Policy for external software developers

External service providers involved in Fronius software development must comply with the following requirements:

Security by Design

IT security and software security standards must be observed and implemented as early as the design phase of the system.

Security by Default

Each delivered product must meet - according to the protection requirement - basic IT security requirements, if applicable, in accordance with the control target lists (OWASP standards) provided by Fronius.

Security in Deployment

"Security in Deployment" refers to the maintainability of a system/product that is already in use at the customer. The product must be easy to deploy and administer in order to keep the application up to date and thus secure in the long term.

Initial IT security concept

IT security requirements must be specified in an initial IT security concept. Depending on the product

- the IT security concept is created by Fronius and transmitted to the external service provider, or
- must be prepared by the external service provider and accepted by Fronius.

For the initial safety concept, the following points in particular must be documented:

- Brief description of the application (purpose, target group)
- High-level system architecture of the application (client/server, web, use of cloud services) with all associated remote services,
- Availability of the application on the Internet (remote maintenance concept, if applicable),
- Autonomous deployment of the application at the customer's site (no backend required, no online connection),
- Approximate number of users accessing the application,
- Systems on which this application depends and systems that depend on this application.
- The IT security concept must be documented in the corresponding system and architecture specifications. Revision is necessary to ensure traceability.

Measures in the development process

- Mandatory use of version control software

- "Published binaries" are to be used by build systems only (Isolated Development Environment).
- Program code, if required by Fronius, must be peer-reviewed for IT security before being incorporated into the published product (e.g., "master branch", "release branch").

Security relevant compiler warnings must not be ignored

Source code must be compiled with the highest available warning level and resulting compiler warnings must be resolved by adequate source code changes. The goal is to reduce security-related compiler warnings to a minimum. If it is not possible to fix the cause of the warnings, appropriate documentation is required (e.g., when using an obsolete 3rd party interface).

Frameworks and libraries used

All frameworks and program libraries used, which are available at least in published versions, must be documented. Frameworks and program libraries must be continuously checked for security-relevant errors.

Functions, protocols, and security features should be based on open standards and must be used from reliable sources (program libraries) (e.g., .Net, openssl). This applies in particular to the following topics:

- Cryptographic methods
- Random number generator
- Key exchange or key password management
- Hash or MAC functions
- Encryption or signature
- Authentication (e.g., software tokens)
- Authorization
- Session management (e.g., creation of session keys, session expiration, cookies).

Test systems and productive data

Only test data or anonymized production data may be used on test systems. If this is not possible, the test system must be configured and operated like a production system.