Change Management Policy

Purpose

Deploying changes, updates, and new software into production may, if not managed effectively, result in outages or other customer disruptions. In order to protect the reliability and availability of Castle services, the company has defined this change management policy to govern all changes within the company's environment. This policy defines the process for reviewing, approving, and applying changes to Castle's services. All changes applied to company systems must adhere to this process. For questions relating to this policy, contact the Operations department.

Scope

This document applies to all company personnel, contractors, third party service providers, or affiliates applying changes to Castle-operated hardware, both physical and virtual, l within its production hosting datacenter(s) or other network facilities.

Exceptions

This document should not be interpreted to apply to Castle customers in governing their implementation of changes to their own equipment or systems, which remain their responsibility.

Policy

Prior to implementation, all changes must be characterized and reviewed to assess the nature and level of risk it presents to Castle systems. In reviewing changes, the following criteria are used in evaluating whether to proceed with implementation:

- The confidentiality, integrity, and availability of Castle production datacenter and network services
- Customer requirements that serve as a business driver
- Internal Castle business objectives and priorities
- Prevention of emerging or imminent disruptions to services
- Changes or planned changes that may be impacted or conflict as a result

During change review and approval, it is the responsibility of the reviewer(s) to balance each of these requirements, with the overall stability of Castle customers being the primary objective.

Change Request Details

Change requests must generally include all of the following information:

- The requester of the change and the proposed implementer (where different)
- Description of the change, including detailed deployment procedure
- Description of the effects of the change and any suspected side-effects
- Justification and purpose of the change
- Scope and scale of the change, including affected location(s)
- Requested implementation schedule and timeline
- Change type (normal or emergency)
- Impact Level (high, medium, low)
- Pre-deployment testing results and post-deployment verification test plans
- Rollback plan
- Expedited maintenance justification (if required)

- Peer review results, where available

Change Approvals

The primary responsibility for oversight and governance of change processes rests with the CTO (Sebastian Wallin), who is also referred to as the Change Manager in this document. The Change Manager is responsible for ensuring that all personnel understand and adhere to this change management process, that change is effectively controlled to effectively balance risks, and communication with all parties about planned changes (when appropriate.)

The Change Manager is empowered to approve Low Impact changes without further approvals. At his or her discretion, any change may be submitted to the Change Approval Board for full review, regardless of assessed impact.

The Change Approval Board consists of a cross-functional group of senior engineers within Castle. The Change Manager is responsible for leading the Change Approval Board (CAB), scheduling regular meetings of the CAB as required, and ensuring that there is adequate and appropriate representation on the CAB.

Standard Change Process

Below are details on the processes for submission of change requests, request approvals, and change implementation:

Change Request Submission

Change tickets are submitted for approval by creating a ticket in JIRA and result in a GitHub Pull Request (PR). Requestors are responsible for ensuring that all fields in the ticket are filled out, and required attachments such as test results or rollback plans are attached. Failure to complete all fields or include all relevant attachments will result in delay of approvals or rejection of the request.

Change Review and Approval

Change requests are evaluated and assessed using a standard approval process. Once the Change Manager accepts a change request as valid and confirms it includes all required information, the change request follows Castle's change approval process.

Depending on the assessed impact of a change, it may be immediately approved by the Change Manager. For changes subject to review by the full CAB, the Change Manager has, at his or her discretion, the option to route the request to each member of the CAB for individual approval, or to schedule a meeting for a group review of the change request. In cases where CAB approval of the change is not unanimous, it is the responsibility of the Change Manager to either work with the requestor and the dissenting parties to reach a resolution, or deny the change request.

Change Deployment

When the change is ready to be deployed, a slack notification is sent to #readonly-log of changes and following the implementation plan submitted and approved as part of the change request. In the event that situations change and the plan needs to be adjusted during maintenance, the Engineering team is responsible for following the rollback plan.

Once the change process has been completed, a slack notification is sent to #readonly-log that the change has been completed. Results of any post deployment verification should be attached to the original change request, and the state of the change request should be changed to Complete.