During developpment, make sure:

* implement secure code in at least two appropriate languages to implement front-end and back-end processes

# **https://kirkpatrickprice.com/blog/secure-coding-best-practices/**8 Best Secure Coding Practices

 by Tori Thurmond / December 27th, 2023

When you hire builders to construct a new home, you expect them to take every precaution to ensure once you move in, you won’t find split beams, foundational errors, or holes in the walls. In the same way, software developers are expected to uphold secure coding practices to ensure they aren’t leaving any vulnerabilities open for hackers to exploit.

## What is Secure Coding?

Secure coding standards govern the coding practices, techniques, and decisions that developers make while building software. They aim to ensure that developers write code that minimizes security vulnerabilities. Development tasks can be solved in many different ways, with varying levels of complexity. Some solutions are more secure than others, and secure coding standards encourage developers and software engineers to take the safest approach, even if it is not the fastest.

For example, secure coding best practices often mandate a “default deny” approach to access permissions. Developers using secure coding techniques create code that denies access to sensitive resources unless an individual can demonstrate that they are authorized to access it.

There are several secure coding standards and coding security guides in widespread use today, including the [OWASP Secure Coding Practices](https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/01-introduction/05-introduction) and the [SEI CERT Coding Standards](https://wiki.sei.cmu.edu/confluence/display/seccode).

## Why You Should Use Secure Coding Standards?

In the [2017 breach at Equifax](https://www.nextgov.com/cybersecurity/2017/09/cybersecurity-breach-equifax-left-pretty-much-everyones-financial-data-vulnerable/140844/), malicious individuals accessed personal information because of compromised software at the foundation of their organization. That isn’t the first organization, or the last, to find holes in its secure coding practices and leave themselves open to exploitation.

According to a 2020 survey completed by [Sonatype](https://www.sonatype.com/2020survey), 24% or respondents confirmed or suspected a breach related to their application development practices. That number is staggering when you consider the odds that your organization will be next to experience a breach if you don’t initiate coding security best practices.

**8 Secure Coding Best Practices**

OWASP provides a secure coding practices checklist that includes 14 areas to consider in your [software development life cycle](https://kirkpatrickprice.com/blog/what-is-a-secure-software-development-life-cycle). Of those secure coding practices, we’re going to focus on the top eight secure programming best practices to help you protect against vulnerabilities.

1. Security by Design
2. Password Management
3. Access Control
4. Error Handling and Logging
5. System Configuration
6. Threat Modeling
7. Cryptographic Practices
8. Input Validation and Output Encoding

### **Security by Design**

Security needs to be a priority as you develop code, not an afterthought. Organizations may have competing priorities where software engineering and coding are concerned. Following software security best practices can conflict with optimizing for development speed. However, a “security by design” approach that puts security first tends to pay off in the long run, reducing the future cost of technical debt and risk mitigation. An analysis of your source code should be conducted throughout your software development life cycle (SDLC), and security automation should be implemented.

### **Password Management**

Passwords are a weak point in many software systems, which is why [multi-factor authentication](https://kirkpatrickprice.com/video/pci-requirement-8-3-2-incorporate-multi-factor-authentication-remote-network-access/) has become so widespread. Nevertheless, passwords are the most common security credential, and following secure coding practices limits risk. You should require all passwords to be of adequate length and complexity to withstand any typical or common attacks. OWASP suggests several coding best practices for passwords, including:

* Storing only salted cryptographic hashes of passwords and never storing plain-text passwords
* Enforcing password length and complexity requirements
* Disable password entry after multiple incorrect login attempts

Implementing [logical access](https://kirkpatrickprice.com/blog/webinars-events/logical-access-fundamentals-for-enhanced-security-a-webinar-recap/) controls like password policies can do wonders for strengthening your organization’s security posture.

### Access Control

Take a “default deny” approach to sensitive data. Limit privileges and restrict access to secure data to only users who need it. Deny access to any user that cannot demonstrate authorization. Ensure that requests for sensitive information are checked to verify that the user is authorized to access it.

Learn more about [access controls for remote employees](https://kirkpatrickprice.com/video/soc-2-academy-access-controls-remote-employees/) and [cloud access management](https://kirkpatrickprice.com/blog/aws-iam-security-best-practices/).

### Error Handling and Logging

Software errors are often indicative of bugs, many of which cause vulnerabilities. Error handling and logging are two of the most useful techniques for minimizing their impact. Error handling attempts to catch errors in the code before they result in a catastrophic failure. Logging documents errors so that developers can diagnose and mitigate their cause.

Documentation and logging of all failures, exceptions, and errors should be implemented on a trusted system to comply with secure coding standards.

### System Configuration

Clear your system of any unnecessary components and ensure all working software is updated with current versions and patches. If you work in multiple environments, make sure you’re managing your development and production environments securely.

Outdated software is a major source of vulnerabilities and security breaches. Software updates include patches that fix vulnerabilities, making regular updates one of the most vital, secure coding practices. A [patch management system](https://kirkpatrickprice.com/blog/10-ways-to-conduct-patch-management/) may help your business to keep on top of updates.

### Threat Modeling

Document, locate, address, and validate are the four steps to threat modeling. To securely code, you need to examine your software for areas susceptible to increased threats of attack. Threat modeling is a multi-stage process that should be integrated into the software lifecycle from development, testing, and production.

### Cryptographic Practices

Encrypting data with modern cryptographic algorithms and following [secure key management best practices](https://kirkpatrickprice.com/webinars/encryption-key-management/) increases the security of your code in the event of a breach.

### Input Validation and Output Encoding

It’s important to identify all data inputs and sources and validate those classified as untrusted. You should utilize a standard routine for output encoding and input validation.

## How to Ensure Your Code Is Secure

By patching your systems regularly, you’re taking these secure coding guidelines to the next level. Patch and [vulnerability management](https://kirkpatrickprice.com/blog/notes-from-the-field-center-for-internet-security-control-7-continuous-vulnerability-management/) is focused on identifying risk and enabling systems to stay up to date. Through these methods and security testing, you’re ensuring that your code is properly checked for errors.

## Work with KirkpatrickPrice to Establish Coding Best Practices in Your Organization

Does finding and mitigating your vulnerabilities using OWASP feel overwhelming? We get it. Anytime you’re dealing with processes or systems that will affect the security of you organization is bound to be a little stressful. But that’s what we’re here for. We want to partner with you on your security and compliance journey to help you reach your goals and become unstoppable. [Connect with one of our experts](https://kirkpatrickprice.com/contact/) to get started today.