A96 – CALA Policy on the use of Computers in Accredited Laboratories

Revision 1.5 – August 4, 2015

CALA

Laboratory Accreditation

TABLE OF CONTENTS

CALA POLICY ON THE USE OF COMPUTERS IN ACCREDITED LABORATORIES

1.0 BACKGROUND

Laboratories accredited by CALA to ISO/IEC 17025:2005 must show their continuing competence to produce technically valid results. This capability is supported, in part, in many laboratories, through the appropriate use of electronic systems (computers and software - information technologies-IT) that:

- Support the collection of data;
- Support the manipulation and reduction of data;
- Support the storage, retrieval, amendment, archiving and transmission of data, documents and records; and,
- Support the development of quality system documents and records

CALA provides this general guidance and appropriate methods for accredited laboratories to:

- Ensure the continuing integrity of their electronic data, documents and records;
- Ensure the continuing validation of their software;
- Ensure the continuing confidentiality of their electronic information;
- Ensure adequate control and tracking for the amendment of their electronic documents, data, and records; and,
- Ensure the continuing retrieval of their electronic data, documents and records

This CALA Policy documents the requirements for accredited laboratories to maintain accreditation to ISO/IEC 17025:2005, with regard to the implementation and use of electronic systems in support of all laboratory operations.

2.0 POLICY STATEMENTS

- *Accredited laboratories shall have appropriate controls and procedures in place for the collection, storage, manipulation, reduction and transmission of electronic data and results.*

- *Accredited laboratories shall have appropriate controls and procedures in place for the development, approval, storage, retrieval, access and archiving of electronic documents and* records.

- Accredited laboratories shall develop, document and implement procedures to formally document the validation of all software and information technology solutions employed to support laboratory operations

- Accredited laboratories shall implement controls and procedures dealing with electronic systems that support laboratory operations so that these systems meet the requirements given in ISO/IEC 17025:2005 for paper-based documents, records, data and results.

3.0 SPECIFIC REQUIREMENTS

The following are the areas that would normally be addressed by electronic system policies and procedures in use at accredited laboratories:

- Integrity and control of electronic data;
- Validation of information technology solutions, including software and applications;
- Confidentiality/security of information – access control;
- Retrieval of electronic data, documents and records; and,
- Maintenance of electronic systems

The clauses in ISO/IEC 17025:2005 that may be cited to address the use of electronic systems used in accredited laboratories are given in Appendix 1 to this Policy.

3.1 Integrity and Control of Electronic Data, Documents and Records

The integrity and control of electronic data, documents and records may depend on the measures taken for their protection from inadvertent or unauthorized amendment and of their direct correlation to original data, documents, records and observations.

3.1.1 Policy Statement

Accredited laboratories shall develop and implement procedures to prevent the inadvertent and/or unauthorized amendment of computer software, electronic records, documents and data. The procedures shall stipulate the steps to be taken to formally amend computer software, electronic data, documents, and records. [4.3, 4.13]

3.1.2 Common Approaches

- Controlled access to software, electronic records, documents and data.
- Create multiple roles that read-only or read-write.
- Specify the persons who are normally granted access.
- Use of user ID and/or passwords.
- Use of read-only storage media.
- Clear and simple procedures to modify software, documents, records and data that provide the tracking information for amendments, which normally includes the identity

of person amending, date and time of amendment, identity of person approving amendment (if applicable), date and time of approval include the reason(s) for change.

- Back ups of current versions, so as to allow restoration to current condition, if current storage media discontinues normal retrieval access.
- Consider migration of data to new media types during the record retention period.

3.2 Validation of Electronic Systems

The validation of computer-based applications is the result of measures taken to validate the ability of the applications to perform as specified. Specifications can vary from simple word-processing applications to complex algorithms in dedicated measurement applications, such as Coordinate Measuring Machines (CMM). The Note in Clause 5.4.7.2 of ISO/IEC 17025:2005, indicating that validation of commercial off-the-shelf software does not apply to computing applications that are used to collect, manipulate or reduce data. For these types of applications, Clause 5.5.2 governs, because the application is considered to be a piece of measurement equipment, whether or not it was purchased from a commercial vendor.

