

# How to know if it is safe to log sensitive information to a file



This page has been made public for vendors

## Question

Fortify has flagged data written to a log file as leaking sensitive or system information. I trust files on my filesystem. How can I know that it is safe?

## Answer

Fortify views all data that leaves an application as potentially exposed to a malicious party. Therefore sensitive and system data that leaves an application is marked as potentially being exposed. This includes data written to log files and other files stored on the local filesystem.

Best practice is to not trust that data written to files cannot be read by an attacker. Vulnerabilities in the operating system, other applications running on the server, and misconfiguration can all lead to compromise of those files. Sensitive and system data should not be written out to files unless required for auditing or business purposes. System data should not be written out to trusted files unless precautions are used to protect those files. Sensitive data, such as PII, should not be written out to files unless they are appropriately encrypted.

While best practices should be followed whenever possible, the Software Assurance Team recognizes that this is not always feasible in all cases for all applications. When it is not possible to follow the best practices described above, the developer can show that the file is adequately protected as follows:

- The developer will need to provide documentation that attests that the server hosting the application is configured and operated securely according to VA hosting facility policy and that the files in question are protected from unauthorized read and/or write access
- If sensitive data such as PII or PHI is being written to a file it should be encrypted. If it is not encrypted the developer will need to provide documentation that attests that the files containing the sensitive data are being handled securely according to VA policy.

## References

- [VA Secure Code Review SOP](#)

*Request code review tools, validations, and support [HERE](#).*