BISHOPFOX

5 PRIVILEGE ESCALATION PITFALLS TO AVOID WHEN SETTING UP AWS

01	**Allowing IAM Permission on Policies** No normal user should be able to change policies that apply to themselves or others.	**Affected Permissions** iam:CreateAccessKey iam:CreateLoginProfile iam:UpdateLoginProfile iam:AddUserToGroup
02	**Allowing IAM Permissions on Other Users** No normal user should be able to change the properties of other users, either directly or through modification of groups or roles.	**Affected Permissions** iam:CreatePolicyVersion iam:SetDefaultPolicyVersion iam:AttachUserPolicy iam:AttachGroupPolicy iam:AttachRolePolicy iam:PutUserPolicy iam:PutGroupPolicy iam:PutRolePolicy
03	**Updating an AssumeRolePolicy** No normal user should be able to change a role's AssumeRolePolicy.	**Affected Permissions** iam:AssumeRolePolicy
04	**Allowing iam:PassRole with Wildcards** Using wildcards will generally lead to dangerous privileges, but iam:PassRole in particular can cause problems as it may allow users to pass privileged roles to AWS services under their control.	**Affected Permissions** **iam:PassRole**
05	**Allowing Priv Esc through AWS Services** Limit the permissions of users on all AWS services, since specific combinations of permissions and services can lead to privilege escalation.	**Affected Permissions** Lambda Glue Cloud formation Data pipeline

More privilege escalation information available at know.bishopfox.com/research/privilege-escalation-in-aws