JISC CYBER INCIDENT RESPONSE SERVICES GENERAL TERMS AND CONDITIONS

1. DEFINITIONS AND INTERPRETATIONS

1.1. In these Terms, the following words will have the following meanings.

Additional Services	has the meaning given to it in Clause 2.5;
Applicable Law	all applicable laws, statutes, regulations, decree directives, legislative enactments, orders, binding decisions of a competent Court or Tribunal, rule, regulatory policies, guidelines, codes, other binding restriction, regulatory permits and licences applicable under law which are in force from time to time during the term of the Contract to which a Party is subject from time to time;
ASC	the additional Services confirmation provided by Jisc under Clause 2.6;
Bribery Legislation	the Bribery Act 2010 and any subordinate legislation made under that Act from time to time together with any guidance or codes of practice issued by the relevant government department concerning the Bribery Legislation;
Business Days	a day (other than a weekend or public holiday) when banks in London are open;
Business Hours	between 08:00 and 18:00 on a Business Day;
Client	the purchaser of the Services as identified on the Statement of Work;
Client Environment	the description of the Client's IT infrastructure and environment as identified in the Statement of Work (as updated from time to time under Clause 6.1.2);
Charges	the charges together with any expenses in respect of the Services as set out in the Statement of Work, as varied from time to time in accordance with Clause 8.7;
Confidential Information	(a) the Contract, and in respect of each Party, all information and data of whatever nature whether disclosed orally, in writing or by any other means which relates to a Party's (or any Group company's) existing or potential customers and personnel, trade secrets, know-how, research, developments, technical and business information relating to products, methods and processes, and any other information whether or not designated as confidential information but which by its nature is confidential; (b) notes, reviews, analysis, reports and other information derived from any of the information in paragraph (a) above; and (c) information designated as confidential or commercially sensitive or which might reasonably be considered as such;
Consultancy Services	the consultancy services described in Schedule 1;
Contract	the Statement of Work, these Terms and any Schedules;
Deliverable	any report or other output generated in the course of the Services and made available to the Client as part of the Services;

Effective Date	the date the Client signs the Statement of Work;
Environmental Information Regulations	the Environmental Information Regulations 2004 (or the Environmental Information (Scotland) Regulations 2004) (as the case may be);
FOIA	the Freedom of Information Act 2000 or the Freedom of Information Scotland Act 2002 (as the case may be) and any subordinate legislation made under that Act from time to time;
Information	has the meaning given to "information" by the FOIA or the meaning given to "environmental information" by the Environmental Information Regulations (as the case may be);
Jisc	Jisc Services Limited, a wholly owned Jisc subsidiary and a company limited by guarantee which is registered in England under company number 02881024 with its registered office at 4 Portwall Lane, Bristol, BS1 6NB (or any successor body thereto);
Intellectual Property Rights	any patent, trade mark, service mark, registered design, copyright, design right, database right, rights protecting confidential information, any applications for or rights to apply for any of the above and any other intellectual property right recognised in any part of the world, whether or not now existing or applied for, and all accrued rights of action in respect of any such rights;
Modern Slavery Legislation	the Modern Slavery Act 2015 and any subordinate legislation made under that Act from time to time together with all applicable anti-slavery and human trafficking laws, statutes, regulations, guidance or codes of practice issued by the relevant government department;
Statement of Work	the Jisc Statement of Work (in the form as set out at Schedule 3 and entered into pursuant to these Terms) to which these Terms are attached and under which these Terms are incorporated by reference, as may be supplemented from time to time under Clause 2.7 which is accepted by the Client by signature;
Services	the Consultancy Services, expressed in terms of a number of days of provision, as identified as being ordered by the Client in the Statement of Work and/or any further services as may be subsequently included under Clause 2.7;
Schedules	any schedule to the Contract;
Special Conditions	any of the special conditions contained in the Statement of Work;
Start Date	in respect of any of the Services, any specific start date identified on the Statement of Work;
Terms	these terms and conditions for the Services, as amended or supplemented by any Special Conditions; and
User	any individual using the Client Environment to access or manage the internet or data.

