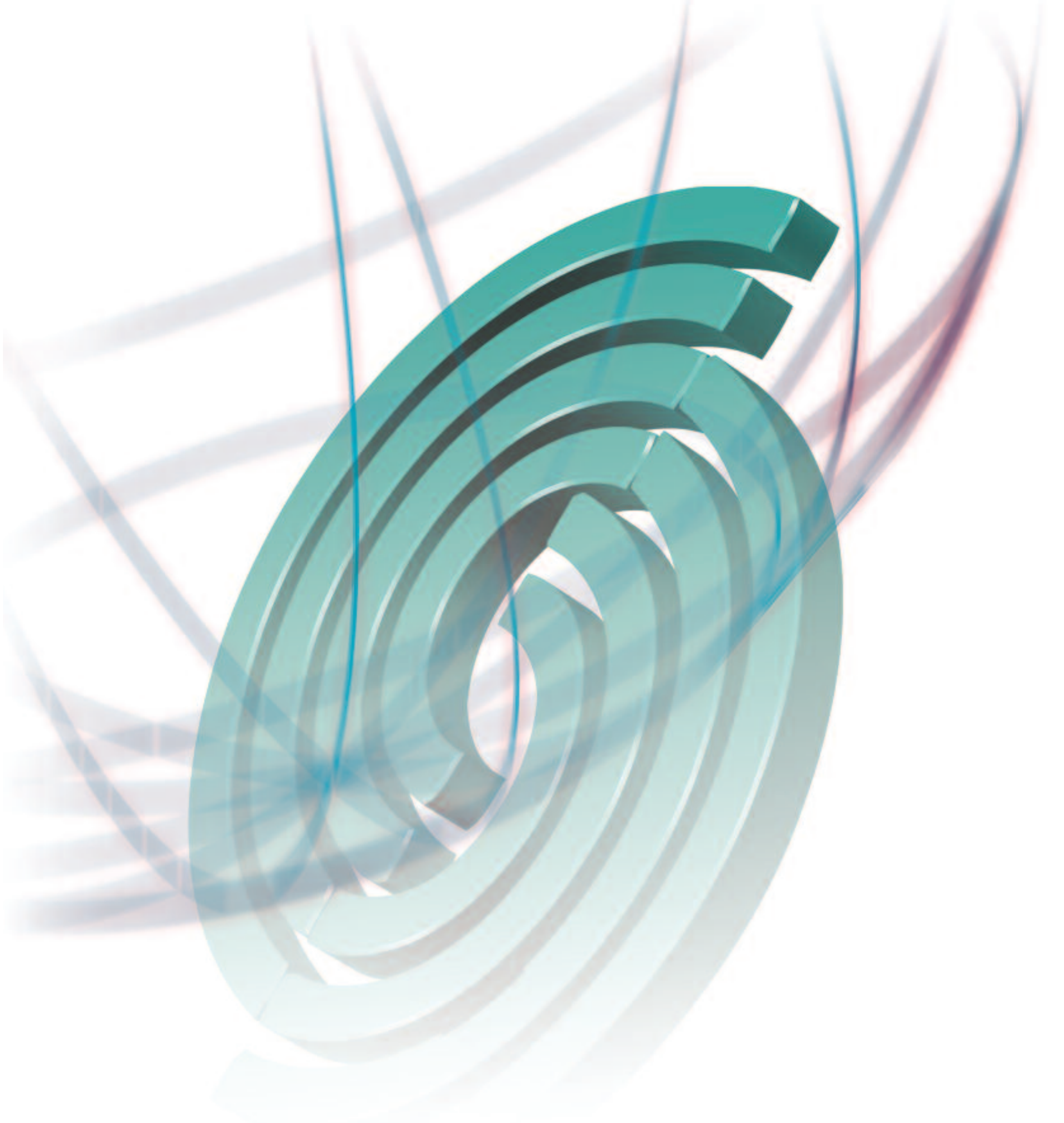
Standards Council of Canada
Conseil canadien des normes



PALCAN Policy on the Use of Information Technology in Accredited Laboratories

CAN-P-1628
November 2006

Canada

PALCAN
POLICY ON THE USE OF INFORMATION TECHNOLOGY IN ACCREDITED LABORATORIES

POLITIQUE DU PALCAN CONCERNANT L'UTILISATION DES TECHNOLOGIES DE L'INFORMATION DANS LES LABORATOIRES ACCRÉDITÉS

CAN-P-1628
November 2006

Standards Council of Canada
270 Albert Street, Suite 200
Ottawa, Ontario
K1P 6N7
Canada
Tel.: (613) 238-3222
Fax.: (613) 569-7808
Email: info@scc.ca
Website: www.scc.ca

NOTE : A French version of this document is available from the:

Standards Council of Canada
270 Albert Street, Suite 200,
OTTAWA, Ontario
K1P 6N7
Tel.: (613) 238-3222
Fax.: (613) 569-7808
Email: info.palcan@scc.ca
Website: www.ccn.ca

NOTE : On peut obtenir un exemplaire français de ce document en écrivant au :

Conseil canadien des normes
270 rue Albert, bureau 200
OTTAWA (Ontario)
K1P 6N7
Tél.: (613) 238-3222
Fax.: (613) 569-7808
Courriel: info.palcan@scc.ca
Site web: www.ccn.ca

TABLE OF CONTENTS

FOREWORD

The Standards Council of Canada ("SCC" or "the Council") is a crown corporation established by an Act of Parliament in 1970, amended in 1996, to foster and promote efficient and effective voluntary standardization in Canada. It is independent of government in its policies and operations, although it is financed partially by Parliamentary appropriation. The Council consists of members from government and the private sectors.

