WWW.EIS.CO.UK

EIS is the trading arm of
Cantium Business Solutions Ltd.

Company House Number: 11242115

Cybersecurity Support and Consultancy

Service Definition Document

Cloud Support

RM1557.15

Version: 1.0

OFFICIAL

1. Introduction

1.1. Cybersecurity Support and Consultancy with EIS

EIS (the trading arm of Cantium Business Solutions Ltd.) can help your organisation to rethink and optimise your entire cybersecurity posture.

We understand that cybersecurity is one of the most resonant issues affecting modern organisations. When threats are always present, you can benefit from industry-leading support and consultancy to maintain robust and secure systems.

Our Security Operations Centre will work with you to improve your cybersecurity and resilience, shifting from a position of reactivity to one of proactivity. We can identify your potential points of weakness and advise your ongoing strategy, improving your ability to detect and resists cyberattack.

Protect your assets and minimise risk to your infrastructure with EIS.

1.2. Features and Benefits

Features	Benefits
• Security Audits. • CIS Benchmarking levels 1&2 • Cyber Essentials Plus, PSN CoCo, and PCI-DSS. • NCSC MailCheck/ MyNCNS Service available. • Advice on email, web filtering, and firewalls. • Advice on VPN, MFA, SSL certificates, domain names, DNS. • Implementation of TLS, SPF, DKIM, and DMARC. • Vulnerability scanning and health checks. • Vulnerability remediation and system-hardening advice. • Endpoint security and perimeter network security. • Device isolation • Cyber training for users	• Assess cyber security maturity levels and quantify cyber risk. • Identity security weaknesses in networks. • Identify security weaknesses in applications, domains, devices, and users. • Increased confidence in security controls and cyber response procedures. • Improved ability to detect, resist and respond to cyber-attack. • Meet compliance requirements. • Detection of vulnerabilities. • Support for remediation of vulnerabilities. • Guidance on achieving accreditation. • Ensuring security of email domains. • Helps reduce user behaviours becoming a vulnerability risk

1.3. About Us

As a Local Authority owned trading organisation (LATCo) and wholly owned by Kent County Council, EIS (the trading arm of Cantium Business Solutions Ltd.) has over 35 years' experience supplying IT services to the Public Sector. As such, we have

developed a comprehensive managed service portfolio, built alongside a strong partner network, to support and complement the services we deliver in-house.

We are in the privileged position of being part of a collection of sister companies under the Commercial Services Group which provides us with access to a network of LATCos, all with a joint focus on improving services within the Public Sector. The Commercial Services Group consists of thirty-three trading brands offering a wide range of services to the Public Sector, from legal and procurement services to education advice, supplies and energy procurement.

Our highly experienced and dedicated teams, consisting of over 300 ICT specialists, provide advice, guidance and support to over 33,000 users. With a customer base of over 700 organisations across the Public, Private and Education sectors, EIS offers a range of ICT services tailored to our customers' individual needs, including fully managed Operational, Security, Professional and Network Services.

As a Local Authority owned business, we are in the unique position to truly understand the Local Government landscape. We appreciate the budget restraints faced within the Public Sector and the delicate balance between implementing new technologies and innovations, whilst ensuring the vital public services remain robust and unaffected by change.

- The Public Sector is part of EIS's DNA.
- Wholly owned by Kent County Council with our profits staying in the public sector.
- Successfully traded for over 35 years both as part of the Local Authority and as a standalone company.
- Experienced at delivering back-office services to a diverse range of customers.
- Commercially astute with a collaborative, partnership-based ethos and approach.
- ICT and Professional partner to over 700 organisations including local authorities, central government, NHS trusts, Multi-Academy Trusts and colleges.

Customer experience is at the heart of what drives us as a business, which has been solidified in our recent glowing report from our Customer Service Excellence (CSE) accreditation. CSE is a diagnostic tool and benchmark for excellent customer service and EIS has proved the very essence of the requirements in the CSE standard; that the customer is truly at the heart of what we do.

2. Service Management

2.1. SLA, Including Support Hours and Availability

We deliver a standard support service to the following SLAs:

Priority	Response Target	Resolution Target	Description
P1	20 Business Minutes	6 Business Hours	Complete loss of service
P2	1 Hour	10 Business Hours	An issue that results in a degradation/ loss of service affecting over 50% of users
P3	1 Business Day	3 Business Days	An issue that results in a degradation/ loss of service affecting more than one user but less 50% of users
P4	1 Business Day	4 Business Days	An issue that results in a degradation/ loss of service affecting one user
P5	Business Days	5 Business Days	A non-service affecting issue, eg, name or hunt group incidents

2.2. Service Desk Availability

Helpdesk Support	Availability
Telephone Support	08:00 to 17:30 (UK time), Monday to Friday excluding English Bank Holidays
Email Support	08:00 to 17:30 (UK time), Monday to Friday excluding English Bank Holidays
Web Chat	08:00 to 17:30 (UK time), Monday to Friday excluding English Bank Holidays

2.3. Service Constraints

There are no constraints applicable to this service.