1.2. In the event of any conflict, inconsistency or contradiction between any of the component documents comprising the Contract, then the following order of precedence will apply (highest to lowest):

1.2.1. the Statement of Work;

1.2.2. these Terms; and

1.2.3. the Schedules.

2. APPLICATION OF THESE TERMS

2.1. The Contract will be formed by the Client accepting and signing the Statement of Work.

2.2. Notwithstanding Clause 2.1, the Contract shall also be deemed to be formed if the Client instructs Jisc to proceed with the Services or permits Jisc to commence the Services prior to the signing of the Statement of Work, in which case the Client shall be deemed to have accepted the Statement of Work and these Terms on the date such instruction is given or such permission is granted.

2.3. These Terms contain the only conditions under which Jisc will provide any of the Services to the Client and will govern the Contract to the exclusion of all other terms and conditions (including any terms and conditions included on any purchase order provided by the Client).

2.4. The Statement of Work identifies the Services to be provided by Jisc to the Client as at the Effective Date.

2.5. If, following the Effective Date, and whilst the Contract is in force, the Client requires Services from Jisc in addition to those identified in the Statement of Work (**Additional Services**), then the Client may submit its request in writing to Jisc, identifying the Additional Services required, together with any necessary updates to the information contained in the Statement of Work which relates to the Additional Services (such as the Client Environment and any Special Conditions).

2.6. Following such request, Jisc will provide to the Client an Additional Service Confirmation ("**ASC**") (which may be by email) which will contain the following information in respect of each Additional Service:

2.6.1. Start Date (if any);

2.6.2. Charges;

2.6.3. any known risks of performing the Services as known by Jisc;

2.6.4. confirmation of any other changes to the Statement of Work relating to the Additional Services, such as Client Environment and any Special Conditions

2.7. The ASC will be deemed contractually binding on the Client and incorporated into the Contract unless the Client notifies Jisc that it has any issues with the ASC within 5 Business Days (or, in the case of emergencies, within 1 Business Day) of the date of the ASC (in which case the parties shall discuss and agree any necessary changes and following agreement, the ASC will be deemed incorporated into the Contract). A copy of the ASC will be added to the Statement of Work as an appendix.

2.8. If the Client requires Additional Services after the Effective Date and the Contract is not then in force, then a new Statement of Work will be required.

3. SERVICE

3.1. Jisc will provide the Services to the Client as set out in the Statement of Work and from any Start Date (where applicable). The Services will be subject to these Terms.

3.2. Subject to earlier termination in accordance with these Terms, Jisc will provide the Services in accordance with the timescales agreed between the parties from time to time or as set out in the Statement of Work .

3.3. Where the Services set out in the Statement of Work have not been fully utilised by the Client, Jisc may, at its discretion, permit an extension or a substitution of the Services.

3.4. The Client acknowledges and agrees that:

3.4.1. Jisc's ability to provide the Services depends on Jisc's knowledge of the technical and operational infrastructure used by the Client as detailed in the Client Environment; and

3.4.2. nothing in these Terms will oblige Jisc to provide any support in respect of the Client Environment or provide any assistance to Users

3.5. Jisc may revise the Services, or any other provision as follows:

3.5.1. changes to the Services, Service Levels or any other provision which would materially increase the obligations of the Customer under the Contract or cost to the Customer of receiving the benefit of the Services under the Contract, or would materially decrease the Customer's rights or remedies will only be made by Jisc after giving at least 3 months' notice to the Client;

3.5.2. any other change can be made at any time by publishing the changes on the Service website.

4. USE OF SERVICES

4.1. The Client will not use any Services or otherwise act or refrain from acting in respect of Services so as to:

4.1.1. provide or support services to third parties other than Users;

4.1.2. attempt to obtain, or assist other third parties, other than Users, in obtaining access to data by means of the

Services outside the scope of the express terms of the Contract, or

4.1.3. transfer, license or otherwise make available temporarily or permanently any of its rights in respect of the Services under the Contract.

