The AET

Change Management Policy

Purpose and Scope

This Change Management Policy defines how changes to applications, systems, services, and infrastructure are planned and implemented. The goal of change management is to increase awareness and understanding of proposed changes across The AET and ensure that all changes are made in a thoughtful way that minimize negative impact to services and customers.

From time to time, The AET may update this policy and implement different levels of security controls for different information assets, based on risk and other considerations. This policy is guided by security requirements specific to The AET including applicable laws and regulations.

This policy applies to all The AET assets and personnel acting on behalf of The AET or accessing its applications, infrastructure, systems or data. All personnel are required to read, accept and follow all The AET policies and plans.

Change Management

All code change requests and critical infrastructure or network-related change requests must be documented end-to-end via The AET's change management and ticketing tools.

Change management should be conducted according to the following procedure:

(1) Product Roadmap

The The AET product management team evaluates which change requests and features will be implemented based on their alignment with the business plan and the overall level of effort required. All change requests should be prioritized in terms of benefits, urgency, effort required, security impacts, and other potential impacts on the organization’s operations.

A ticket should be created to track a change request at the onset. If the change is part of an existing ticket the original ticket may be used and modified appropriately.

(2) Planning and Evaluation

Planning and evaluation must include design, scheduling, and implementation of a communications plan, testing plan, and roll-back plan. During planning, wire-frames, mockups, and functional requirements may be created and reviewed among the applicable team members. The team may set priority levels of the service and may determine any risk that the proposed change introduces to the system. It is during this phase that the scope and impact of the change will be determined.

(3) Build, Test, and Document

During building, The AET sprints may be defined and the overall software design and development occurs.

UI/UX and other optimizations should be performed during this phase to enhance the performance and security of the change across all platforms.

The changes must be tested in a non-production environment before release to production. Test setups and scenarios are built for operational, performance, and security testing. Test scripts and suites should be developed, used, and updated as changes occur.

Documentation must be updated during this phase, such as release notes, help articles, and blog posts. Existing documentation is updated to ensure that team members and customers have the most up-to-date and accurate information related to the changes performed. Customer-facing documentation should be provided to The AET customers as applicable.

(4) Code Review

The AET uses code reviews to maintain the quality of The AET code and products. Code reviewers should look at:

Design
Is the code well-designed and appropriate for your system?

Functionality
Does the code behave as intended by the plan? Is the way the code behaves good for its users?

Complexity
Could the code be made simpler? Would another developer be able to easily understand and use this code when they come across it in the future?

Tests
Does the code have correct and well-designed automated tests?

Security
Are there any security risks in the code as identified by the latest OWASP Top 10?

Naming
Are there clear names for variables, classes, methods, etc.?

Comments
Are the comments clear and useful?

Style
Does the code follow The AET style guides?

Documentation
Was the relevant documentation updated or created?

How to do a code review? Google Engineering Practices Documentation provided under the CC 3.0 License.

Secure Coding
Secure coding practices are incorporated into the development lifecycle and security architecture of The AET. Engineers at The AET are responsible for defining security requirements initially and throughout all phases of the software development life cycle and then evaluating for compliance with those requirements.

All engineers at The AET are responsible for reviewing the OWASP Top 10 Web Application Security Risks.

(5) Approval and Implementation

Once the new release is ready for deployment and the appropriate documentation is in place, the new release must be approved and reviewed by the appropriate product owner prior to being pushed to the production environment.

The ability to push changes to production at The AET must be restricted to a limited set of authorized team members, and the engineer responsible for coding the change should not also be responsible for pushing the change to production, unless there is prior approval of the exception by management.

(6) Communication

Implemented changes should be communicated to all applicable team members and externally as appropriate.

(7) Post-Change Review

The AET continuously measures the success of new releases and identifies areas that can be enhanced further in the future.

The appropriate team must conduct a post-implementation review to determine how the change is impacting The AET and The AET's customers, either positively or negatively. Discuss and document any lessons learned with product management and other appropriate team members.

The AET must utilize version control tools that allow for efficient rollbacks of commits from production if any issues arise during the post-change review.

Hotfixes / Critical Issues / Emergencies

The following are potential emergencies that may require a hotfix:

- A customer is completely out of service
- There is severe degradation of service needing immediate action
- A system/application/component is inoperable and the failure causes a significant negative impact
- A response to a natural disaster
- A response to an emergency business need
- A critical vulnerability or security issue is identified

If a hotfix is required, the applicable manager should be immediately notified.

The notification should include at a minimum the following information:

- Will the change cause an interruption in service?
- What additional customers will be affected (in the event a change is needed to fix an outage) and who needs to be notified?
- What is the possible workaround until the problem is resolved?
- What is the approximate length of the outage?
- Notification of resolution
- Submission of a ticket to accurately describe the outage

Emergencies after normal business hours, on the weekend, or on holidays, must follow an appropriate communication and resolution process. A ticket must be generated and team members may need to notify affected customers, as determined by management. Emergency changes must be revisited to ensure no additional security issues were introduced into the product, service, or supporting infrastructure. A completed ticket should be submitted through the regular reporting process promptly following when the change was made.

Management must review all emergency submissions to ensure the change met the criteria for an “emergency change” and to prevent the process from becoming normal practice to circumvent the Change Management Policy. Any questions will be directed to the individual(s) who approved the change.

Exceptions

The AET business needs, local situations, laws and regulations may occasionally call for an exception to this policy or any other The AET policy. If an exception is needed, The AET management will determine an acceptable alternative approach.

Enforcement

Any violation of this policy or any other The AET policy or procedure may result in disciplinary action, up to and including termination of employment. The AET reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. The AET does not consider conduct in violation of this policy to be within an employee's or contractor's course and scope of work.

Any employee or contractor who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of The AET as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

Responsibility, Review, and Audit

The AET reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

This document is maintained by Roger Hanagriff.

This document was last updated on 01/29/2024.