

## Green Pace Secure Development Policy

Contents

[Overview 2](#_bookmark0)

[Purpose 2](#_bookmark1)

[Scope 2](#_bookmark2)

[Module Three Milestone 2](#_bookmark3)

[Ten Core Security Principles 2](#_bookmark4)

[C/C++ Ten Coding Standards 3](#_bookmark5)

[Coding Standard 1 4](#_bookmark6)

[Coding Standard 2 5](#_bookmark7)

[Coding Standard 3 6](#_bookmark8)

[Coding Standard 4 7](#_bookmark9)

[Coding Standard 5 8](#_bookmark10)

[Coding Standard 6 9](#_bookmark11)

[Coding Standard 7 10](#_bookmark12)

[Coding Standard 8 11](#_bookmark13)

[Coding Standard 9 13](#_bookmark14)

[Coding Standard 10 14](#_bookmark15)

[Defense-in-Depth Illustration 15](#_bookmark16)

[Project One 15](#_bookmark17)

1. [Revise the C/C++ Standards 15](#_bookmark18)
2. [Risk Assessment 15](#_bookmark19)
3. [Automated Detection 15](#_bookmark20)
4. [Automation 15](#_bookmark21)
5. [Summary of Risk Assessments 16](#_bookmark22)
6. [Create Policies for Encryption and Triple A 16](#_bookmark23)
7. [Map the Principles 17](#_bookmark24)

[Audit Controls and Management 18](#_bookmark25)

[Enforcement 18](#_bookmark26)

[Exceptions Process 18](#_bookmark27)

[Distribution 19](#_bookmark28)

[Policy Change Control 19](#_bookmark29)

[Policy Version History 19](#_bookmark30)

[Appendix A Lookups 19](#_bookmark31)

[Approved C/C++ Language Acronyms 19](#_bookmark32)

# Overview

Software development at Green Pace requires consistent implementation of secure principles to all developed applications. Consistent approaches and methodologies must be maintained through all policies that are uniformly defined, implemented, governed, and maintained over time.

# Purpose

This policy defines the core security principles; C/C++ coding standards; authorization, authentication, and auditing standards; and data encryption standards. This article explains the differences between policy, standards, principles, and practices (guidelines and procedure): [Understanding the Hierarchy of Principles,](https://www.linkedin.com/pulse/understanding-hierarchy-principles-policies-standards-wally-beddoe/) [Policies, Standards, Procedures, and Guidelines](https://www.linkedin.com/pulse/understanding-hierarchy-principles-policies-standards-wally-beddoe/).

# Scope

This document applies to all staff that create, deploy, or support custom software at Green Pace.

# Module Three Milestone

## Ten Core Security Principles

|  |  |
| --- | --- |
| **Principles** | Write a short paragraph explaining each of the 10 principles of security. |
| **1.** Validate Input Data | Validating all inputs from untrusted data sources, This can help prevent many of the major software vulnerabilities. Always be aware of external data sources as cause for concern such as command line arguments, environmental variables and network interfaces. |
| **2.** Heed Compiler Warnings | Always use highest warning levels available when compiling your code and eliminate warnings by modifying the code. To help detect and eliminate additional security flaws, use static and dynamic analysis tools. |
| **3.** Architect and Design for Security Policies | Be mindful to make sure that when designing your software architecture that you implement and enforce the proper security policies. |
| **4.** Keep It Simple | Keep you coding design small and simple to avoid having to cater to complex systems which are more susceptible to errors and failed security mechanisms. |
| **5.** Default Deny | Standardize your access decisions based on permission rather than exclusion. By default access should denied with specific conditions to permit access. |
| **6.** Adhere to the Principle of Least Privilege | Process executions should have the least set of privileges to complete the job. Elevated permissions should only be accessed for the time it takes to complete the task. This is to help reduce the chances of attackers use of arbitrary code within those elevated privileges. |
| **7.** Sanitize Data Sent to Other Systems | Sanitize the data passed through complex subsystems. To dissuade attackers from using injection attacks to manipulate the components of subsystems. |
| **8.** Practice Defense in Depth | Always practice defense in depth with multiple layers of security. So when one layer fails there are other layer there to help prevent security flaws from becoming |

|  |  |
| --- | --- |
| **Principles** | Write a short paragraph explaining each of the 10 principles of security. |
|  | exploitable vulnerabilities. |
| **9.** Use Effective Quality Assurance Techniques | Quality assurance techniques can increase chances of identifying and eliminating vulnerabilities. Using multiple testing phases, independent security reviews and external security reviews can all lead to more secure systems. |
| **10.** Adopt a Secure Coding Standard | Always have a secure coding standard for development in whatever language and platform you are using. |

## C/C++ Ten Coding Standards

Complete the coding standards portion of the template according to the Module Three milestone requirements. In Project One, follow the instructions to add a layer of security to the existing coding standards. Please start each standard on a new page, as they may take up more than one page. The first seven coding standards are labeled by category. The last three are blank so you may choose three additional standards. Be sure to label them by category and give them a sequential number for that category. Add compliant and noncompliant sections as needed to each coding standard.