5. WARRANTIES

5.1. Each Party warrants, represents and undertakes that:

5.1.1. it has full capacity and authority to enter into and perform the Contract; and there are no actions, or regulatory investigations pending or, to that Party's knowledge, threatened that might affect the ability of that Party to meet its obligations under the Contract;

5.1.2. in relation to the Contract and its subject matter, neither it nor any of its employees, sub-contractors or agents or others performing services on its behalf has done (or agreed to do) or will do (or agree to do) anything which constitutes a breach by that Party of the Bribery Act 2010 and any subordinate legislation made under that Act from time to time together with any guidance or codes of practice issued by the relevant government department concerning such legislation;

5.1.3. it will and require that each of its sub-contractors will, at all times during the term of the Contract comply with UK Modern Slavery Act; and

5.1.4. it will not engage in any activity, practice or conduct which would constitute either;

5.1.5. it will not engage in any activity, practice or conduct which would constitute either:

i. a UK tax evasion facilitation offence under section 45(1) of the Criminal Finances Act 2017; or

ii. a foreign tax evasion facilitation offence under section 46(1) of the Criminal Finances Act 2017

5.2. Jisc does not make any representations, whether express or implied, about whether the Services will operate in combination with any Customer equipment and software.

6. CLIENT OBLIGATIONS

6.1. The Client will:

6.1.1. provide Jisc, its subcontractors and agents with any documentation, information, co-operation and access to premises and personnel as may be reasonably requested by Jisc from time to time as necessary to provide the Services;

6.1.2. promptly inform Jisc of any changes to the Client Environment;

6.1.3. provide Jisc with all necessary health and safety, security, conduct and other rules, procedures and requirements in relation to the Client's property and systems; and

6.1.4. ensure that any dependencies or conditions expressly set out in any Special Conditions are fulfilled within the timescales reasonable required by Jisc.

6.2. The Client warrants that:

6.2.1. all information relating to the Client Environment or otherwise provided to Jisc is true, accurate and not misleading;

6.2.2. it has obtained all third party consents, licences and rights reasonably required in order to allow Jisc to perform the Services; and

6.2.3. it has made all necessary contingency arrangements (including back-ups) to enable it and any Users to continue to use the Client Environment following any impairment or damage to the Client Environment as a result of the Services.

6.3. Should the Client fail to perform any of its obligations under the Contract then Jisc will not be responsible for any delay, cost increase or other consequences arising from such failure.

7. JISC OBLIGATIONS

7.1. In providing the Services, Jisc will:

7.1.1. perform the Services with reasonable care and skill and in accordance with good practice in Jisc's industry;

7.1.2. obtain and at all times maintain all necessary licences and consents required by Jisc to provide the Services, and comply with all applicable laws in relation to the performance of the Services;

7.1.3. hold all data supplied by or on behalf of the Customer to Jisc in relation to

the Services (the **Customer Data**) in safe custody at its own risk, maintain the Customer Data in the condition in which it was provided until returned to the Customer (if applicable to the Services), and not dispose or use the Customer Data other than in accordance with the Customer's written instructions or authorisation; and

7.1.4. maintain in force, with a reputable insurance company, professional indemnity insurance, employers' liability insurance and public liability insurance to cover the liabilities that may arise under or in connection with the Contract.

8. CHARGES AND PAYMENT

8.1. The Client will pay the Charges in respect of the Services, as set out in the Statement of Work and elsewhere in the Contract without any set-off or deduction. All Charges and other amounts payable under the Contract are exclusive of any applicable value added tax.

8.2. Where out-of-hours support is required, a multiplier of 1.5 shall be applied to the applicable day rate for such support.

8.3. Jisc will issue invoices for the Charges in accordance with the invoicing timetable set out in the Statement of Work. In consideration of the supply of the Services by Jisc, the Client will pay the Charges to Jisc within 30 days of the date of issue of an invoice.

8.4. Charges must be paid by bank transfer (using such payment details as are notified by Jisc to the Client from time to time).

