Jisc Cloud Solutions

Our access to your data on AWS

1. Introduction

The terms of our customer contracts set out our obligations to customers in respect of how we handle their confidential information and process their personal data. This document further describes the approach that our staff follow when accessing our customers' AWS accounts and details the access we have to customer data (including personal data) hosted in AWS.

2. Context

It is important to understand how our customer accounts are organised and managed. This is described below:

We use AWS 'Organizations' to structure all our customer accounts. The use of Organizations follows AWS best practice and allows us to, optionally, use Service Control Policies (**SCP**s) and StackSets to apply security policies and other configurations at the organisation level, rather than having to configure multiple accounts separately. This allows us to configure security settings more consistently and reliably.

Each customer account sits within one of several Organizations. Depending on several factors, including whether we are providing a managed service or not, that Organization may be unique to a single customer or may be shared amongst many customers. **In all cases, we own the management account (sometimes referred to as the payer account) at the root of the Organization.**

The fact that we own the management account gives us the ability to grant ourselves access to any account within the Organization. However, despite having that level of control, we only use this ability to access our customers' accounts as described in sections 3 and 4 below.

In fact we encourage our customers to use CloudTrail (and CloudTrail alerts) to audit our access so that they can confirm for themselves that we are only accessing their accounts in the ways stated in this document. We are happy to help customers configure CloudTrail if necessary.

We also strongly encourage our customers to adhere to AWS best practices, including:

- Not using the management account for anything other than billing and Organization management.
- Encrypting all data in transit and at rest.

Whilst encrypting data does not, typically, prevent Jisc staff from accessing it, it is a significant step towards adopting a good security posture more generally.

3. Resell-only customers

These are customers that buy their AWS accounts through Jisc but for whom we do not provide a managed service.

- We never access our resell-only customer accounts without the customer's permission and under their written instruction and even then only for limited agreed purposes.
- Except in extreme circumstances, we will only ever access the customer's management (i.e. payer) account. For example, this may be necessary during the initial configuration of the Organization. We also require read-only access to billing data so that we can generate invoices for the customer.

4. Managed service customers (Core and Enhanced)

These are customers that buy their AWS through Jisc and for whom we are providing our 'core' or 'enhanced' Managed AWS service.

- We access all our managed service customer accounts so that we can configure and monitor them on behalf of the customer.
- We access (at the operating system level) all customer EC2 instances that we are managing so that we can configure and deploy patching, anti-malware, backups, etc.
- We access all customer RDS instances that we are managing so that we can perform the tasks set out in our Managed Database service.
- For these reasons, it is also technically possible for us to see our managed service customer's data (which may include personal data). However, we will only access this data where it is a necessary part of incident management or handling a support request. Furthermore, where such access is necessary, we will always use reasonable commercial efforts to seek the customer's written consent before doing so.