## Coding Standard 1

|  |  |  |
| --- | --- | --- |
| **Coding Standard** | **Label** | **Name of Standard** |
| **Data Type** | [STD-001- CPP] | Do not cast to an out-of-range enumeration value |

**Noncompliant Code**

enum EnumType { First, Second,

Third

};

void f(**int** intVar) {

EnumType enumVar = static\_cast<EnumType>(intVar);

if (enumVar < First || enumVar > Third) {

// Handle error

}

}

Checks whether a given value is within range of acceptable enumeration values. After casting the type it might not be able to represent the given integer value.

**Compliant Code**

enum EnumType { First, Second,

Third

};

void f(**int** intVar) {

if (intVar < First || intVar > Third) {

// Handle error

}

EnumType enumVar = static\_cast<EnumType>(intVar);

}

The compliant solution checks the value represented by the enumeration type before performing the conversion to guarantee the conversion doesn’t result in an unspecified value. In turn is restricts the converted value to one specific enumerator type.

**Note: Stop here for the milestone. Complete this section for Project One in Module Six.**

**Principles(s):** It is possible for unspecified values to result in a buffer overflow, leading to the execution of arbitrary code by an attacker. However, because enumerators are rarely used for indexing into arrays or other forms of pointer arithmetic, it is more likely that this scenario will result in data integrity violations rather than arbitrary code execution.

**Threat Level**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Severity** | **Likelihood** | **Remediation Cost** | **Priority** | **Level** |
| Medium | Unlikely | Medium | P4 | L3 |

**Automation**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
| Axivion  Bauhaus Suite | 6.9.0 | CertC++ - INT50 |  |
| Helix QAC | 2021.1 |  |  |
| Parasoft C/C++ test | 2020.2 | CERT\_CPP – INT50-a | An expression with enum underlying type shall only have values corresponding to the enumerators of the  enumeration |
| PRQA QA- C++ | 4.4 | 3013 |  |
| PVS – Studio | 7.07 | V1016 |  |

## Coding Standard 2

|  |  |  |
| --- | --- | --- |
| **Coding Standard** | **Label** | **Name of Standard** |
| **Data Value** | [STD-002- CPP] | Use valid references, pointers, and iterators to reference elements of a container |

**Noncompliant Code**

#include <deque>

void f(const double \*items, std::size\_t count) { std::deque<double> d;

auto pos = d.begin();

for (std::size\_t i = 0; i < count; ++i, ++pos) { d.insert(pos, items[i] + 41.0);

}

}

In this noncompliant code example, pos is invalidated after the first call to insert(), and subsequent loop iterations have undefined behavior.

#include <deque>

void f(const double \*items, std::size\_t count) { std::deque<double> d;

auto pos = d.begin();

for (std::size\_t i = 0; i < count; ++i, ++pos) { pos = d.insert(pos, items[i] + 41.0);

}

}

In this compliant solution, pos is assigned a valid iterator on each insertion, preventing undefined behavior.

**Compliant Code**

**Note: Stop here for the milestone. Complete this section for Project One in Module Six.**

**Principles(s):** Using invalid references, pointers, or iterators to reference elements of a container results in undefined behavior.

**Threat Level**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Severity** | **Likelihood** | **Remediation Cost** | **Priority** | **Level** |
| High | Probable | High | P6 | L2 |

**Automation**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
| Astree | 20.10 | Overflow\_unpon\_dereference |  |
| Helix QAC | 2021.1 |  |  |
| Parasoft C/C++  test | 2020.2 | CERT\_CPP-CTR51-a | Do not modify container while  iterating over it |
| PVS – Studio | 7.07 | V783 |  |

## Coding Standard 3

|  |  |  |
| --- | --- | --- |
| **Coding Standard** | **Label** | **Name of Standard** |
| **String Correctness** | [STD-003- CPP] | Do not attempt to create a std::string from a null pointer |

**Noncompliant Code**

#include <cstdlib> #include <string>

void f() {

std::string tmp(std::getenv("TMP")); if (!tmp.empty()) {

// ...

