Appendix A – General Security Questionnaire

SUPPLIER DETAILS	
Supplier Name	The Clinical Informatics Research Unit, Faculty of Medicine, University of Southampton
Supplier Address	The CIRU, Care of the National Blood and Transplant Service, MP 852, Coxford Road, Southampton, SO16 5AF, UK
Supplier Email Address	edge@soton.ac.uk
Supplier Phone Number	+44 (0)23 82027 200
Supplier Websites	www.southampton.ac.uk (Parent Organisation Website) www.the-ciru.com (Department Website) www.edgeclinical.com (Marketing Website) www.au.edge-clinical.org (Australian Application) www.edge-canada.ca (Canadian Application) www.be.edge-clinical.org (Belgium Application) www.in.edge-clinical.org (Indian Application) www.nz.edge-clinical.org (New Zealand Application) www.sa.edge-clinical.org (South Africa Application) www.edge.nhs.uk (UK Application)
Supplier Data Protection Officer Contact	The Data Protection Officer Legal Services University of Southampton, Highfield Southampton, SO171BJ, UK
Supplier ICO Registration Number	Z6801020
Supplier DSP Toolkit Identifier	EE133879-CIRU

Appendix A – General Security Questionnaire

Supplier Cyber Essential Identifier	**IASME-CE-003619**
No. of Staff employed by supplier	**The University of Southampton: 6000** **The Clinical Informatics Research Unit: 47**
How long has the supplier been providing services?	**The Clinical Informatics Research Unit has been operating within, and providing services to the UK and International healthcare organisations for over 23 years.**

Appendix A – General Security Questionnaire

SYSTEM / APPLICATION DETAILS	
System Name	EDGE
Latest version of the system	V3.2 (15/05/2023)
Next upgrade	V3.2.1 (Release Date: TBC)

ROLES, RESPONSIBILITIES & DEFINITIONS	
Data Subjects	An individual who is the subject of personal data All EDGE End Users and participants are defined as Data Subjects
Data Controller	A person / legal entity who (either alone or jointly or in common with others) determines the purposes for which and the manner in which any personal data are, or are to be, processed The legal entity subscribing to the EDGE licence is defined as the Data Controller
Data Processor	Any person / organisation (other than an employee of the data controller) who processes the data on behalf of the data controller The University of Southampton and its third party supplier are the Data Processors

APPLICATION IDENTITY AND USER ACCESS MANAGEMENT	
How does the supplier manage standard user accounts?	User account management is the responsibility of the subscribing organisation's local EDGE Administrator (Data Controller).
How does the supplier manage privileged user accounts?	Privileged account management is the responsibility of the subscribing organisation's local EDGE Administrator (Data Controller).
What is the authentication method to access the system as an Administrator or a User?	Username and Password
Are password policies defined and enforced?	Yes Password change frequency is defined by the subscribing organisation (Data Controller) as either: • 30, 60, 90, 180, 360 days (by default 180 days) Password criteria: • At least 1 upper case letter (A-Z) • At least 1 lower case letter (a-z) • At least 1 number (1-9) or special character / symbol (!$&#~) • At least 8 characters in length EDGE utilises API's with password breach databases to identify the use of passwords which are insecure. Any password identified as insecure will be rejected by the system.
Are secure password reset procedures defined and implemented?	Yes
Is failed element (username/password) identified to user?	No
Failed password attempts before user account is locked	Three failed attempts

APPLICATION AUDIT LOG	
What actions are captured in the System Audit Log?	The EDGE audit log captures the following items: • Time and date of action • User performing the action • The type of action and context performed • Data change / action The types of action which the audit log will capture are: • Create • Delete • Insert • Merge • Update • Reorder
What period do the audit logs cover?	Audit logs cover from the start of the organisations use of EDGE. Audit log from previous version of the application are made available on request.
Who can access the audit logs?	Any End-User who has been provided with Administrative permissions can access and query the audit log.

Appendix A – General Security Questionnaire

DATA STORAGE AND MANAGEMENT	
Is the application stored in Public or Private Cloud?	Public Cloud
Where will the data be stored?	Microsoft Azure Data Centre in instance-specific geographies
What is the physical geographic location of the data?	EDGE Australia – Azure - New South Wales, Australia (Sydney) EDGE Belgium – Azure – Western EU, Netherlands (Amsterdam) EDGE Canada – Azure – Canada East (Toronto) EDGE India – Azure – India West (Mumbai) EDGE New Zealand – Azure - New South Wales, Australia (Sydney) EDGE South Africa – Azure – South Africa West (Cape Town) EDGE United Kingdom – Azure – UK South (London)
Which jurisdiction is the supplier / CSP subject to?	UK Law
Can the subscriber data be given to or shared with third parties and used for purposes other than the provision of service without the tenant's consent?	No – See EDGE Privacy Policy - https://edgeclinical.com/privacy