3.2.1 Policy Statement

Accredited laboratories shall develop and implement procedures to formally document the validation of computer systems (software and applications) in support of laboratory operations. Such validation shall be commensurate with each type of computer-based solution used in the laboratory and its intended purpose and scope. [5.4, 5.5]

3.2.2 Common Approaches

- Determine the level of validation required for the electronic system (hardware, firmware, or software, or parts of all of them) from its classification as either Commercial, Commercial-user-modified, User-developed.
- Document the validation process used. See Figure 3 of *Software Validation in Accredited Laboratories (reference 1).*
- Monitor the continuing validation of the electronic system throughout its life cycle in the laboratory. See Figure 1 of "*Software Validation in Accredited Laboratories.*"
- ASTM E2066 Standard Guide for Validation of Laboratory Information Management Systems
- EPA 2185 Good Automated Laboratory Practices (http://nepis.epa.gov, publication no. EPA-220-B-95-006)

3.3 Confidentiality/Security of information – Access Control

The security of software and electronic information, regardless of its configuration as data, records or documents, is the result of measures taken to protect it from unauthorized access, viewing and dissemination.

3.3.1 Policy Statement

Accredited laboratories shall develop and implement procedures to provide adequate protection for software, electronic records, documents and data in order to prevent access and viewing by unauthorized persons. Such protection shall be commensurate with each type of record, document or observation/data point collected, stored, or maintained by the laboratory. [4.3, 4.13, 5.4, 5.5]

3.3.2 Common Approaches

- Controlled access to software, electronic records, documents and data.
- Specify the persons who are normally granted access.
- Use of passwords or digital signatures.
- Tracking of access to software, electronic records, documents and data.
- Use of increased levels of security, such as Public Key Infrastructure (PKI), or other types of encryption, in the transmission and receipt of electronic records, documents and data.
- Use of firewalls to control external access.
- Assurance that electronic-signatures are permanently linked to specific instances of data.

3.4 Retrieval of Electronic Data, Documents and Records

The retrieval of electronic data, records or documents, is a continuing measure of its availability, both during and after its use within the laboratory.

3.4.1 Policy Statement

Accredited laboratories shall develop and implement procedures to provide adequate facility for the continuing retrieval of electronic records, documents and data in order to permit access and reference to such records, documents and procedures for as long as the laboratory may require such access and reference. [4.3, 4.13]

3.4.2 Common Approaches

- Off-site storage.
- Use of formats that are likely to be used in the future such as Adobe Acrobat (*.pdf) format or XML format or ASCII format.
- Use of media that are likely to be used in the future such as CD-ROM, DVD ROM, memory cards and USB drives.
- Ensure migration of data when it needs to be transferred to new media.
- Use of an appropriate method of indexing archived data to facilitate ease of retrieval.

3.5 Maintenance of Electronic Systems (Computers/Software)

The maintenance of electronic systems (software and applications) in a laboratory is a measure of the ability of the laboratory to monitor the performance of all of the components of the electronic system and effect preventive and corrective actions on their use.

3.5.1 Policy Statement

Accredited laboratories shall develop and implement procedures to effect the maintenance of electronic systems (software and applications), which may include software, firmware and/or hardware, so as to prevent non-conforming operation of the electronic system. [5.5]

3.5.2 Common Approaches

- Operation by trained and qualified personnel.
- Preventive maintenance schedules for hardware.
- See reference 1 below by Gregory D. Gogates, *Software Validation in Accredited Laboratories,* 27 Sep 2001.
- Document the validation process used.
- Monitor the continuing validation of the electronic system throughout its life cycle in the laboratory.
- Inclusion of electronic systems within laboratory calibration program, as required.
- Identification of triggers to re-validate that define when re-validation needs to occur and the level of detail required.