}

}

In this noncompliant code example, a std::string object is created from the results of a call to std::getenv(). However, because std::getenv() returns a null pointer on failure, this code can lead to undefined behavior when the environment variable does not exist (or some other error occurs).

**Compliant Code**

#include <cstdlib> #include <string>

void f() {

const char \*tmpPtrVal = std::getenv("TMP"); std::string tmp(tmpPtrVal ? tmpPtrVal : ""); if (!tmp.empty()) {

// ...

}

}

In this compliant solution, the results from the call to std::getenv() are checked for null before the std::string object is constructed.

**Note: Stop here for the milestone. Complete this section for Project One in Module Six.**

**Principles(s):** Dereferencing a null pointer is undefined behavior, typically abnormal program termination. In some situations, however, dereferencing a null pointer can lead to the execution of arbitrary code [Jack 2007, van Sprundel 2006]. The indicated severity is for this more severe case; on platforms where it is not possible to exploit a null pointer dereference to execute arbitrary code, the actual severity is low.

**Threat Level**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Severity** | **Likelihood** | **Remediation Cost** | **Priority** | **Level** |
| High | Likely | Medium | P18 | L1 |

**Automation**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
| Astree | 20.10 | Assert\_failure |  |
| Helix QAC | 2021.1 |  |  |
| ParasoftC/C++  test | 2020.2 | CERT\_CPP-STR51-a | Avoid null pointer dereferencing |

## Coding Standard 4

|  |  |  |
| --- | --- | --- |
| **Coding Standard** | **Label** | **Name of Standard** |
| **SQL Injection** | [STD-004- CPP] | Do not store already-owned pointer value in an unrelated smart pointer |

#include <memory>

void f() {

int \*i = new int; std::shared\_ptr<int> p1(i); std::shared\_ptr<int> p2(i);

}

In this noncompliant code example, two unrelated smart pointers are constructed from the same underlying pointer value. When the local, automatic variable p2 is destroyed, it deletes the pointer value it manages.

Then, when the local, automatic variable p1 is destroyed, it deletes the same pointer value, resulting in a double-free vulnerability.

**Noncompliant Code**

**Compliant Code**

#include <memory>

void f() {

std::shared\_ptr<int> p1 = std::make\_shared<int>(); std::shared\_ptr<int> p2(p1);

}

In this compliant solution, the std::shared\_ptr objects are related to one another through copy construction. When the local, automatic variable p2 is destroyed, the use count for the shared pointer value is decremented but still nonzero. Then, when the local, automatic variable p1 is destroyed, the use count for the shared pointer value is decremented to zero, and the managed pointer is destroyed. This compliant solution also calls std::make\_shared() instead of allocating a raw pointer and storing its value in a local variable.

**Note: Stop here for the milestone. Complete this section for Project One in Module Six.**

**Principles(s):** Passing a pointer value to a deallocation function that was not previously obtained by the matching allocation function results in undefined behavior, which can lead to exploitable vulnerabilities.

**Threat Level**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Severity** | **Likelihood** | **Remediation Cost** | **Priority** | **Level** |
| High | Likely | Medium | P18 | L1 |

**Automation**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
| Astree | 20.10 | Dangling\_pointer\_use |  |
| Helix QAC | 2021.1 |  |  |
| Parasoft C/C++ test | 2020.2 | CERT\_CPP-MEM56-a | Do not store an already-owned pointer value in an unrelated  smart pointer |
| PVS – Studio | 7.01 | V1006 |  |

## Coding Standard 5

|  |  |  |
| --- | --- | --- |
| **Coding Standard** | **Label** | **Name of Standard** |
| **Memory Protection** | [STD-005- CPP] | Properly deallocate dynamically allocated resources |

**Noncompliant Code**

In this noncompliant code example, the local variable space is passed as the expression to the placement new operator. The resulting pointer of that call is then passed to ::operator delete(), resulting in undefined behavior due to ::operator delete() attempting to free memory that was not returned by ::operator new().

#include <iostream> struct S {

S() { std::cout << "S::S()" << std::endl; }

~S() { std::cout << "S::~S()" << std::endl; }

};

void f() {

alignas(struct S) char space[sizeof(struct S)]; S \*s1 = new (&space) S;

// ...

delete s1;

}

## Compliant Code

#include <iostream>

struct S {

S() { std::cout << "S::S()" << std::endl; }

~S() { std::cout << "S::~S()" << std::endl; }

};

void f() {

alignas(struct S) **char** space[sizeof(struct S)]; S \*s1 = new (&space) S;

This compliant solution removes the call to ::operator delete(), instead explicitly calling s1's destructor. This is one of the few times when explicitly invoking a destructor is warranted.

