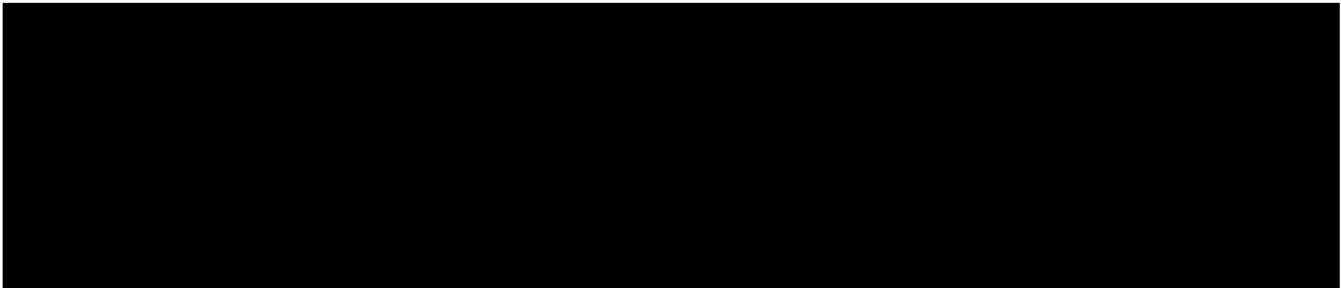





PLAN

ITSM Zone portals can be very quickly deployed, meaning there is a quick set up with no delays to the customer.



AQ9 – EXIT PLAN



SV2 – SOCIAL VALUE: POLICY OUTCOME – INCREASE SUPPLY CHAIN RESILIENCE AND CAPACITY

ITSM Zone is an SME focussed on utilising best practice technology and processes to create, deliver and support e-Learning courses that deliver value to IT Services Professionals.

We are committed to identifying and managing cyber security risks in the delivery of contracts to provide e-Learning. This includes identifying and managing risks within the supply chain.

DIVERSE SUPPLY CHAINS

ITSM Zone works with four Examination Institutes to provide certification exams that provide students with the opportunity to become certified in the qualification that they have studied for.

ITSM Zone also offers a sub-contracted opportunity to

and with

INNOVATION AND DISRUPTIVE TECHNOLOGIES

ITSM Zone takes pride in the use of innovative and new technology to deliver a high-quality learning experience to students. The switch to e-Learning provides a flexible, cost effective alternative to the more traditional classroom environment, and removes the requirement for travel to training venues.

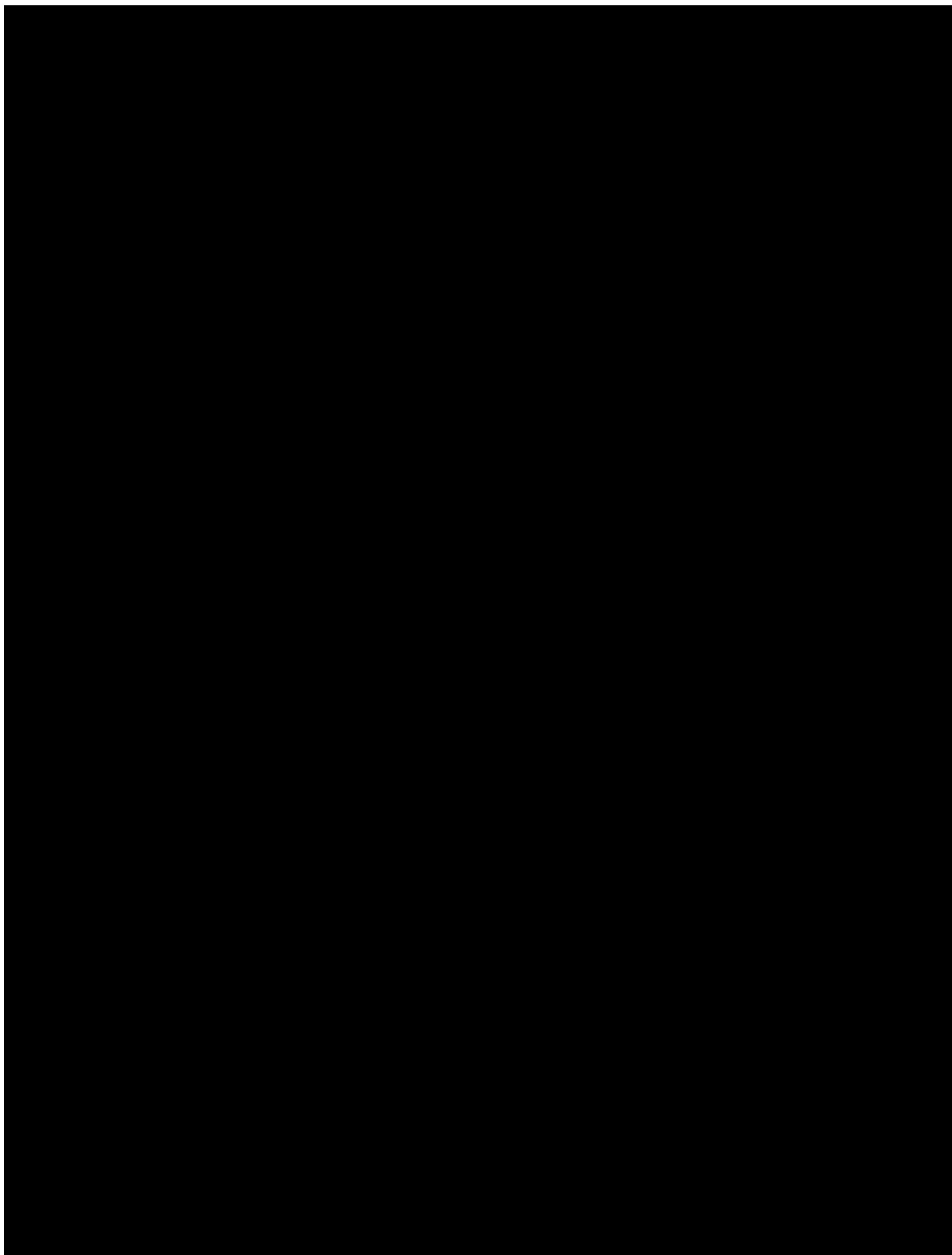
There is a commitment to continually assess new products to the market, and evaluate whether these can be utilised to further enhance our offering.

