Filestash

Information Security
System Development Life Cycle

Summary

The Filestash System Development Life Cycle is our framework for creating, deploying, and retiring information systems and product features. It is based on guidelines from the National Institute of Standards and Technology and covers five main phases: Initiation, Development, Implementation, Operations, and Disposal. By integrating information security into every phase, Filestash protects data and avoids costly revisions later on. The following sections describe how we apply these secure practices throughout the SDLC and highlight the key security activities involved.

Contents

1 Initiation Phase

During the Initiation Phase, Filestash defines why a new system or enhancement is needed and documents its purpose. We identify the information the system will handle and the people who will need access. We also clarify whether the project is a new system or an extension of an existing one. At this stage, we perform a preliminary risk assessment to look for threats, vulnerabilities, and any regulatory requirements. By recognizing security needs early, we can establish the overall risk context for the new project. If the project is approved, we refine the goals and specify high-level security requirements, which may include references to existing Filestash policies.

2 Development Phase

In the Development Phase, Filestash designs, codes, purchases, or otherwise creates the components that were defined in the Initiation Phase. We follow secure coding practices that align with established guidelines, including those published by the Open Web Application Security Project (OWASP). This approach helps us identify and mitigate common vulnerabilities while ensuring our functional and security requirements are defined at the same time. For instance, we may require features such as access control, encryption, logging, or secure code reviews, and we also include operational practices like developer training. This stage can include traditional system development or involve acquiring external services if needed. If we work with external partners, we include security clauses in contracts so that service-level agreements reflect Filestash security needs.

Filestash also uses separate development, testing, and staging environments for all code changes and infrastructure updates. Each environment is set up to closely match the production configuration so that we can validate features and security measures under conditions that resemble actual usage. We run developmental testing on new features and security controls before moving on to Implementation, and this testing can include unit tests, integration tests, or specialized security tests. If any security gaps appear, we fix them to make sure the system meets our standards prior to deployment.

3 Implementation Phase

Once the solution has passed internal testing, Filestash installs it in the operational environment. We configure and enable every security feature, such as encryption or access management, before releasing the product. We also verify that the system design and security specifications match what was originally planned. If we add new controls, we test them separately to confirm they do not disrupt existing parts of our platform. We document all test results and any updates so that the final system status is clear.

4 Operations Phase

After successful deployment, Filestash continues to monitor and maintain the system. This includes handling updates, fixing bugs, and enhancing features. We continuously review system performance and security. For instance, we may look at application logs, run vulnerability scans, and update operating systems or libraries. Configuration management is part of this effort, and any changes to the system are evaluated for their security impact. By actively watching for operational issues, we can fix potential security concerns quickly and maintain trust with our users.

5 Disposal Phase

Eventually, every Filestash system or component reaches the end of its useful life. During the Disposal Phase, we archive necessary data, retire hardware, and remove software without leaving behind any sensitive information. We follow legal and regulatory requirements for data preservation, which may include storing cryptographic keys to ensure future access to encrypted data. We also sanitize or destroy all media used by the system to prevent unauthorized recovery of sensitive details. This approach might involve clearing, purging, or physically destroying disks and other storage. Our formal process ensures that sensitive information is not exposed once a system is taken out of service.

6 Security Activities Within the SDLC

Filestash integrates several security activities at each phase of this lifecycle. We start with a risk assessment during the Initiation Phase to guide our initial security planning. During the Development Phase, we enhance this plan and perform detailed testing. In the Implementation Phase, we verify that our security controls function as designed in the final environment. During Operations, we continuously monitor the system and update configurations. At the end, in the Disposal Phase, we properly remove or archive any data, hardware, or software in a secure manner. By carrying out these steps in every phase, Filestash remains committed to strong and proactive security measures.

7 Conclusion

Filestash's Secure Development Lifecycle Policy reflects our dedication to embedding security at every step of our development process. By following the NIST model and aligning with recommended standards, we provide reliable products while protecting the confidentiality, integrity, and availability of our users' data. This policy supports the needs of our customers, meets procurement and regulatory expectations, and ensures that Filestash systems remain resilient throughout their entire lifecycle.