle of least privilege, with permissions limited to only those necessary for the required functionality. Access rights must be reviewed quarterly with documented evidence of these reviews maintained. Any permissions found to be unused or no longer required must be removed immediately.

8.2. Permission assignments for all service accounts must be clearly documented and maintained. Credential rotation must be automated and occur at minimum every 90 days. All credentials must be stored using industry best practices for secure storage. Access logging must be comprehensive and cover all service account activities. Automated monitoring of service account usage must be implemented to detect and alert on any unusual patterns or potential security concerns.

9. Definitions

9.1. Where commencing with a capital letter:

Application means the “NLIS production API application form” issued by ISC.

Approved Software Vendor means a commercial software provider who has entered into, and has a current NLIS API System Access Agreement with ISC.

Confidential Information means all confidential or other commercially valuable information of whatever description and in whatever form relating to ISC, its activities, business, products, processes, NLIS API or the NLIS System.

ISC means the Integrity Systems Company Limited ABN 34 134 745 038.

National Livestock Identification System is a nationally agreed system, managed by Integrity System Company Ltd (ISC), which enables secure electronic data transfer between approved parties using standardised interfaces**.**

NLIS API System Access Agreement means an agreement under which ISC grants to a commercial software provider the right to access and use the NLIS API to provide NLIS capability for their customers.

NLIS Operational User Guide and Terms of Use means the NLIS data and transaction permissions and the rules for using the NLIS Database.

Software Product means the software developed by the software provider that accesses the NLIS APIs.

Standard means this document which is the eNVD System standard issued by ISC.