Omeka Services Security Audit Policy

Omeka Services security audits of the Amazon Web Services instances are conducted quarterly, and upon the establishment or dissolution of a hosting account, and include the following reviews:

I. Review AWS Account Credentials

1. Remove unused root access keys.
2. Rotate root access keys regularly.

II. Review IAM Users

Take these steps when you audit your existing IAM users:

1. Delete users that are not active.
2. Remove users from groups that they don't need to be a part of.
3. Review the group policies.
4. Delete security credentials that users do not need or that might have been exposed.
5. Rotate (change) user security credentials periodically, or immediately if they are ever share them with an unauthorized person.

III. Review IAM Groups

Take these steps when you audit your IAM groups:

1. Delete unused groups.
2. Review users in each group and remove users who don't belong.

3. Review the policies attached to the group.

RECORD OF CHANGES:
Reviewed and updated May 15, 2019 -- SML