

Registered Company Name	Niche Science & Technology Ltd
Company Registration No.	3545417
Registered Company Address	Unit 26 Falstaff House Bardolph Road Richmond TW9 2LH
Company Website	www.niche.org.uk
Main Contact Name	Ben Stevenson
Main Contact Job Title	Quality and Training Officer
Main Contact Email Address	Ben.stevenson@niche.org.uk

1. GENERAL COMPANY INFORMATION

Years business was started	1998
Current number of employees	Between 28–32
Staff turnover in the last 3 years	10%
Briefly describe the services NST provide:	Clinical Operations: • Full service clinical project management • Monitoring • eTMF management Medical Writing: • Regulatory document development • Regulatory affairs • Manuscript preparation and review Quality Management: • Full service quality management • SOP/Policy development • Ad hoc advice More details can be found at www.niche.org.uk
Do NST have professional indemnity and public liability insurance?	☒ Yes ☐ No Details can be provided upon request.

2. QUALITY

Do NST have a documented Quality Management System (QMS)?	Yes
Is NSTs QMS certified to ISO 9000?	☐ Yes ☒ No NST QMS is based on ISO 9000 but is not accredited.
Is NSTs QMS based on any recognised standard (e.g., GCP)? If so, please specify which standard.	☒ Yes ☐ No GCP
Please describe how NSTs QMS is managed	NST QMS is managed by a dedicated Quality and Training officer. This function is independent of the other NST departments. NST policies and SOPs are reviewed every two years to ensure compliance with applicable regulations and guidelines. All policies and SOPs are formally approved by the Managing Director, Head of Department or a Team Leader. Internal audits are conducted to ensure compliance with SOPs and these follow the NST annual audit programme. CAPAs are managed and tracked to ensure timely implementation. A list of NST SOPs can be made available on request, specific SOPs can also be shared on request.
Do NST have a Quality Department?	☒ Yes ☐ No
If yes, how many staff are in this department?	1 full time member of staff plus a representative from each department.
Have NST been inspected by a regulatory authority (e.g., MHRA)?	☒ Yes ☐ No MHRA Dec2011–Jan2012 – no critical findings
Does NST have a Risk Management policy and/or documented processes for the management of risk?	☒ Yes ☐ No
3. TRAINING	
Please describe NSTs training processes:	All personnel complete an induction training programme when they join the company. This covers company systems, relevant procedures, and role-specific responsibilities to ensure employees are properly trained to perform their job-related activities.

	Policies, SOPs and Guidance Documents are read and understood by employees. Core training is provided by external e-Learning providers (e.g., GCP, GDPR, cyber security) In-house training and role specific training is followed by an assessment and the individual receives a certificate of successful completion.
How is NSTs training recorded?	All staff members are trained on the relevant SOPs as determined by the NST Curriculum. Training acknowledgement forms are signed by all individuals for which the SOP is mandatory. All other training is recorded in the individual's training record which is maintained by the employee and reviewed at least annually by the Quality and Training Officer. For mandatory training delivered in-house all attendees sign an attendance record.
How frequently do NST staff undergo GCP training?	All staff complete GCP training following employment with NST. The Clinical Operations department completes the commercial training every 2 years. The MW team receives in-house refresher training annually.
What GCP training course do NST use?	Whitehall training In-house slides delivered by the Quality and Training Officer.
What professional bodies are NST staff members of?	RQA EMWA AHPPI EUFEMED
4. CONTRACTS AND SUBCONTRACTING	
Do NST use subcontractors?	NST do not use subcontractors for standard delivery of client projects. However, in the case of full-service project management NST may engage with subcontractors on behalf of the Sponsor. In which case, all subcontractors will be validated following the NST service provider selection and qualification process.
5. FACILITIES	

Please describe the facilities where tasks are carried out:	NST has an office in Richmond, London. However, the NST team are primarily remote workers. All project tasks will be complete remotely with the exception of monitoring visits.
What security systems are present?	The office has restricted access with a lockable entry door and burglar alarm system.
What fire prevention systems are in place?	Company premises are equipped with fire detection systems, including smoke detectors and fire alarms, to ensure early identification and response in the event of a fire.
Do NST have a Disaster Recovery Plan documented in a policy or SOP?	☒ Yes ☐ No
Please specify when NSTs Disaster Recovery Plan was last tested	The DRP and BCP is tested annually, usually in Q1 of the year.
Do NST keep hard copies of client/clinical trial documents on site?	☐ Yes ☒ No
What is the retention period for the storage of client/clinical trial documents?	All NST generated records relevant for a clinical trial are retained for 25 years.
Describe NSTs system for the storage of electronic documents:	All NST electronic records are stored on the NST secure SharePoint.
6. COMPUTERISED SYSTEMS	
List the computerised systems NST use:	VieDoc – latest version and release notes can be found here: Release Notes Viedoc Validation package can be provided on request Microsoft 365
Describe NSTs computer validation processes:	Systems are validated through a documented process within the company's Quality Management System. Proposed systems are assessed against user and functional requirements and undergo vendor assessment. Off-the-shelf systems are validated through installation, operational, and performance qualification testing, while custom systems may be validated by a Computer System Validation (CSV) specialist in line with GAMP principles. NST do not currently use any custom systems.