THIRD PARTY SUBCONTRACTORS / DATA PROCESSORS	
Does the supplier use any third parties to process data on their behalf?	Yes

TELEFONICA TECH UK	
Head Office Address	Trinity Building, 39 Tabernacle Street, Shoreditch, London, EC2A 4AA
Services	Cloud Solution Provider for MS Azure Infrastructure
Data Processed	EDGE Database
GDPR Compliance	Yes Click Here for GDPR Compliance
Data Retention Period	In line with subscriber EDGE Contract & SLA
DPA Signed with the CIRU	Yes
Privacy Policy	Yes Click Here for Privacy Policy
Accreditations	ISO 27001, ISO14001, ISO 20000, ISO 22301, ISO 9001, ISO 27017, DSP Toolkit, Cyber Essentials
Website	https://telefonicatech.uk/

MICROSOFT AZURE	
Head Office Address	Microsoft Campus, Thames Valley Business Park, Reading, RG6 1WG
Services	Cloud Data Centre Hosting
Data Hosting Location	UK, EU, Australia, India
Data Processed	EDGE Database for applicable geographic location instances
GDPR Compliance	Yes Click Here for GDPR Compliance
DPA Signed with the CIRU	Yes (via Telefónica Tech UK)
Data Retention Period	In line with the subscriber's EDGE contract & SLA
Privacy Policy	Yes Click Here for Privacy Statement
Accreditations	ISO 9001, ISO 27001, ISO 27018, ISO 27017, ISO 22301, SOC 1 Type 2, Soc 2 Type 2, SOC 3, CSA Level 1, DSP Toolkit, Cyber Essentials
Website	https://azure.microsoft.com/en-gb/

SALESFORCE	
Head Office Address	Lotus Park, 2 The Causeway, Staines, TW18 3AG
Services	SAAS Help Desk and Customer Relationship Management Software
Data Hosting Location	SFDC EMEA Data Centre Limited, CS110 Datacentre, Floor 26 Salesforce Tower, 110 Bishopsgate, London, EC2N 4AY
Data Processed	End User Name / Email Address
GDPR Compliance	Yes Click Here for GDPR Compliance
DPA Signed with the CIRU	Yes
Data Retention Period	180 Days

Privacy Policy	**Yes Click Here for Privacy Policy**
Accreditations	**ISO 27001 / 27017 / 27018, SOC 1 & SOC 2 Type 2 Reports**
Website	**https://compliance.salesforce.com/en/**

SENDGRID UK (TWILIO)	
Head Office Address	41 Corsham Street, Hoxton, London, N1 6DR
Services	Transactional email service to enable EDGE service delivery e.g. Password Resets
Data Hosting Location	6th Floor One London Wall, London, EC2Y 5EB
Data Processed	End User Email Address
GDPR Compliance	Yes Click Here for GDPR Compliance
DPA Signed with the CIRU	Yes
Data Retention Period	61 Days
Privacy Policy	Yes Click Here for Privacy Statement
Accreditations	ISO 27001 / 27017 / 27018, SOC 2 Type 2 Reports
Website	https://sendgrid.com/policies/security/

ACTIVE CAMPAIGN	
Head Office Address	Suite 03-101, 160 Shelbourne Road, Dublin, DO4 E7K5
Services	Marketing and Service Alert Emails e.g. Conference Invitations & Surveys
Data Hosting Location	TBC
Data Processed	End User Email Address
GDPR Compliance	Yes Click Here for GDPR Compliance
DPA Signed with the CIRU	Yes
Data Retention Period	61 Days
Privacy Policy	Yes Click Here for Privacy Statement
Accreditations	ISO 27001 / 27017 / 27018, SOC 2 Type 2 Reports
Website	https://sendgrid.com/policies/security/

SUPPLY CHAIN / SUBCONTRACTOR MANAGEMENT	
Does the supplier use the services of any third parties / subcontractors for the provision of services?	Yes (See THIRD PARTY SUBCONTRACTORS / DATA PROCESSORS section)
Will the supplier inform the subscriber of the third parties / subcontractors?	Yes through the EDGE Contract and through application specification documents
Will the supplier inform the subscriber of changes to third parties / subcontractor during the life of the contract?	Yes through written notification

DOCUMENTATION	
Does the supplier have a Data Protection Policy?	Yes from The University of Southampton
Does the supplier have an Information Security Policy?	Yes from The University of Southampton
Does the supplier have an Incident Management Procedure and Policy?	Yes from The University of Southampton

