ISO IEC JTC 1 SC 22 WG 23 N0705
4 April 2017

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 issues shall be resolved.

3. The source code shall be run through a static source code analysis tool to detect security 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. Dynamic memory, files, tasks and threads shall be allocated and freed at the same level of abstraction.

6. Error detection, error reporting, error correction, and recovery shall be implemented at instances where error conditions could occur.

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

8. Deprecated language features shall not be used.

9. Assignments shall be standalone expressions.

10. 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.

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