EssentialSkillz

Overview of Technical and Organisational Measures

Document Reference:	Overview of Technical and Organisational Measures 1.2
Confidentiality Level:	External
Document Owner:	Data Security Officer
Version:	1.2
Date of Version:	03/11/2022
Replaces Version:	1.1
Document Author:	Jason Stirland
Approved by:	Jason Stirland
Date of Approval:	03/11/2022
Reviewed by:	Jason Stirland
Next Review date:	03/11/2023

Revision History

Version	Date	Revision Author	Summary of Changes
(Draft) 1.0	09/04/2020	Jack Rawlings	Created initial draft
1.0	09/04/2020	Jack Rawlings	Approved
1.0	16/04/2021	Liam Carolan	Push review date to Q3 2021 to reflect that will be formally reviewing out AWS infrastructure at that point
1.0	22/09/2021	Liam Carolan	Moved review date to reflect rescheduling of AWS consultation (Q4 2021).
1.1	18/01/2022	Liam Carolan	Moved review date to reflect rescheduling of AWS consultation (Q2 2022). Updated wording in section 4.

Distribution

Location/Holders	Updated/Notified by
Security Documents Folder	Data Security Officer
Internal ISMS page	Data Security Officer
Essentialskillz.com Website	Devops

Approval

Name:	Jason Stirland
Role:	CTO
Signature:	Jason Stirland
Date:	03/11/2022

Table of Contents

1.0 Introduction

1.1 Purpose

The purpose of this document is to provide a high level overview of the information security and data protection measures in place at EssentialSkillz. It is intended as a guidance document. It is not considered to be an exhaustive list, nor should it be considered to constitute part of any agreement.

1.2 Scope

This document is relevant to all accounts hosted on our AWS infrastructure.
Note: As of writing all new clients are to be hosted on AWS

1.3 Users

This document is for the most part intended for use by current and prospective clients. This document is considered **External** and is thus intended to be shared with clients or other external parties. It is visible to all staff, but does not need to be purposefully distributed.

2.0 Reference Documents

- AWS Compliance

3.0 Technical Measures

3.1 C-I-A triad

- **Confidentiality** of access to data. Restricted to IT staff using approved public/private keys.
- Customer databases are segregated to ensure **Integrity.**
- **Availability** and resilience is ensured through our backup policies.

3.2 Backup policy

- Managed database service with automatic failover
- Built-in high availability and durability (multiple copies of database)
- We can also restore data from a backup or perform a point-in-time restore operation thereby minimising any potential data loss to a matter of minutes
- Durability and high availability are built-in to AWS file storage systems

3.3 Building Security

- Customer data is stored and processed on our AWS hosted infrastructure which complies with the highest industry standards

3.4 Disposal

- We retain the data for the duration of the contract, unless the customer would like EssentialSkillz to purge redundant data periodically.
- Office devices are disposed of after hard disk drives have been securely wiped using a low-level zero filling method. Each bit present in the disk is replaced by a zero value, hence the name zero filling - once the data are overwritten with zeros, the process cannot be undone from the hard drive.
- When laptops are retired, they are wiped using the secure erase disk feature of Parted Magic. The IT Administrator confirms that the hard drive has been correctly erased. Laptops are donated to charity or auctioned to employees.
- AWS uses the techniques detailed in DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or NIST 800-88(“Guidelines for Media Sanitization”) to destroy data as part of the decommissioning process.

3.5 Cyber Security

3.5.1 Firewalls

- EssentialSkillz operate a deny-all policy and ports are only opened for specific purposes and for authorised users
- Default usernames and passwords are changed
- Multi-tier protection including network and server firewalls. AWS Shield is also in place on application servers which defends against most common, frequently

occurring networks such as infrastructure (layer 3 and 4) attacks like SYN/UDP floods, reflection attacks, and other DDoS attacks that may target our applications.

3.5.2 Antivirus

- Office hardware is protected by ESET anti-virus software. Application servers are protected by CLAM antivirus software.
- Automatic updates are enabled in both cases.

3.5.3 Encryption

- Personal data is always encrypted in-transit and at-rest
- Customer data at rest is encrypted (AWS) - AWS KMS uses the Advanced Encryption Standard (AES) algorithm in Galois/Counter Mode (GCM), known as AES-GCM. AWS KMS uses this algorithm with 256-bit secret keys.
- Communication between the customer and WorkWize is conducted over HTTPS connection using TLS protocols. HTTP Strict Transport Security (HSTS) is also configured on our production server to ensure that only HTTPS connections can be used.

3.5.4 Application Development

- We proactively monitor application code for vulnerabilities during development and perform an independent third party application penetration test and vulnerability scan.
- Penetration test are performed Annually
- As part of our software development process, developers use tools such as ZAP scanner to continuously monitor changes for OWASP vulnerabilities.

3.5.5 Patches

- Security patches to managed services such as database and file storage are managed by AWS as part of the shared model responsibility. EssentialSkillz performs operating system and application patches which are applied on a quarterly basis or immediately in case of a critical security patch.

3.6 Passwords

- WorkWize passwords can be configured by the customer to set:
    - Minimum length
    - Maximum length
    - Alphanumeric
    - Upper/lower case
    - Enforce special characters
- Default admin passwords must be changed,
- Password hashing uses the Bcyrpt algorithm which is based on the Blowfish cipher
- We provide SSO (SAML 2.0) and recommend our customers to use it where possible for enhanced password security.