**Compliant Code**

// ...

s1->~S();

}

**Note: Stop here for the milestone. Complete this section for Project One in Module Six.**

**Principles(s):** Passing a pointer value to a deallocation function that was not previously obtained by the matching allocation function results in undefined behavior, which can lead to exploitable vulnerabilities.

**Threat Level**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Severity** | **Likelihood** | **Remediation Cost** | **Priority** | **Level** |
| High | Likely | Medium | P18 | L1 |

**Automation**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
| Astree | 20.10 | Invalid\_dynamic\_memory\_alocation\_d  angling\_pointer\_use |  |
| Axivion  Bauhaus Suite | 6.9.0 | CERTC++-MEM51 |  |
| Clang | 3.9 | clang-analyzer-  cplusplus.NewDeleteLeaks  -Wmismatched-new-delete clang-analyzer-  unix.MismatchedDeallocator | Checked by clang-tidy, but does not catch all violations of this rule |
| CodeSonar | 6.0p0 | ALLOC.FNH ALLOC.DF  ALLOC.TM | Free non-heap variable Double free  Type mismatch |
| Helix QAC | 2021.1 |  |  |
| Klocwork | 2021.1 | CL.FFM.ASSIGNFM CL.FFM.COPY CL.FMM  FMM.MIGHT FMM.MUST FNH.MIGHT FNH.MUST FUM.GEN.MIGHT FUM.GEN.MUST  UNINIT.CTOR.MIGHT |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
|  |  | UNINIT.CTOR.MUST UNINIT.HEAP.MIGHT UNINIT.HEAP.MUST  UNINIT.STACK.ARRAY.MIGHT UNINIT.STACK.ARRAY.MUST UNINIT.STACK.MIGHT  UNINIT.STACK.MUST |  |
| LDRA tool suite | 9.7.1 | 232 S, 236 S, 239 S, 407 S, 469 S, 470  S, 483 S, 484 S, 485 S, 64 D, 112 D | Partially implemented |
| Parasoft C/C++ test | 2020.2 | CERT\_CPP-MEM51-a CERT\_CPP-MEM51-b CERT\_CPP-MEM51-c CERT\_CPP-MEM51-d | Use the same form in corresponding calls to new/malloc and delete/free  Always provide empty brackets ([]) for delete when deallocating arrays  Both copy constructor and copy assignment operator should be declared for classes with a nontrivial destructor  Properly deallocate dynamically  allocated resources |
| Parasoft Insure  ++ |  |  | Runtime Detection |
| Polyspace Bug Finder | R2020a | CERT C++: MEM51-CPP | Checks for:  Invalid deletion of pointer Invalid free of pointer Deallocation of previously deallocated pointer  Rule partially covered. |
| PRQA QA-C++ | 4.4 | 2110, 2111, 2112, 2113, 2118,  3337, 3339, 4262, 4263, 4264 |  |
| PVS – Studio | 7.07 | V515, V554, V611, V701, V748, V773 |  |
| SonarQube  C/C++ Plugin | 4.10 | S1232 |  |

## Coding Standard 6

|  |  |  |
| --- | --- | --- |
| **Coding Standard** | **Label** | **Name of Standard** |
| **Assertions** | [STD-006- CPP | Use a static assertion to test the value of a constant expression |

**Noncompliant Code**

#include <assert.h> struct timer {

unsigned char MODE; unsigned int DATA; unsigned int COUNT;

};

int func(void) {

assert(sizeof(struct timer) == sizeof(unsigned char) + sizeof(unsigned int) + sizeof(unsigned int));

}

This noncompliant code uses the assert() macro to assert a property concerning a memory-mapped structure that is essential for the code to behave correctly:

**Compliant Code**

struct timer { unsigned char MODE; unsigned int DATA; unsigned int COUNT;

};

#if (sizeof(struct timer) != (sizeof(unsigned char) + sizeof(unsigned int) + sizeof(unsigned int)))

#error "Structure must not have any padding" #endif

For assertions involving only constant expressions, a preprocessor conditional statement may be used, as in this compliant solution:

**Note: Stop here for the milestone. Complete this section for Project One in Module Six.**

**Principles(s):** Static assertion is a valuable diagnostic tool for finding and eliminating software defects that

may result in vulnerabilities at compile time. The absence of static assertions, however, does not mean that code is incorrect.