3.6 References

1. ISO/IEC 17025:2005, General requirements for the competency of testing and calibration laboratories.
2. Gregory D. Gogates, *Software Validation in Accredited Laboratories,* 27 Sep 2001, http://www.a2la.org/guidance/adequate_for_use.pdf
3. Marianne Swanson, National Institute of Standards and Technology (NIST), *Security Self-Assessment Guide for Information Technology Systems*, NIST Special Publication 800-26, US Government Printing Office, Washington, August 2001, pp. 98. *Note: NIST SP 800-26 is superseded by NIST SP 800-53 (revision 4) and the NIST SP 800 53A (Revision 1). http://csrc.nist.gov/publications/PubsSPs.html*
4. ASTM E2066 Standard Guide for Validation of Laboratory Information Management Systems
5. EPA 2185 Good Automated Laboratory Practices (http://nepis.epa.gov, publication no. EPA-220-B-95-006), 1995.

4.0 APPENDIX 1 – COMMON REFERENCES WITHIN ISO/IEC 17025:2005 THAT APPLY TO THE USE OF ELECTRONIC SYSTEMS IN AN ACCREDITED LABORATORY. THIS APPENDIX FORMS PART OF THIS POLICY

Clause	Extract / Wording	Policy Consideration
4.1.5.c	*"…shall have policies and procedures to ensure the protection of its clients' confidential information and proprietary rights, including procedures for protecting the electronic storage and transmission of results…"*	**Integrity of data and Access control** Procedures exist to protect client's information
4.3.1	*"…shall establish and maintain procedures to control all documents…. ….. in this context, "document" could be … …. software…. These may be on various media, whether hard copy or electronic, ….."*	**Integrity of data and Access control** Procedures to control software
4.3.2.1	*"All documents issued… ….shall be… …reviewed and approved for use…."*	**Integrity of data** Quality system reviewed and approved by authorized personnel by electronic signatures or password protection and/or retention of approval records in hard copy.
4.3.2.2	*"The procedure(s) adopted shall ensure that: a) authorized editions of appropriate documents are available at all locations….."*	**Integrity of data and Retrieval of data** Authorized editions of appropriate documents all locations. (Intranet, NT file Share)
4.3.3.2	*"..the altered or new text shall be identified…"*	**Integrity of data** Altered or new text shall be identified (electronic document)
4.3.3.4	*"Procedures shall be established….. …documents maintained in computerized systems are made and controlled".*	**Integrity of data** Procedures shall describe how changes in documents, including software are controlled.
4.13.1.2	*"All records… …shall be… …readily retrievable…" "…hard copy or electronic media…"*	**Retrieval of data** Records (electronic media) shall be stored and maintained so that they are retrievable
4.13.1.4	*"The laboratory shall have procedures to protect and back-up records stored electronically and to prevent unauthorized access to or amendment of these records."*	**Integrity of data and Access control** Procedures to protect and back-up electronic records.

Clause	Extract / Wording	Policy Consideration
4.13.2.1	*"…shall retain records… …to establish an audit trail…"*	**Integrity of data and Retrieval of data** Retain records for the retention period (old versions of software also)
4.13.2.2	*"Observations, data and calculations shall be recorded…"*	**Integrity of data** Observations shall be recorded at the time they are made. (electronic).
4.13.2.3	*"When mistakes occur in records,……….In the case of records stored electronically, equivalent measures shall be taken to avoid loss or change of original data".*	**Integrity of data and Access control** Electronic records shall avoid loss to original data (audit trails) Do Databases and spreadsheets include "audit trails" to not allow previously recorded data to be obscured?
5.2.1	*"The laboratory management shall ensure the competence of all who operate specific….."*	**Validation and Maintenance of electronic system** Does evidence show that personnel involved in use of Custom Software have adequate training? If the Custom Software was developed in-house, is there evidence that they have adequate training in the development of these types of solutions?
5.3.4	*Access to and use of areas affecting… …quality… …shall be controlled.*	**Integrity of data and Access control** Server rooms or server access should have limited access
5.4.1	*"The laboratory shall have instructions on the use and operation of equipment…."*	**Integrity of data Validation and Maintenance of electronic system** This includes software. Do adequate instructions exist for the operation & maintenance of the software?
5.4.7.1	*"Calculations and data transfers shall be subject to appropriate checks in a systematic manner."*	**Integrity of data and Validation of Electronic system** Calculations (spreadsheet) and data transfers (tables) shall be subject to checks. Where other programming approaches are used to effect data manipulation and transfer, there must be some method established to ensure that these are checked as well.
5.4.7.2 a)	*"computer software developed by the user is documented in sufficient detail and suitably validated ….."*	**Validation of Electronic system** Software shall be validated and documented – even if commercial software is configured for specific use
5.4.7.2 b)	*"procedures are established for protecting data, such procedures shall include integrity, confidentiality…"*	**Integrity of data and Access control** Procedures are established to protect data
5.4.7.2 c)	*"computers and automated equipment are maintained…"*	**Integrity of data and Maintenance of Electronic system** Computer and automated equipment are maintained