4.0 Organisational Measures

4.1 Data Protection Impact Assessment

- Completed an organisation-wide DPIA as part of our GDPR compliance efforts

4.2 Access control

- Elevated or special access privileges, such as system administrator accounts are restricted to a limited number of authorised individuals

4.3 Records and Logs

- Security and event logs are maintained on servers, workstations and laptops.

4.4 Information Security Policies

- EssentialSkillz aligns our procedures and policies with industry standards.
- EssentialSkillz currently maintains Cyber Essentials certified, Cyber Essentials Plus, and IASME Governance Self-Assessed accreditations.
- Information Security policy has been approved by management and communicated throughout the organisation.
- Policies are reviewed on an annual basis

4.5 Business Continuity

- We operate a Business Continuity Plan and Disaster Recovery Policy.
- AWS cloud services are tested in a staggered fashion in order to minimise the potential of impact on customer service delivery.
- Although a single support/account manager may be your point of contact, all our team are fully trained and in the event of the loss of an individual, the support/account manager would be replaced from within our team. We also document all operational procedures, so that an extensive knowledge base is available within the business.

4.6 Risk Assessment

- We have implemented a Risk Assessment and Treatment Methodology which governs Risk Assessments throughout the organisation

4.7 Policies and Procedures

- In conjunction with our Information Security Policy we have implemented a number of policies including, but not limited to:
    - Data Protection Policy
    - Acceptable Usage Policy
    - Privacy Policy

  - Data Breach Policy
  - Business Continuity Policy
  - Disaster Recovery Policy
  - Physical and Environmental Security Policy
- We use WorkWize to roll-out our information security related policies and procedures to employees, including but not limited to Data Protection, Acceptable Use and Privacy policies.

4.8 Awareness and Training

- EssentialSkillz staff undergo regular information security training using our in-house WorkWize Learning Management System. This training includes online courses covering Cyber Security, Phishing Awareness, Internet, Email and Social Media Use as well as GDPR Awareness.

4.9 Due Diligence

- Amazon Web Services (AWS) provides our data hosting platform. AWS are GDPR compliant and maintain a long list of internationally-recognized certifications and accreditations, demonstrating compliance with rigorous international standards, such as ISO 27001 for technical measures, ISO 27017 for cloud security, ISO 27018 for cloud privacy, SOC 1, SOC 2 and SOC 3, PCI DSS Level 1, and EU-specific certifications such as BSI’s Common Cloud Computing Controls Catalogue (C5)

5.0 EssentialSkillz AWS Infrastructure

WorkWize is hosted on the Amazon Web Services (AWS) infrastructure which provides a secure, scalable and reliable technical platform to deliver our services.

5.1 Hosting technology

- AWS Cloud / virtualized hardware using Xen hypervisor technology

5.2 Location / Data Centre

- Client accounts are hosted on one of three AWS locations:
    - Amazon Web Services - Dublin, Ireland
    - Amazon Web Services - London, UK

5.3 Scalability

- On-demand scalable computing resources
- Backed by Amazon's infrastructure, we have access to compute and storage resources as we need them and as our customer base/requirements grow.

5.4 Encryption in transit

- Encryption in transit with TLS across all services.

5.5 Encryption at rest

- All customer data is securely encrypted at rest using built-in KMS

5.6 Disaster recovery

- Highly available architecture (built-in redundancy)
- Recovery time and recovery point is a matter of minutes which minimises any potential loss of customer data.
- Autoscaling of web tier, self-healing database tier, durable storage (s3 and efs)

5.7 Security and patching

- Shared responsibility
- Security patches to managed services such as database and file storage are managed by AWS as part of the shared model responsibility.
- EssentialSkillz perform operating system and application patches.

5.8 Database server

- Amazon Aurora MySQL 5.6
- Built-in high availability and durability

5.9 Database backup

- Managed database service with automatic failover
- Amazon Aurora automatically maintains 6 copies of our data across 3 Availability Zones and will automatically attempt to recover our database in a healthy AZ with no data loss.
- In the unlikely event your data is unavailable within Amazon Aurora storage, we can restore from a DB Snapshot or perform a point-in-time restore operation to a new instance.

5.10 Files backup

- Durability and high availability are built-in to AWS file storage systems.

5.11 IDS / WAF

- WAF programmatically available / IDS from AWS marketplace
- All our customers benefit from the automatic protections of AWS Shield Standard, at no additional charge.
- AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that may target our applications.
- We use AWS Shield Standard with Amazon CloudFront and Amazon Route 53, which provide comprehensive availability protection against all known infrastructure (Layer 3 and 4) attacks.

5.12 Antivirus

- ClamAV with on-access threat detection

5.13 Firewall

- Multi-tier protection including network and server firewalls
- AWS Shield also defends against most common, frequently occurring network and DDoS attacks that may target our applications.

5.14 Certifications

- AWS data centers are certified to the highest industry standards including ISO 27001, ISO 9001, SOC 1, SOC2, SOC3 and Cyber Essentials Plus

5.15 Monitoring and logging

- AWS CloudWatch tools provide server monitoring and performance metrics and ability to set up proactive alerts (billing, technical)
- AWS Trusted Advisor on Cost, performance, security, fault tolerance and service limits
- AWS CloudTrail / CloudWatch with alert notifications, log aggregation options

5.16 Key Management

- Built-in Amazon KMS

6.0 Validity and Document Evaluation

This document is valid as of 09/04/2020.

The owner of this document is the *Data Security Officer* who must check and, if necessary update, the document at least once a year

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- Changes to Technical security measures
- Changes to Organisational security measures
- Updates to AWS infrastructure and configuration