

Secure Coding Specifications & Developer Guidelines

September 2009

Security is the most important software *quality*.

Whether you write custom SAP extensions internally or outsource this task to consulting companies: Insecure code will put your business at risk and cost you additional money. Also, if your project specification does not contain security requirements, you can't even hold the consulting company responsible.

Insecure software can damage your reputation, damage your business and may even lead to compliance violations.

Aim for highest software quality, especially regarding security.

Education is the best way to secure software.

If developers know the most common security risks and have a guideline at hand to avoid them, you will have much more secure software right from the beginning.

More secure software from the beginning means less money, time and resources for fixing bugs in QA tests. Less money, time and resources for re-testing. Also, it will help keeping your going-live schedules.

Our solution

Virtual Forge's Secure Coding Specifications and Developer Guidelines are a very important step towards a high security and compliance level in your business applications.

While the specifications define *what* has to be done, the guidelines define *how* a developer can write secure software.

Key advantages

The specifications and guidelines

- Contain unique ABAP security know-how, by the authors of "Secure ABAP-Programming"
- Explain what pitfalls exist and how developers should deal with them
- Are written in a clear and easy to understand way
- Are state of the art and always up-to-date – through optional maintenance

The *General Guideline* contains development best practices and requirements that are independent of the programming language. They are for internal and external use.

Language-specific guidelines are available for *ABAP* and *Java*. They contain to the point instructions for secure development. While those guidelines are for internal use, they are coupled with specifications for external development. These specifications should be included in all projects as mandatory security requirements.

All guidelines are available with an *optional maintenance* that guarantees continuous updates in case new threats arise.

