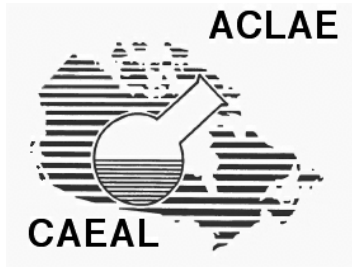


DRAFT PALCAN POLICY on the use of IT IN ACCREDITED LABS

J.E.J. (Ned) Gravel, P.Eng., NQI-LA
Manager, Quality and Training
CAEAL



SCC/CAEAL Accreditation Partnership



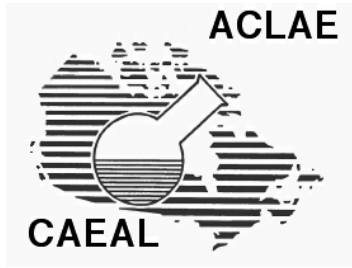
Outline



- Why do we need this policy?
- What does it need to do?
- What should it say?
- What should it contain?



SCC/CAEAL Accreditation Partnership



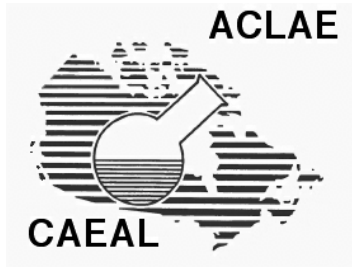
Usefulness of a Policy



- We have to understand what an IT solution can do...and what it cannot do
- It can support the collection of data
- It can support the manipulation and reduction of data
- It can support the storage, retrieval, amendment, archiving and transmission of data, documents and records
- It can support the development of QMS documents and records



SCC/CAEAL Accreditation Partnership



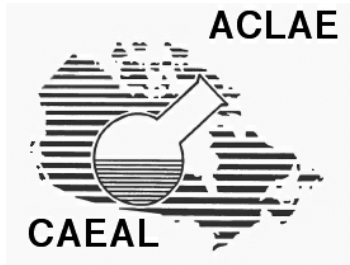
Usefulness of a Policy



- It cannot replace QA/QC in a laboratory.
- It cannot replace the human intervention in the production and approval of QMS documents
- It cannot authorise the release of test and calibration results
- It cannot guarantee error free manipulation and transmission of data.



SCC/CAEAL Accreditation Partnership

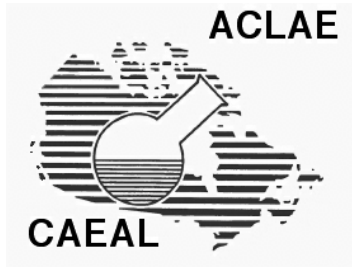


What it needs to say



- Continue to require integrity of laboratory documents, records and data
- Require the laboratory to validate their IT solutions
- Continue to require the laboratory to protect the confidentiality of their electronic information
- Continue to require the laboratory to track amendments and changes to electronic documents and records.
- Continue to require the laboratory to provide for ready retrieval of electronic records and documents.
- Require the laboratory to adequately maintain their IT solutions