**Threat Level**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Severity** | **Likelihood** | **Remediation Cost** | **Priority** | **Level** |
| Low | Unlikely | High | P1 | L3 |

**Automation**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
| Axivion  Bauhaus Suite | 6.9.0 | CERTC-DCL03 |  |
| Clang | 3.9 | misc-static-assert | Checked by clang-tidy |
| CodeSonar | 6.0p0 | (customization) | Users can implement a custom check that reports uses of the  assert() macro |
| Compass/Rose |  |  | Could detect violations of this rule merely by looking for calls to assert(), and if it can evaluate the assertion (due to all values being known at compile time), then the code should use static-assert instead; this assumes ROSE can  recognize macro invocation |
| ÉCLAIR | 1.2 | CC2.DCL03 | Fully implemented |
| LDRA tool suite | 9.7.1 | 44 S | Fully Implemented |

## Coding Standard 7

|  |  |  |
| --- | --- | --- |
| **Coding Standard** | **Label** | **Name of Standard** |
| **Exceptions** | [STD-007- CPP] | Handle all exceptions thrown before main() begins executing |

**Noncompliant Code**

struct S {

S() noexcept(false);

};

static S globalS;

In this noncompliant example, the constructor for S may throw an exception that is not caught when globalS is constructed during program startup.

**Compliant Code**

struct S {

S() noexcept(false);

};

S &globalS() { try {

static S s; return s;

} catch (...) {

// Handle error, perhaps by logging it and gracefully terminating the application.

}

// Unreachable.

}

This compliant solution makes globalS into a local variable with static storage duration, allowing any exceptions thrown during object construction to be caught because the constructor for S will be executed the first time the function globalS() is called rather than at program startup. This solution does require the programmer to modify source code so that previous uses of globalS are replaced by a function call to globalS().

**Note: Stop here for the milestone. Complete this section for Project One in Module Six.**

**Principles(s):** Throwing an exception that cannot be caught results in abnormal program termination and can lead to denial-of-service attacks.

**Threat Level**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Severity** | **Likelihood** | **Remediation Cost** | **Priority** | **Level** |
| Low | Likely | Low | P9 | L2 |

**Automation**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
| Astree | 20.10 | [Insert text.] potentially-throwing-  static-initialization | Partially Checked |
| [Insert text.] Axivion  Bauhaus Suite | 6.9.0 | CERTC++-ERR58 |  |
| Clang | 3.9 | Cert-eer58-cpp | Checked by clang-tidy |
| Helix QAC | 2021.1 |  |  |
| Parasoft C/C++ test | 2020.2  CERT\_CPP-  ERR58-a |  | Exceptions shall be raised only after start-up and before  termination of the program |
| PRQA QA-C++ | 4.4 | 4634, 4636, 4637, 4639 |  |
| Rule Checker | 20.10 | potentially-throwing-static-  initialization | Partially checked |

## Coding Standard 8

|  |  |  |
| --- | --- | --- |
| **Coding Standard** | **Label** | **Name of Standard** |
| **Input output** | [STD-008- CPP] | Do not alternately input and output from a file stream without an intervening positioning call |

**Noncompliant Code**

This noncompliant code example appends data to the end of a file and then reads from the same file. However, because there is no intervening positioning call between the formatted output and input calls, the behavior is undefined.

#include <fstream> #include <string>

void f(const std::string &fileName) { std::fstream file(fileName);

if (!file.is\_open()) {

// Handle error return;

}

file << "Output some data"; std::string str;

file >> str;

}

## Compliant Code

#include <fstream> #include <string>

void f(const std::string &fileName) { std::fstream file(fileName);

if (!file.is\_open()) {

// Handle error return;

}

file << "Output some data";

In this compliant solution, the std::basic\_istream<T>::seekg() function is called between the output and input, eliminating the undefined behavior.

**Compliant Code**

std::string str; file.seekg(0, std::ios::beg); file >> str;

}

**Note: Stop here for the milestone. Complete this section for Project One in Module Six.**

**Principles(s):** Alternately inputting and outputting from a stream without an intervening flush or positioning call is undefined behavior.

