AWS IAM User and Key Pair for Authentication on AWS accounts

An IAM (Identity and Access Management) user enables you to access the FSDI (Federal Spatial Data Infrastructure) AWS (Amazon Web Services) accounts. For each user, a user/password account and/or a key pair can be created.

For each needed FSDI AWS account one distinct user has to be created. Independently of the type of access (login/password or key pair), the present form must be filled. An appendix will list the types of accesses that are associated with the requester at time of signing. Any addendum to permissions stated in this document must be performed via the Helpdesk ticketing system (helpdeskbgdi@swisstopo.ch, Subject "AWS IAM access") and does not require further signing.

In order to prevent misuse please read the following directives carefully and fill the form at the end.

1 IAM key pair

If a key pair is requested, this can be provided in the following ways:
   a) Clear text file deployed via ssh into a folder on a linux machine, with 600 permission for the requester
   b) Via signed email, in an encrypted file
   c) Via USB-key, in an encrypted file

In order to guarantee the confidentiality of your private key the following conditions have to be respected:

   1. The private key is personal:
      – do **not share** it with others
      – do **not store it unprotected** (e.g. read permissions of the private key file for other users, public folder, public github repository, etc)

2 IAM Password and double factor authentication

If an IAM user, with login/password authentication is requested, a second factor authentication is needed. AWS provides several second factor authentication methods, to access your FSDI AWS account you will need to use your existing smartphone or tablet running any application that supports the open TOTP standard (e.g. google authenticator).

2.1 Password
In order to guarantee a secure password the following conditions have to be respected:

   1. The password has to contain at least **12 characters**.

   2. The password has to contain different characters from the 4 following categories:
      – **numbers** [0-9]
      – **lower case letters** [a-z]
      – **upper case letters** [A-Z]
      – **special characters**, e.g.,[$,&,%,-,@,+,_,#,etc.]

   3. The password is personal:
      – do **not share** it with others
      – do **not store** it unprotected (e.g. unencrypted text file or open memo at your workplace)

<table>
<tr><td>

Tip

In order to build a strong password imagine a sentence which is easy to remember. Then use special characters, numbers and the first letter of each word to compose your password.

Example:
«*In Bern a beefsteak and 5 potatoes costs 30 Dollar*»
becomes
« *IBab&5pc30$* »

</td></tr>
</table>

2.2 Changing Password

It is recommended that you change your password in a monthly interval. To change the password login into AWS console and change your password in your account settings.

3 Sign Off

Inform swisstopo if you do not require your IAM access anymore (e.g. when the related project has finished).

<table>
<tr><td>

Send an email to helpdeskbgdi@swisstopo.ch with the subject « **AWS IAM access** ».

Indicate your **name** and your intention to **sign off**.

</td></tr>
</table>

4 Agreement

Please **fill** the form below and **return** it to the following address:

Federal Office of Topography swisstopo
COGIS
Geoinformatik IGI
Seftigenstrasse 264
3084 Wabern

Last Name   _____

First Name   _____

Organisation   _____

Email   _____

Telephone   _____

Purpose   _____

                  _____
                  (mission or project the AWS IAM credential is being used for)

By signing below, you certify that you have read, understand and comply to the directives stated in this document and the appendix:

Place and Date   _____

Signature   _____

5 Appendix

List of FSDI AWS credentials:

_____

_____

_____

_____

_____

_____

_____