2.4. Training and Support / Consultancy

Any training necessary for the deployment of this solution can be discussed with our Onboarding team as part of your ongoing support and consultancy service.

EIS provides a comprehensive training programme of Cybersecurity expertise, designed to train a range of users including administrative, financial, and managerial staff. Training can be provided in bespoke sessions designed around your individual requirements.

2.5. Financial Recompense for not meeting Service Levels

Please refer to EIS's terms and conditions of sale for financial recourse arising from default by either party. Service credits are not included in this framework offer, unless defined within the service or product Service Level Agreement (SLA).

3. Onboarding and Offboarding

3.1. Onboarding

EIS prioritises establishing a clear and effective onboarding strategy with every new customer. We will ensure that every migration to a new application, software, or service is performed with the least possible disruption and highest possible satisfaction.

We make every effort to be as transparent as possible during the Onboarding process.

From EIS's Onboarding Team, you will be appointed a dedicated Onboarding Officer. The onboarding process will begin with a Project Initiation Meeting, the launchpad for your Cybersecurity Support and Consultancy service with EIS. With EIS's support, your migration will be kept as simple as possible. We will develop a suitable governance framework, enabling delivery teams to implement the solution in a clear, simple fashion.

Following the initial meeting your Onboarding Officer will also set up regular project calls with you and any relevant members of the EIS team to help keep the project on track, update stakeholders on progress and highlight any areas of concern.

Onboarding is where we have our first opportunity to establish a great relationship with our customers; put simply, we know that first impressions matter. Our onboarding approach covers five key steps, as shown below:

3.2. Implementation Plan

From day one, EIS will work with you in order to respect your needs and requirements.

We will work together to outline your aims, create an implementation plan, and establish stakeholders in order to keep the Onboarding process as transparent as possible.

EIS's experience and expertise combine to create a truly bespoke service for your organisation. Using industry-leading, proven methods, we can work hand-in-hand with you to take your ICT Services to the next level.

We will work with you to create a bespoke support plan that caters to your organisation's individual needs.

EIS will work with you to understand your existing processes and where they can be improved to maximise the performance of your Cybersecurity solution. Your configuration set will be delivered in line with your priorities as part of the overall project scope.

Your Implementation Plan will follow the principles of our Project Delivery Approach. Every service, software, application, and consultancy that we offer follows these principles, ensuring your solution is planned and executed thoroughly.

Our delivery approach covers four key principles: Assess, Design, Build and Operate. A summary of these principles are as follows:

3.3. Offboarding

We take Offboarding and Exit Planning seriously, ensuring that our transparency and flexibility at the end of your solution's lifetime matches that of the beginning.

When offboarding, all property, data and information held in connection with the Framework or Call Off Contract will either be returned or destroyed as per EIS's Secure Disposal Policy.

An Exit Plan specific to the individual customer's service requirements will be agreed as part of the Offboarding process ensuring that you receive a bespoke service and will be issued as part of the call-off contract.

Your Offboarding plan will include:

- A dedicated Offboarding Officer who will be responsible for fine-tuning the offboarding process.
- A clear data return policy, defined as part of your original Onboarding process. All of your data will be either returned or destroyed, in line with EIS's Secure Disposal Policy and your own individual needs.
- Clear communication throughout the contract termination process.
- Clear advice and support during any migration.

For details relating to Contract Termination, please refer to G-Cloud framework terms and associated EIS standard Terms and Conditions of sale for rights to terminate.

All Offboarding process and Exit Plans must be agreed with in line with EIS's Terms and Conditions of Sale.

3.4. Outcomes and Deliverables

Specific outcomes and deliverables will be agreed upon with your Onboarding Officer as part of the initial Implementation Plan. Part of communicating our shared vision is establishing clear outcomes and deliverables, working towards them, and reviewing them as part of our ongoing transparency.

3.5. Trial Availability

There is no trial available for this service.

4. Responsibilities and Requirements

4.1. Customer Responsibilities

All responsibilities between EIS and the customer will be agreed upon before the Implementation Plan is executed. These responsibilities will be agreed upon in an SLA.

4.2. Technical Requirements

Any specific technical requirements can be discussed as part of the ongoing Cybersecurity Support and Consultancy service.

5. Prices, Invoicing and Contracts

5.1. Pricing Model

Please refer to our G-Cloud rate card.

5.2. Ordering and Invoicing

Customers will be required to complete and sign the G-Cloud framework offer terms and conditions order form.