**Threat Level**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Severity** | **Likelihood** | **Remediation Cost** | **Priority** | **Level** |
| Low | Loikely | Medium | P6 | L2 |

**Automation**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
| Helix QAC | 2021.1 |  |  |
| Parasoft C/C++ test | 2020.2 | CERT\_CPP\_FIO50-a | Do not alternately input and output from a stream without an intervening flush or positioning  call |
| Polyspace Bug Finder | R2020a | ECRT C++: FIO50-CPP | Checks for alternating input and output from a stream without flush or positioning call (rule fully  covered) |

## Coding Standard 9

|  |  |  |
| --- | --- | --- |
| **Coding Standard** | **Label** | **Name of Standard** |
| **Object Oriented Programing** | [STD-009- CPP] | Do not invoke virtual functions from constructors or destructors |

**Noncompliant Code**

struct B {

B() { seize(); }

virtual ~B() { release(); }

protected:

virtual void seize(); virtual void release();

};

struct D : B {

virtual ~D() = default;

protected:

void seize() override { B::seize();

// Get derived resources...

}

void release() override {

// Release derived resources... B::release();

}

};

In this noncompliant code example, the base class attempts to seize and release an object's resources through calls to virtual functions from the constructor and destructor. However, the B::B() constructor calls B::seize() rather than D::seize(). Likewise, the B::~B() destructor calls B::release() rather than D::release().

**Compliant Code**

class B {

In this compliant solution, the constructors and destructors call a nonvirtual, private member function (suffixed with mine) instead of calling a virtual function. The result is that each class is responsible for seizing and releasing its own resources.

**Compliant Code**

void seize\_mine(); void release\_mine();

public:

B() { seize\_mine(); }

virtual ~B() { release\_mine(); }

protected:

virtual void seize() { seize\_mine(); } virtual void release() { release\_mine(); }

};

class D : public B { void seize\_mine(); void release\_mine();

public:

D() { seize\_mine(); }

virtual ~D() { release\_mine(); }

protected:

void seize() override { B::seize(); seize\_mine();

}

void release() override { release\_mine(); B::release();

}

};

**Note: Stop here for the milestone. Complete this section for Project One in Module Six.**

**Principles(s):**

**Threat Level**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Severity** | **Likelihood** | **Remediation Cost** | **Priority** | **Level** |
| Low | Unlikely | Medium | P2 | L3 |

**Automation**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
| Astree | 20.10 | virtual-call-in-constructor  invalid\_function\_pointer | Fully checked |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
| Axivion  Bauhaus Suite | 6.9.0 | CertC++-OOP50 |  |
| Clang | 3.9 | clang-analyzer-  alpha.cplusplus.VirtualCall | Checked by clang-tidy |
| Helix QAC | 2021.1 |  |  |
| LDRA tool suite | 9.7.1 | 467S, 92D | Fully implemented |
| Parasoft C/C++ test | 2020.2 | CERT\_CPP-OOP50-a CERT\_CPP-OOP50-b CERT\_CPP-OOP50-c CERT\_CPP-OOP50-d | Avoid calling virtual functions from constructors  Avoid calling virtual functions from destructors  Do not invoke class's virtual functions from any of its constructors  Do not invoke class's virtual  functions from its destructor |
| PRQA QA-C++ | 4.4 | 4260, 4261, 4273, 4274,  4275, 4276, 4277, 4278,  4279, 4280, 4281, 4282 |  |
| PVS-Studio | 20.10 | Virtual-call-in-customer | Fully checked |
| SonarQube  C/C++ Plugin | 4.10 | S1699 |  |

## Coding Standard 10

|  |  |  |
| --- | --- | --- |
| **Coding Standard** | **Label** | **Name of Standard** |
| Miscellaneous | [STD-010- CPP] | Value returning functions must return a value from all exit paths |

**Noncompliant Code**

int absolute\_value(int a) { if (a < 0) {

return -a;

}

}

In this noncompliant code example, the programmer forgot to return the input value for positive input, so not all code paths return a value.

**Compliant Code**

int absolute\_value(int a) { if (a < 0) {

return -a;

}

return a;

}

In this compliant solution, all code paths now return a value.

**Note: Stop here for the milestone. Complete this section for Project One in Module Six.**

**Principles(s):** Failing to return a value from a code path in a value-returning function results in undefined behavior that might be exploited to cause data integrity violations.