Appendix A – General Security Questionnaire

INDEPENDENT AUDITS	
Does the data hosting provider have an approved Information Security Policy?	https://docs.microsoft.com/en-us/azure/security
What is the hosting provider availability?	99.982% (Tier 3 equivalence)
How frequently is the supplier and its third parties / subcontractors audited by an independent third party?	The University of Southampton Annual Audits: Cyber Essentials, DSP Toolkit, EDGE Penetration Test Microsoft Azure Annual Audits: ISO 9001, ISO 27001, ISO 27018, ISO 27017, ISO 22301, SOC 1 Type 2, Soc 2 Type 2, SOC 3, CSA Level 1, CCM v3, Penetration Test https://docs.microsoft.com/en-gb/azure/compliance/ Salesforce Annual Audits: ISO 9001, ISO 27017, ISO 27018, NEN 7510, SOC1, SOC 2, SOC 3, Cyber Essentials Plus, Penetration Test SendGrid (Twilio) Annual Audits: ISO 27001 / 27017 / 27018, SOC 2 Type 2 Reports, Penetration Test Active Campaign Annual Audits: ISO 9001 / ISO 27001, SOC 2 Type 2 Reports, Penetration Test

RISK MANAGEMENT	
Does the supplier undertake a regular security risk assessment and take steps to mitigate any risks identified?	Yes The CIRU reports to the Data Protection Impact Assessment panel of the University of Southampton on an annual basis and makes an annual DSP toolkit submission. Threat Risk Analysis (TRA) and Risk Assessments are embedded within the departments Standard Operating Procedures (SOP's) for Operational Deployment and as part of the Software Development Lifecycle.

VULNERABILITY MANAGEMENT	
Is there a patch management process implemented by the cloud service?	Yes Patch management cycles for Day 14 and Day 0 patches are managed by the Cloud Services Provider.
Is there a patch management process implemented by the application?	Yes Patch management cycles for Day 14 (low) and Day 0 (high) patches are managed through the EDGE development SPRINT process.
Is the database encrypted at rest?	Yes Data is encrypted to AES 256
Is the data encrypted in transit?	Yes TLS 1.2 and above

SUPPORT	
Does the supplier offer a support contract for the system?	Yes Level 1, 2 and 3 support as per the EDGE application contract or Service Level Agreement.
What are the contracted support hours?	Monday to Friday 8am – 5pm UK time, excluding UK public holiday and the University of Southampton closure days.
Support Contract end date?	As per the subscriber's contract
How many environments does the EDGE application have?	There are three subscriber-facing environments for EDGE: LIVE (Production) DEMO (Training and Demonstration) UAT (User Acceptance Testing)

BACK UP AND DISASTER RECOVERY	
Does the supplier have an approved Disaster Recovery Plan?	Yes Disaster Recovery is managed by CIRU in conjunction with Telefónica Tech services management and Microsoft Azure Security Controls.
How often is the data backed up?	Full back up every 24 hours. Transactional back up every 30 minutes.
How often is the back-up mechanism tested?	An automated test restore from the back-up database is performed quaterly. A manual back-up and restore is performed annually.
Are back-ups stored off site?	Back-ups are sent to co-located failover facilities every 24 hours.
What are the Service Level Agreement RTOs and RTPs?	Recovery Time Objective: 24 Hours Recovery Point Objective: 30 Minutes

BUSINESS CONTINUITY	
Does the supplier hold an Incident Management / Business Continuity Plan?	Yes
How frequently does the supplier test their Business Continuity / Disaster Recovery Plans?	At least annually
Does the hosting supplier hold an Incident Management / Business Continuity Plan?	Yes
How frequently does the hosting supplier test their Business Continuity / Disaster Recovery Plans?:	At least annually

PERFORMANCE	
How frequently does the supplier report to the subscriber on performance?	Quarterly through Account Management Meetings
What advance notifications will you provide prior to any changes or interruption to the service?	Where possible, notification of service interruption or downtime will be advised with five days' notice. Any changes to the service will be notified in line with the EDGE application subscriber contract. For release notes to system updates 7 days' notice will be provided

INCIDENT MANAGEMENT	
In the event of an Information Security incident, would the subscriber deal directly with the supplier?	Yes – The subscriber would deal directly with the University of Southampton.
What are your incident response and resolution times?	For full details, please see the EDGE application Service Level Agreement. Critical / Major / Minor

TERMINATION & EXIT	
Upon contract termination notice, will an 'Exit Manager' be designated by the supplier for the notice period?	Yes The subscriber's Account Manager will also provide Exit Manager services upon contract termination notice.
What exit management requirements will be required from the subscriber?	The subscriber will need to provide supplier with: - Exit Management Transition Schedule - Exit Management Data Extraction Format and Requirements
Will the supplier remove all subscriber data from the database and back-ups upon termination of service?	Yes – Data will be removed within 60 days.
Will the supplier issue a Data Destruction Certificate to confirm removal of all subscriber data?	Yes – Upon contract termination, the data destruction process will be initiated and a certificate with be issued within 60 days.