Clause	Extract / Wording	Policy Consideration
5.4.7.2 Note	*“Commercial off-the-shelf software… …in general use, within their design application range, may be considered suitably validated. However, software configuration/ modifications should be validated as in 5.4.7.2 a)”*	**Validation of Electronic system** The software validation note allows labs to take credit for assumed validation efforts made by the manufacturer of purchased software but requires that individual spreadsheets, macros, and all configuration / modifications / setups be validated. This does not apply to electronic systems used to acquire, manipulate or reduce data, such as hard-coded *firmware*[⊕] that is often supplied with computer-driven devices.
5.5.2	*“Equipment, and its software…….shall be capable of achieving the accuracy required……. Before being placed in service, equipment (software) shall be calibrated or checked to establish that it meets the labs requirements·…….”*	**Validation and Maintenance of Electronic system** Does the accuracy of the Firmware/Software meet or exceed the accuracy required by the test method or other relevant specification? A good test is the uncertainty contribution of the device (and its programming) to the overall uncertainty of the test result. All deployed software should be verified prior to being placed in service by performing some user acceptance testing such as a comparison of the requirements against features. This includes placement into service following a move or after being shipped back from calibration or maintenance.
5.5.4	*“Each item of equipment and its software used for testing… …shall… …be uniquely identified.”*	**Maintenance of Electronic system** Each item of equipment & software shall be uniquely identified. Procedures should include documenting the versions in use (version control)
5.5.5	*“Records shall be maintained…”*	**Maintenance of Electronic system** Records shall be maintained of equipment & software.
5.5.11	*“Where calibrations give rise to… …correction factors… …procedures to ensure that copies (e.g. in computer software) are correctly updated.”*	**Validation of Electronic system** Does evidence exist confirming correct software deployment at each target installation? Consider the same approach to software as for other documents such as document control (software management), distribution control.

[⊕] Firmware is programming that is inserted into programmable read-only memory (programmable ROM), thus becoming a permanent part of a computing device. Firmware is created and tested like software (using microcode simulation). When ready, it can be distributed like other software and, using a special user interface, installed in the programmable read-only memory by the user. Firmware is sometimes distributed for printers, modems, and other devices controlled by computers.

Clause	Extract / Wording	Policy Consideration
5.5.12	*Test and Calibration equipment, including software, shall be safeguarded from adjustments…"*	**Integrity of data and Maintenance of Electronic system** Software shall be safeguarded from adjustments such as password protection on spreadsheets or other files.
5.10.1 NOTE 2	*"The test reports or calibration certificates may be… ….by electronic data transfer…"*	**Integrity of data** Reports may be issued electronically
5.10.2.j	*"the… …identification of person(s) authorizing the test report or calibration certificate."*	**Integrity of data** Reports may contain electronic signatures. LIMS systems should have established authorization protocols.
5.10.7	*"in the case of transmission of test or calibration results by… …electronic… …means, the requirements of this International Standard shall be met…"*	**Integrity of data** Reports may be transmitted electronically. Whatever method of transmission is used, it must provide an the same level of protection of integrity of information afforded to paper documentation.