MANAGE CYBER SECURITY RISKS

ITSM Zone has robust policy and procedure in place, and follows the “10 Steps To Cyber Security” as advocated by the National Cyber Security Centre.

- Risk management regime: We identify and manage risks to our organisation, data and systems. Engaged suppliers have policies and risk management regimes checked. We continually work to mitigate risks to customers and students and policies are reviewed at regular intervals.
- Secure configuration: We identify and baseline technology builds to ensure they have latest security updates. All plug ins are updated to latest version. We remove or disable unnecessary functionality from systems and fix known vulnerabilities. When selecting suppliers, we ensure their security meets required standards.
- Network security is provided with a third-party supplier, on a cloud infrastructure with multiple redundancy built in and is supported and patched to the latest security level. Monthly compliance checks ensure required security patches have been completed.
- Managing privileges: Our team are provided with a reasonable (but minimal) level of system privileges and rights for their role. Privileges are extended to administrators of training portals; allowing them access to only necessary information.
- Education and awareness: ITSM Zone recognise all personnel play an important role in organisational security. Team members have clear guidance on the use of technology and equipment and have cyber security awareness training.
- Incident management: 24/7 monitoring and support is in place.
- Malware prevention: training is provided on malware and the risks that email, downloads, and using the internet pose. ITSM Zone protect customers by clearly providing details of the email address(es) which will be used in the fulfilment of any contract to provide training, so that students can confidently open communications pertaining to courses.
- Monitoring: ITSM Zone have instructed 3rd party hosting with live 24/7 monitoring. Audits ensure that systems are being used appropriately, with any issues or concerns discussed during team meetings.
- Removable media controls: ITSM Zone urge caution when using external media. Where use is unavoidable, media must be scanned for malware before importing onto a business computer.
- Home and mobile working: ITSM Zone’s home working policy allows the flexibility to work from home or office. All team members are issued with company laptop / PC to be used for business purposes only. Training is provided on the risks associated with accessing devices on unsecured networks.
- Working with suppliers: ITSM Zone work with carefully selected suppliers, including Examination Institutes. Appropriate ITSM Zone personnel have access to their systems to issue exam vouchers. During this process, we have identified that we are logging into secure systems and provide only information necessary to have the voucher issued. This removes the need for communication between ITSM Zone and the exam provider by email.
- Keeping customer data secure: ITSM Zone is registered with the ICO and has a GDPR policy in place. Only appropriate student data is entered into the training portal – a student name and email address only.
- Cyber security insurance: ITSM Zone have cyber security insurance in place, provided by Hiscox CyberClear. This is designed to support and protect from evolving cyber threats and risks associated with data, whether electronic or non-electronic.

Annex 4 – Charges (below)



Annex 5

DATA SECURITY – PART A Technical and Organisation Measures

The Supplier is an independent Controller, and recognises that it is responsible for ensuring its processing – including any processing carried out by a Processor on its behalf – complies with the UK GDPR. The Supplier is responsible for taking appropriate technical and organisation measures to manage the data.