The mandate of the Council is to promote the participation of Canadians in voluntary standards activities, promote public-private sector cooperation in relation to voluntary standardization in Canada, coordinate and oversee the efforts of the persons and organizations involved in the National Standards System, foster quality, performance and technological innovation in Canadian goods and services through standards-related activities, and develop standards-related strategies and long-term objectives.

In essence, the Council promotes efficient and effective voluntary standardization in Canada in order to advance the national economy, support sustainable development, benefit the health, safety and welfare of workers and the public, assist and protect consumers, facilitate domestic and international trade and further international cooperation in relation to standardization.

In addition, the Council serves as the government's focal point for voluntary standardization and represents Canada in international standardization activities, sets out policies and procedures for the development of National Standards of Canada, and for the accreditation of standards development organizations, of product certification bodies, of testing and calibration laboratories, of quality and environmental management systems registration bodies and of quality management systems and environmental auditor certifiers and training course providers, and promotes and supports the principle of recognition of accreditation or equivalent systems as a means of decreasing the number of multiple assessments and audits, both in Canada and with Canada's trading partners.

This document is one of several issued by the Standards Council of Canada to define the policies, plans, and procedures established by the Council to help achieve its mandate.

Requests for clarification and recommendations for amendment of this document, or requests for additional copies should be addressed to the publisher directly at info.palcan@scc.ca .

BACKGROUND

1. Laboratories accredited within the PALCAN program to CAN-P-4E (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 information technologies (IT) that:

a. Support the collection of data;
b. Support the manipulation and reduction of data;
c. Support the storage, retrieval, amendment, archiving and transmission of data, documents and records; and
d. Support the development of quality system documents and records.

2. General guidance is required on acceptable and appropriate methods for accredited laboratories to:

a. Ensure the continuing integrity of their electronic data, documents and records;
b. Ensure the continuing validation of their software;
c. Ensure the continuing confidentiality of their electronic information;
d. Ensure adequate control and tracking for the amendment of their electronic documents, data, and records; and
e. Ensure the continuing retrieval of their electronic data, documents and records.

3. This PALCAN Policy documents the requirements for accredited laboratories to maintain accreditation to CAN-P-4E, with regard to the implementation and use of IT in support of all laboratory operations.

POLICY STATEMENTS

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

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

3. Accredited laboratories shall implement controls and procedures dealing with information technology support to laboratory operations that meet the requirements given in CAN-P-4E for paper-based documents, records, data and results.

4. 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.

SPECIFIC REQUIREMENTS

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

a. Integrity and control of electronic data;
b. Validation of information technology solutions;
c. Confidentiality/security of information – access control;
d. Retrieval of electronic data, documents and records;
e. Maintenance of IT solutions.

2. The clauses in CAN-P-4E that may be cited to address the use of IT solutions in accredited laboratories are given in Appendix 1 to this Policy.

INTEGRITY AND CONTROL OF ELECTRONIC DATA, DOCUMENTS AND RECORDS

1. The integrity and control of electronic data, documents and records are a measure of their protection from inadvertent or unauthorized amendment and of their direct correlation to original data, documents, records and observations.

Policy Statement

Accredited laboratories shall develop and implement procedures to prevent the inadvertent and/or unauthorized amendment of electronic records, documents and data. The procedure shall stipulate the steps to be taken to formally amend electronic data, documents, and records. [CAN-P-4E, clauses 4.3, 4.13]

Common Approaches

- Controlled access to electronic records, documents and data.
- Specify the persons granted access and modification/amendment rights
- Use of passwords.
- Use of read-only storage media.
- Clear and simple procedures to modify 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.
- Back ups of current versions, so as to allow restoration to current condition, if current storage media discontinues normal retrieval access.

VALIDATION OF IT SOLUTIONS

1. The validation of IT applications is a continuing measure of the ability of the application 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).

Policy Statement

Accredited laboratories shall develop and implement procedures to formally document the validation of IT solutions in support of laboratory operations. Such validation shall be commensurate with each type of IT solution used in the laboratory and its scope. [CAN-P-4E, clauses 5.4, 5.5]

NOTE: In general, the degree of rigor for the validation relates to the level of risk for the initial records that form part of the auditable trail. The impact of the retention period of these records also needs to be considered.

Common Approaches

- See paper by Gregory D. Gogates, A2LA Assessor, member EA ad-hoc group on the use of computers, "*Software Validation in Accredited Laboratories,*" 27 Sep 2001.
- Determine the level of validation required for the IT solution (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*".
- Monitor the continuing validation of the IT solution throughout its life cycle in the laboratory. See Figure 1 of "*Software Validation in Accredited Laboratories*".