	Validation outcomes are reviewed and approved by management, users are trained before use, and all documentation is maintained within the QMS.
Describe NSTs back-up processes:	NST SharePoint is backed up 3 times per day.
Describe NSTs electronic archiving processes:	Project files are archived or deleted in accordance with client instructions. Where no specific instructions are provided, completed project files are moved to a designated archive area within the company's secure SharePoint environment to maintain an organised active project workspace.
Do NST comply with the 21 CFR Part 11 requirements for electronic signatures?	☒ Yes ☐ No NST uses DocuSign to comply with 21 CFR Part 11 requirements.
7. IT, CYBER SECURITY AND DATA PROTECTION	
Does the company have a formal information security policy or set of policies in place?	☒ Yes ☐ No
Are all NST members of staff trained in GDPR and cyber security?	☒ Yes ☐ No e-Learning for GDPR and cyber security is completed annually.
How often is the company's information security strategy reviewed?	At least every 2 years.
Summarise the controls in place to limit physical access to datacentres, or any other areas where systems and data are stored or processed:	Data is stored within secure cloud environments (Microsoft SharePoint / Microsoft 365) hosted in professionally managed data centres operated by the provider, where physical access is restricted to authorised personnel and controlled through established security measures. Within Niche, access to systems is limited to authorised staff using company laptops. Access is controlled through individual user accounts, strong passwords, multi-factor authentication (MFA), and pre-approved, role-based permissions to ensure only personnel with a legitimate business need can access the data.

What data will NST process?	The company will process, access, and store information necessary to deliver the contracted services. This may include study documentation, project-related communications, operational data, and other materials provided by the client for the purpose of supporting the project. Access is limited to authorised personnel and used solely for the delivery of the agreed services. We do not intend to store PII, as we assume that all data provided will be at least pseudonymised.
Does NST comply with UK/ EU data protection requirements?	☒ Yes ☐ No
Is NST ISO 27001 accredited?	No, but our IT management service provider are accredited.
Does NST hold a Cyber Essentials certificate	Yes, NST is Cyber Essentials certified.
Who at NST is responsible for system and information security?	Ammar Moussa, Business Manager
Do NST staff sign non-disclosure agreements?	All personnel are subject to confidentiality obligations through clauses included in their employment contracts, which require them to protect confidential and client information.
Is all data storage and processing (including cloud storage) located within the UK and/or EU?	☒ Yes ☐ No
7. CLOUD SECURITY	
What standard does NSTs cloud provider follow?	Microsoft SharePoint (Microsoft 365) complies with ISO 27001, ISO 27017, ISO 27018, and SOC 1/SOC 2. It also supports GDPR-compliant data handling.
What controls are in place to protect NSTs cloud data in transit?	Data is transmitted via Microsoft 365/SharePoint, which uses encrypted HTTPS/TLS connections to protect data in transit. Access is further secured through password-protected accounts and multi-factor authentication (MFA).

Where is the cloud data stored physically?	Data is stored within Microsoft 365 / SharePoint cloud infrastructure, hosted in data centres located in the UK or EU, in accordance with Microsoft's regional data storage policies.
What measures are there in place to access cloud data upon request?	Authorised personnel can access cloud data via secure login to SharePoint, using individual credentials and multi-factor authentication (MFA). Access permissions are managed and granted based on role and project requirements.
What measures does NSTs cloud provider have in place to guarantee availability?	Microsoft 365 / SharePoint includes built-in redundancy, high availability architecture, and regular backups managed by Microsoft. This infrastructure is designed to ensure continuous availability and rapid recovery in the event of system failures.
How are NSTs cloud services separated from other tenants?	Data is separated through Microsoft's "tenant isolation controls", ensuring that our organisation's data is accessible only to authorised users within our tenant environment.
What tools are used on the cloud service to monitor and audit logs?	Monitoring and audit logging are performed using the built-in Microsoft 365 / SharePoint audit and activity logging tools, which record user access, file activity, and administrative actions. These logs can be reviewed by authorised administrators to monitor system activity and investigate potential security issues.