The Supplier is responsible for the following:

- **Compliance with the data protection principles:** it must comply with the data protection principles listed in Article 5 of the UK GDPR.
- **Individuals' rights:** it must ensure that individuals can exercise their rights regarding their Personal Data, including the rights of access, rectification, erasure, restriction, data portability, objection and those related to automated decision-making.
- **Security:** it must implement appropriate technical and organisational security measures to ensure the security of Personal Data.
- **Choosing an appropriate Processor:** it can only use a Processor that provides sufficient guarantees that it will implement appropriate technical and organisational measures to ensure their processing meets UK GDPR requirements. This means the Supplier is responsible for assessing that its Processor is competent to process the Personal Data in line with the UK GDPR's requirements taking into account the nature of the processing and the risks to the Data Subjects.
- **Processor contracts:** it must enter into a binding contract or other legal act with its Processors, which must contain a number of compulsory provisions as specified in Article 28(3) of UK GDPR.
- **Notification of Personal Data Breaches:** the Supplier is responsible for notifying Personal Data breaches to the Information Commissioner's Office and, where necessary, other supervisory authorities in the EU, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. It is also responsible for notifying affected individuals (if the breach is likely to result in a high risk to their rights and freedoms).
- **Accountability obligations:** it must comply with the UK GDPR accountability obligations, such as maintaining records, carrying out data protection impact assessments and appointing

a data protection officer. For more information please read our guidance on accountability and governance.

- **International transfers:** the Supplier must comply with the UK GDPR's restrictions on transfers of Personal Data outside the EU.
- **Appointing a representative within the European Union:** If the Supplier is based outside the EU but offer services to or monitor individuals inside the EU, it may need to appoint a representative in the EU.
- **Co-operation with supervisory authorities:** it must cooperate with supervisory authorities (such as the Information Commissioner's Office) and help them perform their duties.
- **Data protection fee:** it must pay the Information Commissioner's Office a data protection fee unless it is exempt.

Without limitation, the Supplier shall comply with UK GDPR, see Chapters 1 to 5 in particular Articles 4(7), 5(2), 13-14, 24-28, 30-37, 44, 46-49 and 82 and Recitals 58-61, 73-74, 78-79, 80-89, 97, 101, 108-110 and 146.

DATA SECURITY - PART B

DSP Toolkit and ISO Standards

1. It is the Department of Health and Social Care's policy that all organisations which process NHS patient information must provide security assurance through annual completion and publication of the Data Security and Protection (DSP) Toolkit (<https://www.dsptoolkit.nhs.uk>).
2. To provide assurance that good information governance practices are being maintained, the Supplier must demonstrate, and will allow NHS Digital to audit, that it:

A) meets or exceeds the DSP Toolkit standards required by NHS Digital for their organisation type organisation code in the DSP Toolkit;


If A does not apply, B and/or C, as the Data Discloser may require and specify in writing:

B) is certified against international security standard ISO 27001;

and/or

C) has other security assurance in place which, without prejudice to any other elements of such assurance, meets the requirements below.

3. In cases where the Supplier has not completed a DSP Toolkit assessment to the NHS Digital's satisfaction and where the Supplier is not ISO 27001 certified, the Supplier must ensure that it meets the requirements set out in clause 3 of this Part B of Schedule 2, which NHS Digital reserves the right to audit.
4. Where the Supplier has provided information in writing about what other security assurance it has in place, and without prejudice to the Supplier's other obligations under this agreement, the Supplier shall:
 - process Personal Data only for the provision of health care or adult social care, or the promotion of health, and only for purposes described in this agreement, and which are consistent with the purposes recorded in the Supplier's data protection registration with the Information Commissioner's Office;
 - request and process the minimum data necessary (e.g. using age range rather than age if sufficient);
 - deploy secure processes, procedures, practice and technology for storage and access, commensurate with the Personal Data being Processed;
 - ensure the rights of Data Subjects are met, such as satisfying subject access requests received, ensuring data accuracy and correcting errors, and handling objections and complaints;
 - permanently destroy/delete or erase the Data once it is no longer required for the purpose for which it was collected and confirm destruction to the NHS Digital;

- 
- ensures all Supplier Personnel with access to Personal Data provide a written undertaking that they understand and will act in accordance with the Data Protection Laws, will not share passwords, and will protect the confidentiality of the Personal Data;
 - report immediately to the Data Discloser any security incidents relating to the Data, and any instances of breach of any of the terms of this agreement; and
 - comply with any specific legislation in relation to the Data (such as the Statistics and Registration Services Act 2007).