Proposed Basic Coding Guidelines for Language Independent Standards Document

1. External input shall be validated for type, length, format, and range, known valid and safe data.

2. Compiler static analysis checking shall be enabled and any resultant security and safety issues shall be resolved.

3. The source code shall be run through a static source code analysis tool to detect security and safety anomalies and security anomalies shall be resolved.

4. Explicit bounds checking shall be performed at point of use when it cannot be shown statically that bounds will be obeyed, when bounds checking is not provided by the implementation, or if automatic bounds checking is disabled.

5. A strategy shall be specified and obeyed, by which dynamically allocated resources such as memory, files, tasks, threads or locks, are freed when no longer needed.

6. Error detection, error reporting, and error handling shall be implemented where errors could occur.

7. Non-deterministic constructs shall be verified for all permitted behaviours.

8. Constructs with side-effects shall not be part of enclosing expressions.

9. Sensitive data shall be sanitized, erased or encrypted to prevent it from being visible to others such as when it is in freed memory or in transmitted data.

10. Default passwords shall be required to be changed upon first use.

Additions possible:
More than top 10, maybe reuse almost all guidance from TR 24772-1 Clause 5.4

We need rules about how deviations to the rules above must be quantified, qualified and approved in the context of this standard.

Stephen Michell 2017-4-6 10:15 AM
Deleted: 5

Stephen Michell 2017-4-9 6:02 PM
Deleted: ... [1]

Stephen Michell 2017-4-9 6:03 PM
Formatted: Centered, Indent: First line: 0 cm

Stephen Michell 2017-4-9 6:03 PM
Formatted: Font:18 pt

Stephen Michell 2017-4-6 9:57 AM
Formatted: Font:10 pt

Stephen Michell 2017-4-6 10:19 AM
Deleted:

Stephen Michell 2017-4-6 9:57 AM
Formatted: Font:10 pt

Stephen Michell 2017-4-6 9:45 AM
Deleted: Dynamic memory, files, tasks and threads shall be allocated and freed at the same level of abstraction. ... [2]

Stephen Michell 2017-4-6 10:06 AM
Deleted: error correction

Stephen Michell 2017-4-6 10:06 AM
Deleted: ,

Stephen Michell 2017-4-6 10:03 AM
Deleted: and recovery

Stephen Michell 2017-4-6 10:08 AM
Deleted: at instances

Stephen Michell 2017-4-6 9:45 AM
Deleted: condition

Stephen Michell 2017-4-6 10:07 AM
Deleted: known possible

Stephen Michell 2017-4-6 10:14 AM
Deleted: Deprecated language features shall not be used. ... [3]

Stephen Michell 2017-4-6 10:11 AM
Formatted: Font:10 pt

Stephen Michell 2017-4-6 10:14 AM
Deleted: 10

Stephen Michell 2017-4-6 10:14 AM
Deleted: 1