Cloud Security

Changes to the Cloud Environment

Changes to the Cloud Environment include:

- Provisioning new compute & storage resources
- Updating configurations & base images for compute & storage resources
- Updating Virtual Private Cloud & Security Group rules
- Provisioning new subnet IPs
- Modifying DNS records
- Updating TSL certificates

All changes are subject to:

- A change to deployment, architecture & cloud environment documentation in the codebase
- A review of the methodology and documented changes
    - The developer requesting changes must explain any risks associated with the change, mitigations, and advance testing methods that may be used.
- Providing a full audit log of actions taken upon deployment
- Verification via manual testing, access & network logging, load testing, etc. as appropriate by the release engineer.

Notification of Changes: We will notify our client and customers of changes to the cloud environment in cases where the change is likely to disrupt services, workflows, or introduce new security vulnerabilities. Our chief technology officer will communicate the planned change and the associated risks at least 48 hours before the change is implemented.

Cloud-related Access Policy

Only release engineers are provided access to the Cloud Environment via IAM. Release engineer accounts have minimal necessary authorizations to make environmental changes and run standard deployments; only the technical lead of NK has administrator level access. Release engineers may only execute changes, after review. Access to the Cloud Environment itself is enabled by SSH keys. The NK technical lead may grant, revoke, or refresh these keys as needed during personel additions, removals, and potential leaks.

Training & Certification

All Nested Knowledge developers with production access (release engineers) receive at minimum AWS Cloud Practitioner certification. New release engineers are supervised during their first 5 deployments or Cloud Environment modifications.

Compliance Statement

All Employees and Contractors who access Nested Knowledge’s information systems will be provided

with and required to review the Cloud-Related Access Policy.

Revision History

Author	Date of Revision/Review	Comments/Description
K. Holub	11/17/2021	Review Completed
K. Cowie	11/17/2021	Initial Draft Completed