Skillzminer Limited
163 Bath Street
Glasgow
G2 4SQ
www.skillzminer.com

Title	InfoSec FAQ
Version	1.1
Authorised by	Kirsty Mitchell
Published date	27/6/2022
Next review date	27/6/2023

1. **Describe the security elements of the system, including which features of AWS are used to protect customer data.**

   Our solution has been designed with consideration to system resilience of which security is an important and inherent element. Skillzminer has teams who develop using secure design and coding practices and have our solutions reviewed by third-party experts. We are cognizant of and well versed in the practice of following Open Web Application Security Project (OWASP) guidelines and we take advantage of the AWS modular security landscape, available to us as APN AWS partners within AWS.

   a. Access to the application is handled via AWS Amplifys front end which communicates with our identity provider(Cognito) to create temporary access credentials for users upon successful logins.
   b. All APIs are managed via API Gateway which is configured to only allow Cognito authenticated access. Separate Identify and Access Management (IAM) roles and policies are in place for different users to allow different access to different resources. Backend Lambda functions handle further checks based on organisations and roles before accessing any user data.
   c. Storage of user data is held via DynamoDB which is encrypted both rest and transit. We utilise AWS's regional data centres to ensure compliance with local data regulations. We currently have instances in the UK (London) and Ireland (Dublin) but new regions can be activated quickly

2. **Provide additional information about security features in AWS that are utilised to protect the solution.**

   As expounded in our response to Q1 above consider them also here. We have also added some more examples of our following good practices as an extension to the above response and this question and would ask that their component parts be considered in the round.

   a. All AWS users have Multi-Factor Authentication (MFA) enabled (Including root user). Restriction on user accounts is handled via AWS IAM. Users are granted permission for services based on role requirements. We use AWS Security Hub to ensure we adhere to “AWS Foundational Security Best Practices” security standards.
   b. All services have restricted access based on authenticated usage via API Gateway.

c. Right now we are in the process of revising our EC2 network access rules. This includes restricting port access with new security groups.

3. Provide information about the backup/disaster recovery elements of the solution itself.

Skillzminer has a mature approach to backup and protection. We follow the National Cyber Security Centre (NCSC) backup guidelines, viz., 3-2-1+1. Our solution is GDPR compliant in terms of how and what we store and its residency.

a. User data stored via dynamo has continual Point-In-Time Recovery (PITR), as well as on-demand backups triggering monthly with year-long retention.
b. Backups for all assets including images and containers are stored in S3 via AWS Backup and handled daily with monthly long retention and monthly with year-long retention. Other images and containers are versioned and stored via S3 (and so archived with Backup)
c. We retain one backup copy offline
d. Restoration of backups is done via Dynamo & AWS Backup management console respectively.
e. We test and restore our solution at least quarterly
f. This was last completed on 11/04/2022

4. Describe additional authentication methods used for administrative accounts/database access, such as multifactor authentication or access only from particular network segments/locations. There is mention of "identity authentication processes" and MFA in the 3rd party assessment document; it would be good to get some more detail.

Skillzminer implements additional controls for privileged access. It is not generally our position to disclose all of the measures we have in place for this. We have additional controls in place to restrict access to specific elements based on geography, IP, role etc. As an example:

a. Virtual MFA is enforced on all AWS console access. IAM restrictions are enforced on users based on the required use. Please also see our answers to Q2 above

5. Provide additional information or extracts from the third-party assessments and vulnerability scans of the system

As you would expect we have our platforms scanned regularly for vulnerabilities and have a regime for patch management. Our overall platform is tested regularly by Seric, award-winning cyber security practice for vulnerabilities and we have had our architectural design reviewed by them and AWS also. If you require more than what we have stated above have an additional charge for this.

6. Details of configurable options around authentication for account passwords.

Skillzminer have secure password practices which align with the elements described (password complexity, length, history or change frequency)

a. Password complexity - they must contain a combination of characters, numbers and special characters/symbols.
b. Password Length – all passwords must be at least 8 characters long
c. We are also looking into providing MFA for candidates and job seekers as well as Password Change Frequency – Passwords must be reset every X months

7. Details of the forgotten password/reset mechanism for users.

Skillzminer has implemented a secure self-service password reset.

- **a.** To authenticate users must use a temporary password which is valid for 30 days from being issued. Once logged in using the temporary credentials users must create a permanent password. This applies to both jobseekers and staff.
- **b.** Once authenticated users can reset forgotten passwords from the jobseeker or staff login pages. A MFA token is sent to their email address which must be used to reset their password.

8. Details of any account lock-out period.

Skillzminer confirms that we do implement account lockout.

- **a.** Users can attempt but fail to sign in correctly five times before Amazon Cognito temporarily locks them out. Lockout time starts at one second and increases exponentially, doubling after each subsequent failed attempt, up to 15 minutes. Amazon Cognito ignores attempts to log in during a temporary lockout period, and these attempts don't initiate a new lockout period. After a user waits 15 minutes, Amazon Cognito resets the temporary lockout. This behaviour is subject to change.
- **b.** Users are logged out after a period of 60 minutes of inactivity.

9. Details of SSO to utilise ADFS.

- **a.** Skillzminer's base solution, being proposed here does not include SSO. This is available as a costed option or as part of one of our other package options.