CONFIDENTIALITY/SECURITY OF INFORMATION – ACCESS CONTROL

1. The security of electronic information, regardless of its configuration as data, records or documents, is a continuing measure of its protection from unauthorized access.

Policy Statement

Accredited laboratories shall develop and implement procedures to provide adequate protection for electronic records, documents and data in order to prevent access, modification 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. [CAN-P-4E, clauses 4.3, 4.13, 5.4, 5.5]

Common Approaches

- Controlled access to electronic records, documents and data.
- Specify the persons granted access and modification/amendment rights.
- Use of passwords or “digital signatures.”
- Tracking of access to 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.

RETRIEVAL OF ELECTRONIC DATA, DOCUMENTS AND RECORDS

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

Policy Statement

Accredited laboratories shall develop and implement procedures to provide adequate secure and control facility for the continuing retrieval of electronic records, documents and data in order to permit access, modification and reference to such records, documents and procedures for as long as the laboratory may require such access and reference. [CAN-P-4E, clauses 4.3, 4.13]

Common Approaches

- Secure and controlled off-site storage.
- Use of formats that are likely to be used in the future such as Adobe Acrobat (*.pdf) format.
- Use of media, such as CD-ROM and DVD-ROM, that are likely to be used in the future.
- Use of an appropriate method of indexing archived data to facilitate ease of retrieval.

NOTE: When electronic data is retained for more than five to seven years the laboratories must consider the need for procedures to warehouse/convert the data in order to ensure the integrity and retrievability of the data for the specified retention period. Such procedures would normally include regular conversions, or at least verifications of the data for example, to confirm its retrievability and integrity.

MAINTENANCE OF IT SOLUTIONS

1. The maintenance of IT solutions in a laboratory is a measure of the ability of the laboratory to monitor the performance of IT solutions and effect preventive and corrective actions on their use.

Policy Statement

Accredited laboratories shall develop and implement procedures to effect the maintenance of IT solutions, which may include software, firmware and/or hardware, so as to prevent non-conforming operation of the IT solution. [CAN-P-4E, clause 5.5]

Common Approaches

- Operation by trained and qualified personnel.
- Preventive maintenance schedules for hardware.
- See paper by Gregory D. Gogates, A2LA Assessor, member EA ad-hoc group on the use of computers, "*Software Validation in Accredited Laboratories,"* 27 Sep 2001.
- Document the validation process used. See Figure 3 of "*Software Validation in Accredited Laboratories".*
- Monitor the continuing validation of the IT solution throughout its life cycle in the laboratory. See Figure 1 of "*Software Validation in Accredited Laboratories".*
- Inclusion of IT solutions within laboratory calibration program, as required.

LIST OF ATTACHMENTS

Appendix 1 – Common references within CAN-P-4E that apply to the use of IT solutions in an accredited laboratory

REFERENCES

Gregory D. Gogates, A2LA Assessor, member EA ad-hoc group on the use of computers, *Software Validation in Accredited Laboratories,* 27 Sep 2001, pp. 5. http://www.a2la.net/guidance/adequate_for_use.pdf

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.

APPENDIX 1

Common references within CAN-P-4E that apply to the use of IT Solutions in an accredited laboratory

NOTE: **Procedures** where required must specify a way to perform the activity and must usually contain the purpose and scope of the activity, what shall be done and by whom, when, where and how it shall be done. The procedure must also address what materials, equipment and documents shall be used and how it shall be controlled and recorded.

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 (electronic signatures).
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, Operating System (OS) file share rights).
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 that constitute the auditable trail for the specified 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 data to be obscured?.
5.2.1	"The laboratory management shall ensure the competence of all who operate specific….."	**Validation and Maintenance of IT solution** Does evidence exist showing that personnel involved in Custom Software development have adequate training?
5.4.1	"The laboratory shall have instructions on the use and operation of equipment…."	**Integrity of data Validation and Maintenance of IT solution** 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 IT solution** Calculations (spreadsheet) and data transfers (tables) shall be subject to checks.
5.4.7.2 a)	"computer software developed by the user is documented in sufficient detail and suitably validated ….."	**Validation of IT solution** Software shall be validated – even if commercial software that 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 IT solution** Computer and automated equipment are maintained.
5.4.7.2 NOTE 1	"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 IT solution** 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.

Clause	Extract / Wording	Policy Consideration
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 IT solution** Does the accuracy/resolution/ uncertainty of the Firmware/Software meet or exceed the accuracy required by the test method or other relevant specification?
5.5.4	"Each item of equipment and its software used for testing… …shall… …be uniquely identified."	**Maintenance of IT solution** Each item of equipment & software shall be uniquely identified.
5.5.5	"Records shall be maintained…"	**Maintenance of IT solution** 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 IT solution** Does evidence exist confirming correct software deployment at each target installation?
5.5.12	Test and Calibration equipment, including software, shall be safeguarded from adjustments…"	**Integrity of data and Maintenance of IT solution** Software shall be safeguarded from adjustments including imbedded formulas in spreadsheets, tables, etc..
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.
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.