**Threat Level**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Severity** | **Likelihood** | **Remediation Cost** | **Priority** | **Level** |
| Medium | Probable | Medium | P8 | L2 |

**Automation**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
| Astree | 20.10 | Return-implicit | Fully chcecked |
| Axivion | 6.9.0 | CertC++-MSC52 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Tool** | **Version** | **Checker** | **Description Tool** |
| Bauhaus Suite |  |  |  |
| Clang | 3.9 | -Wreturn-type | Does not catch all instances of this  rule, such as function-try-blocks |
| CodeSonar | 6.0p0 | LANG.STRUCT.MRS | Missing return statement |
| Helix QAC | 2021.1 |  |  |
| LDRA tool suite | 9.7.1 | 2 D, 36 S | Fully implemented |
| Parasoft C/C++ test | 2020.2 | CERT\_CPP-MSC52-a | All exit paths from a function with non-void return type shall have an explicit return statement with an  expression |
| Polyspace Bug  Finder | R2020a | Cert C++: MSC52-a | Checks for missing return  statements (rule partially covered) |
| SonarQube  C/C++ Plugin | 4.10 | S935 |  |
| PRQA QA- C++ | 4.4 | 1510 |  |
| PVS-Stuido | 7.07 | V591 |  |
| RuleChecker | 20.10 | Return-implicit | Fully checked |

**Defense-in-Depth Illustration**

This illustration provides a visual representation of the defense-in-depth best practice of layered security.



**Project One**

There are seven steps outlined below that align with the elements you will be graded on in the accompanying rubric. When you complete these steps, you will have finished the security policy.

**Revise the C/C++ Standards**

You completed one of these tables for each of your standards in the Module Three milestone. In Project One, add revisions to improve the explanation and examples as needed. Add rows to accommodate additional examples of compliant and noncompliant code. Coding standards begin on the security policy.

**Risk Assessment**

Complete this section on the coding standards tables. Enter high, medium, or low for each of the headers, then rate it overall using a scale from 1 to 5, 5 being the greatest threat. You will address each of the seven policy standards. Fill in the columns of severity, likelihood, remediation cost, priority, and level using the values provided in the appendix.

**Automated Detection**

Complete this section of each table on the coding standards to show the tools that may be used to detect issues. Provide the tool name, version, checker, and description. List one or more tools that can automatically detect this issue and its version number, name of the rule or check (preferably with link), and any relevant comments or description—if any. This table ties to a specific C++ coding standard.

**Automation**

Provide a written explanation using the image provided.



Automation will be used for the enforcement of and compliance to the standards defined in this policy. Green Pace already has a well-established DevOps process and infrastructure. Define guidance on where and how to modify the existing DevOps process to automate enforcement of the standards in this policy. Use the DevSecOps diagram and provide an explanation using that diagram as context.

[Insert your written explanations here.]

**Summary of Risk Assessments**

Consolidate all risk assessments into one table including both coding and systems standards, ordered by standard number.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rule** | **Severity** | **Likelihood** | **Remediation Cost** | **Priority** | **Level** |
| STD-001-CPP | High | Unlikely | Medium | High | 2 |
| STD-002-CPP | Medium | Likely | Low | Medium | 3 |
| STD-003-CPP | Low | Likely | Low | Low | 1 |
| STD-001-SYS | High | Unlikely | High | High | 4 |
| STD-002-SYS | Medium | Likely | Medium | Medium | 3 |
| STD-003-SYS | Low | Likely | Low | Low | 1 |

**Create Policies for Encryption and Triple A**

Include all three types of encryption (in flight, at rest, and in use) and each of the three elements of the Triple-A framework using the tables provided***.***

Explain each type of encryption, how it is used, and why and when the policy applies.

Explain each type of Triple-A framework strategy, how it is used, and why and when the policy applies.

Write policies for each and explain what it is, how it should be applied in practice, and why it should be used.

| 1. **Encryption** | **Explain what it is and how and why the policy applies.** |
| --- | --- |
| Encryption in rest | This policy requires all sensitive data stored on Green Pace systems to be encrypted when at rest. This means that data, such as customer records or confidential files, must be encrypted to protect against unauthorized access, even when it's stored on disks or in databases. This policy applies to all systems and databases that store sensitive information. Encryption at rest helps safeguard data in case of physical breaches or unauthorized access to storage systems. |
| Encryption at flight | This policy mandates that all data transmitted over networks must be encrypted during transit. It applies to data transferred between systems, users, or over the internet. Encryption in transit ensures that sensitive data remains confidential and secure during communication and helps prevent eavesdropping and man-in-the-middle attacks. |
| Encryption in use | This policy focuses on protecting sensitive data while it's actively being used or processed. Any applications or processes that handle sensitive information must use encryption to ensure data integrity and confidentiality. This policy aims to prevent data leakage and breaches while data is being utilized. |

| 1. **Triple-A Framework\*** | **Explain what it is and how and why the policy applies.** |
| --- | --- |
| Authentication | Green Pace implements strict authentication policies to ensure that only authorized users gain access to systems and data. This involves username and password-based authentication, multi-factor authentication, or other secure access methods. This policy applies to all systems, applications, and services that require user authentication. |
| Authorization | Authorization policies determine what actions and resources users or systems are allowed to access. This includes setting access permissions, roles, and privileges. The policy defines who has access to what data and functionalities and under what conditions. |
| Accounting | Green Pace maintains detailed logs and records of user activities, changes to the database, additions of new users, user access levels, and file access by users. This information is crucial for auditing, monitoring, and traceability to ensure compliance and detect any unauthorized activities. |