DRAFT IT POLICY

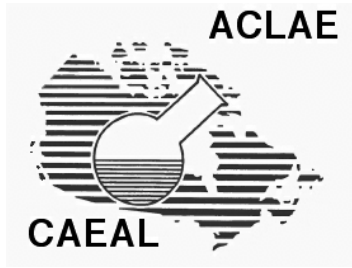


■ Control systems that support tests

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



SCC/CAEAL Accreditation Partnership



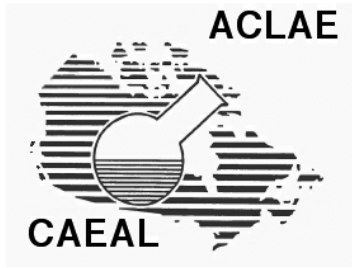
DRAFT IT POLICY



■ Control document support systems

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





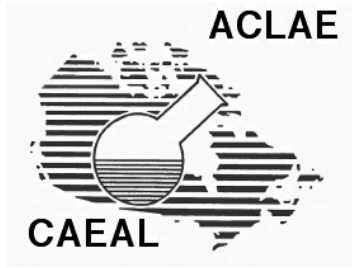
DRAFT IT POLICY



- **Same as for a paper-based system**

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



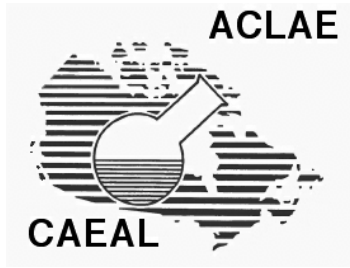


Data Integrity/Doc Control



- Protection from inadvertent or unauthorised modification and directly correlate to original observations/recordings.
- How?
 - Access control
 - Specify authorised users
 - Passwords and/or digital signatures
 - PKI or other confidence builder or encryption
 - Firewalls



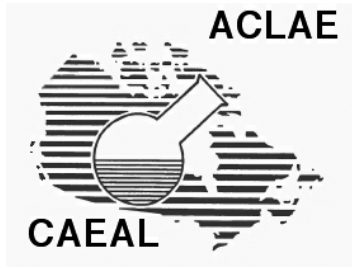


IT Solution Validation



- Formally documented validation of the solution (especially software)
- How?
 - Easy guide by Greg Gogates
 - Is it Commercial, Modified commercial, or User-developed?
 - Document the validation (compare to hand calcs if necessary)
 - Continuous monitoring - for as long as the IT solution is in use



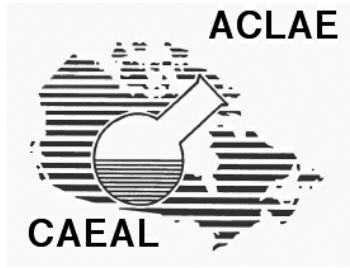


Confidentiality/Security



- Protect from unauthorised viewing/access.
- How?
 - Access control
 - Passwords and digital signatures
 - Specify persons having access
 - Track access
 - Use PKI or encryption
 - Use firewalls
 - (Threat assessment of a system - NIST checklist)





Data/Doc Retrieval



- Provide for retrieval during and after document/record/data point is no longer in use for as long as is necessary
- How?
 - Off-site storage
 - Future formats
 - Future media
 - Indexing





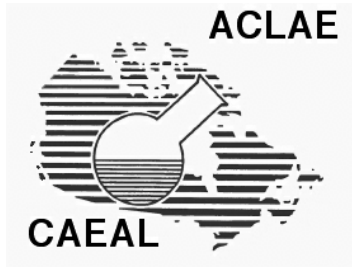
Maintenance of IT Solution



- Prevent non-conforming operation
- How?
 - Operation by qualified persons
 - Preventive maintenance schedules
 - Ongoing validation
 - Treat as other lab equipment (GC/MS etc)
 - Use lab calibration program



SCC/CAEAL Accreditation Partnership

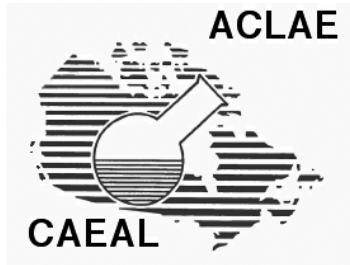


Appendix 1



- Compendium of references within CAN-P-4D that give the clearest direction for the specific requirements of such a policy.
- Correlation with the specific aspect of the policy, such as Validation, Access Control, Confidentiality etc.



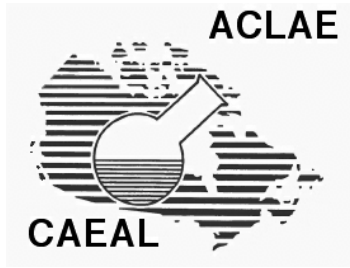


Attachment 1



- Paper written by Greg Gogates, and used with his permission, to walk lab through the process of developing software validation criteria
- Is basis for A2LA and EA backbone policies.
- Canadian policy not fully developed. When asked by EA/LC about the desirability of an overall policy, Canada replied:
 - “We do not know. We have security and legal metrology document on the topic”





Attachment 2



- The most thorough EIRA I have ever seen published outside of the intelligence community. Not for the faint-hearted.
- What most labs really need is to understand the “reasonable person” concept under law:
 - What are the steps that a reasonable person would make to protect the confidentiality of client information?

