Supplier Questionnaire: Information Security

Please provide a detailed response to each question. For questions that are not applicable to the services provided to New College Durham please mark the question as "N/A" and provide an explanation.

Part 1: Document Control

Name & Address:	
Assessment Completed by:	
Date of assessment:	

Part 2: Policy Compliance

Control Area	Control Question	Supplier response
Security Policies	Does your organisation have a documented information security policy?	
	What accreditation do you currently hold? (ISO standards, Cyber essentials etc.)	
	Are all security policies and standards readily available to all users (e.g., posted on company intranet)?	
	Tick the security areas which are addressed within your information security policies and standards: ☐ Acceptable Use ☐ Remote Access / Wireless ☐ IT Security Incident Response ☐ Data/System Classification ☐ Third Party Connectivity ☐ Physical Security ☐ Network/Perimeter Security ☐ Other: ☐ Data Privacy ☐ Access Control ☐ Encryption Standards ☐ Anti-Virus ☐ Email / Instant Messaging ☐ Personnel Security ☐ Clear Desk	

Part 3: Detailed Security Control Assessment

Control Area	Control Question	Supplier response
Organisational Security	Have the security policies, standards, and procedures been audited by an external agency?	
	What exterior security is provided (i.e. gates, secure vehicle access, security cameras, etc.)?	
	Describe the physical security mechanisms that prevent unauthorised access to your office space, user workstations, and server rooms/data centres?	
	Are all critical equipment and assets located in a physically secure area?	
	What type of fire suppression systems are installed in the data centres?	
Environmental	Do you have business continuity and disaster recovery processes?	
	Do you have a maintenance process for the facilities?	
	Are the systems configured to record system faults?	
	Do you have a formal media destruction policy?	
	Are logs maintained that record all changes to information systems?	
Communications and Operations Management	Describe how changes are deployed into the production environment.	
	If you use a third-party contractor to maintain your systems, is the contractor subjected to a vetting process?	

	How do you protect your systems against newly-discovered vulnerabilities and threats?	
	Do you prevent end users from installing potentially malicious software (e.g., list of approved applications, locking down the desktop)?	
	Do you scan traffic coming into your network for viruses and threats? Do you employ systems such as Cloudflare?	
	How would you protect the confidentiality and integrity of data between our two organisations	
	Are system documentation (network diagrams, ip ranges, configuration guides, etc.) secured from unauthorised access?	
	Are backup procedures documented and monitored to ensure they are properly followed?	
	Describe how you protect information media (e.g., back-up tapes) that may be shipped offsite.	
	Are new employees vetted before being granted access to secure resources?	
Access Control	Do you have account and password policies	
	Are failed login attempts recorded and reviewed on a regular basis?	
	Describe your authentication methods used for external Connections (VPN, MFA etc).	
	Do you conduct periodic checks on users' access to ensure their access matches their responsibilities?	

	Describe how you segment your network (i.e. security zones, pLans, DMZs, etc).	
	Do you enable MFA on any remote administration capabilities on servers?	
	Do workstations or production servers use Host Intrusion Prevention/Detection of Firewall software?	
Information Security Incident Management	After an incident, are policies and procedures reviewed to determine if modifications need to be implemented?	
	Are incident reports issued to appropriate management?	
Business Continuity Management	Has an organisational disaster recovery plan coordinator been appointed	
	Has a scenario to recover normal operations been tested?	
	Is a copy of the Disaster Recovery Plan stored at the backup site and updated regularly?	
	Are contingency arrangements in place should they be required?	
Compliance	Are the security policies and procedures routinely tested?	
	Are audit logs or other reporting mechanisms in place?	
	Are audits performed on a regular basis?	
	Is someone responsible for managing audit results?	