All customers will be required to apply for a trade account and provide supporting evidence relating to all financial due diligence enquiries requested by EIS.

Trade account payment terms are 30 days from issue date of an undisputed invoice.

While this is our standard approach, EIS's aim is to make partnering with us as simple as possible. If you would like to discuss further options, please contact us at sales@eis.co.uk or telephone 03301 650000.

5.3. Contract Termination

For details relating to Contract Termination, please refer to the G-Cloud framework terms and associated EIS standard Terms and Conditions of sale for rights to terminate.

6. Security and Resilience

6.1. Data Backup, Data Restoration and Disaster Recovery

Protecting our customer's data is of paramount importance to EIS, across all our services and sectors. Responsibility and openness when providing backup and restore services lies at the heart of every partnership we share with our customers.

6.2. Business Continuity and Disaster Recovery

EIS's approach to Business Continuity Management is aligned with industry best practice and standards including ISO 22301:2019. It provides a framework for corporate and service level management of business continuity to ensure that EIS is resilient and able to continue to deliver its services and recover effectively from a significant business disruption.

EIS's Business Continuity and Disaster Recovery (BCDR) plan details the processes and arrangements EIS (and its subcontractors) will follow to:

- Ensure continuity of the Customer's business processes and operations supported by the services following any failure or disruption of any element of the deliverables; and
- Recover the deliverables in the event of a disaster.

EIS's BCDR plan is tested regularly to ensure its effectiveness in the event of a failure or disruption to the services.

6.3. Business Continuity and Disaster Recovery Objectives

EIS's Business Continuity and Disaster Recovery plan supports the delivery of the following objectives:

- To ensure continuity of provision of the deliverables in accordance with the Contract at all times during and after invocation of the BCDR plan.
- To minimise, as far as reasonably possible, the adverse impact of any disaster.
- To provide a process for the management of disaster recovery testing.
- To ensure compliance with security standards is maintained for any period during which the plan is invoked.

- To ensure BCDR arrangements are upgradeable and sufficiently flexible to support changes to the deliverables and business operations supported by them.
- To recover to standard operation mode with minimal disruption to services.
- To ensure lessons are learned and inform the continuous improvement of BCDR arrangements.

EIS undertake due diligence on subcontractors to ensure adequate BCDR arrangements are in place before engaging them as part of our supply chain and review this on an ongoing basis.

Where elements of the services are supported by subcontractors of EIS, EIS and the subcontractor will notify the other party in the event their respective BCDR plans are invoked. EIS will work together with the subcontractor to manage any failure or disruption in line with the BCDR arrangements in our contract with the subcontractor.

6.4. Information Security

We commit to ensuring that all personal and sensitive data processed on behalf of our customers is done so in accordance with Data Protection legislation, information governance and security best practice.

6.5. Our Organisational Controls

We will maintain appropriate organisational and technical measures to ensure the services we provide are secure and fully compliant with Data Protection legislation. These include, but are not limited to, the following:

- Data Protection, Information Security, Information Governance and related policies and procedures are in place and reviewed regularly. Copies of these can be provided upon request.
- All staff are required to complete mandatory Information Governance, GDPR/ Data Protection and Cyber Security e-learning which is renewed every two years.
- Physical access controls including swipe card/ ID card access to buildings, buildings opened and locked by security each day, clear desk and screen policy and control of access to secure areas.
- All staff contracts of employment include a clause detailing the responsibilities required of every individual when handling data of any kind.

6.6. Security Management

It is the policy of EIS to maintain an Information Security Management System designed to meet the requirements of ISO 27001. EIS has a dedicated Strategy & Governance team that is responsible for ensuring our organisation complies with all legal requirements, codes of practice and requirements prescribed to maintain our

certifications which include ISO 9001, ISO 14001, ISO 27001 and Cyber Essentials Plus.

We have a range of established policies and processes to support the controls mentioned above, meaning you can feel safe in the knowledge that we have the necessary controls already in place to deliver a fully secure and compliant service. These include, but are not limited to:

- Statement of Applicability for Security Measures
- Acceptable Use Policy
- Access Control Policy
- Cyber Security Incident Management Policy
- Disposal and Destruction Policy
- Information Security Policy
- Password Policy
- Safe Use of Removable and Online Storage
- Software Update and Patch Management Policy
- Supplier Security Policy.

6.7. Data Protection

EIS is committed to fulfilling its obligations under the EU General Data Protection Regulation 2016 (GDPR) and UK Data Protection Act 2018 and any subsequent data protection legislation, incorporating any appropriate additional obligations as required by the customer.

EIS is registered with the Information Commissioners Office (ICO) and has appointed a Data Protection Officer to monitor compliance with data protection legislation across our business activities.

7. Accreditations

WWW.EIS.CO.UK