**\***Use this checklist for the Triple A to be sure you include these elements in your policy:

User logins

Changes to the database

Addition of new users

User level of access

Files accessed by users

**Map the Principles**

Map the principles to each of the standards, and provide a justification for the connection between the two. In the Module Three milestone, you added definitions for each of the 10 principles provided. Now it’s time to connect the standards to principles to show how they are supported by principles. You may have more than one principle for each standard, and the principles may be used more than once. Principles are numbered 1 through 10. You will list the number or numbers that apply to each standard, then explain how each of these principles supports the standard. This exercise demonstrates that you have based your security policy on widely accepted principles. Linking principles to standards is a best practice.

**NOTE:** Green Pace has already successfully implemented the following:

Operating system logs

Firewall logs

Anti-malware logs

**Map the Principles**

To map principles to your standards, consider the following:

**Standard:** STD-001-CPP

**Principles Supported:** Principles 2, 4, and 7

**Explanation:**

* **Principle 2 (Least Privilege):** STD-001-CPP enforces that developers should only use libraries, functions, and features that are necessary for the functionality of their code. This aligns with the principle of least privilege by reducing the attack surface and potential vulnerabilities.
* **Principle 4 (Defense in Depth):** STD-001-CPP promotes coding practices that adhere to best practices for security. By doing so, it contributes to a defense-in-depth approach by adding layers of security measures within the codebase to protect against various threats.
* **Principle 7 (Auditability):** The coding standard STD-001-CPP ensures that code is well-documented and that noncompliant code is clearly identified. This aligns with the principle of auditability by providing a clear trail for code compliance and noncompliance.

The only item you must complete beyond this point is the Policy Version History table.

**Audit Controls and Management**

Every software development effort must be able to provide evidence of compliance for each software deployed into any Green Pace managed environment.

Evidence will include the following:

Code compliance to standards

Well-documented access-control strategies, with sampled evidence of compliance

Well-documented data-control standards defining the expected security posture of data at rest, in flight, and in use

Historical evidence of sustained practice (emails, logs, audits, meeting notes)

**Enforcement**

The office of the chief information security officer (OCISO) will enforce awareness and compliance of this policy, producing reports for the risk management committee (RMC) to review monthly. Every system deployed in any environment operated by Green Pace is expected to be in compliance with this policy at all times.

Staff members, consultants, or employees found in violation of this policy will be subject to disciplinary action, up to and including termination.

**Exceptions Process**

Any exception to the standards in this policy must be requested in writing with the following information:

Business or technical rationale

Risk impact analysis

Risk mitigation analysis

Plan to come into compliance

Date for when the plan to come into compliance will be completed

Approval for any exception must be granted by chief information officer (CIO) and the chief information security officer (CISO) or their appointed delegates of officer level.

Exceptions will remain on file with the office of the CISO, which will administer and govern compliance.

**Distribution**

This policy is to be distributed to all Green Pace IT staff annually. All IT staff will need to certify acceptance and awareness of this policy annually.

**Policy Change Control**

This policy will be automatically reviewed annually, no later than 365 days from the last revision date. Further, it will be reviewed in response to regulatory or compliance changes, and on demand as determined by the OCISO.

**Policy Version History**

| **Version** | **Date** | **Description** | **Edited By** | **Approved By** |
| --- | --- | --- | --- | --- |
| **1.0** | 08/11/20223 | Initial Template | Kourosh Farrehiyazdi | Kourosh Farrehiyazdi |
| **1.1** | 26/11/20223 | Updated Encryption Policy | Kourosh Farrehiyazdi | Kourosh Farrehiyazdi |
| **1.2** | 26/11/20223 | Initial Template | Kourosh Farrehiyazdi | Kourosh Farrehiyazdi |

**Appendix A Lookups**

**Approved C/C++ Language Acronyms**

| **Language** | **Acronym** |
| --- | --- |
| **C++** | CPP |
| **C** | CLG |
| **Java** | JAV |