8.5. If the Client fails to pay any amount properly due and payable by it under the Contract, this will be a material breach for the purposes of Clause 14, and Jisc will additionally have the right to:

8.5.1. suspend performance of its obligations under the Contract; and/or

8.5.2. charge interest on the overdue amount at the rate of 4 percent per annum above the base rate for the time being of the Bank of England accruing on a daily basis from the due date up to the date of actual payment, whether before or after judgement; and/or

8.5.3. on 5 Business Days' written notice (in the absence of receipt of a disputed invoice notice from Client) suspend the provision of the Services until such amounts have been paid in full by the Client and Jisc will be entitled to continue charging the Client for the Services during such period of suspension; and/or

8.5.4. where the non-payment exceeds 30 days, Jisc may give notice of termination of the Contract in accordance with Clause 14.2.2.

8.6. The Client will reimburse (on production of such evidence as the Client may reasonably require) all expenses properly and reasonably incurred in the course of performing the Services. Such expenses will be included in the invoices submitted to the Client by Jisc under Clause 8.1.

8.7. The Client acknowledges that the Charges in respect of the Consultancy Services will be the time and materials rates set out in the Statement of Work, or as notified to the Client and/or published on Jisc's website from time to time.

8.8. Where a Client requests to amend an agreed Start Date for any Service the following additional Charges will apply:

8.8.1. Where the Client notifies Jisc more than 10 Business Days before the Start Date, no additional charge;

8.8.2. Where the Client notifies Jisc between 10 and 5 Business Days before the Start Date, 1 day to be charged at the day rate specified in the Statement of Work;

8.8.3. Where the Client notifies Jisc fewer than 5 Business Days before the Start Date, 2 days to be charged at the day rate specified in the Statement of Work.

8.9. Save where the Client's non-payment relates to a bona fide dispute, the Client will not have any right to withhold, or any right of set-off, with respect to payments due to Jisc under the Contract.

8.10. Any retained incident response days purchased under this Contract must be utilised within twelve (12) months of the Effective Date. Any unused retained days remaining after this period shall automatically expire and will not be carried forward, refunded, or credited.

9. LIMITATION OF LIABILITY

9.1. Nothing in the Contract will:

9.1.1. limit or exclude the liability of a Party for death or personal injury resulting from negligence;

9.1.2. limit or exclude the liability of a Party for fraud or fraudulent misrepresentation by that party; or

9.1.3. limit or exclude any liability of a Party in any way that is not permitted under applicable law.

9.2. The limitations and exclusions of liability set out in this Clause 8.9 and elsewhere in the Contract:

9.2.1. are subject to Clause 9.1; and

9.2.2. govern all liabilities arising under the Contract or in relation to the subject matter of the Contract, including liabilities arising in contract, in tort (including negligence) and for breach of statutory duty.

9.3. Neither Party will be liable:

9.3.1. in respect of any loss of profits, income, revenue, use, production or anticipated savings;

9.3.2. for any loss of business, contracts or commercial opportunities;

9.3.3. for any loss of or damage to goodwill or reputation;

9.3.4. in respect of any loss or corruption of any data, database or software; or

9.3.5. in respect of any special, indirect or consequential loss or damage.

9.4. Jisc's liability in relation to any event or series of related events will not exceed the total amount paid and payable by the Client to Jisc under the Contract during the 12 month period immediately preceding the event or events giving rise to the claim and if the claim arises within the first 12 months following the Effective Date, then the total amount that would have been payable in such 12 month period.

9.5. Jisc will not be liable in any way to the Client if:

9.5.1. the Client uses or interacts with the Services other than in accordance with the Contract or contrary to Jisc's instructions, documentation or reasonable expectations;

9.5.2. problems are caused by errors, omissions or misinformation in any documents, information, instructions or scripts provided to Jisc by the Client, or any actions taken by Jisc at the Client's direction;

9.5.3. Jisc's knowledge of the Client Infrastructure is deficient for any reason;

9.5.4. problems arise from the use of hardware or software or data or services of or supplied by the Client or other third party; or

9.5.5. problems arise from viruses transmitted through the Services. The Client acknowledges that the Services do not perform virus checking and that it is the Client's responsibility to ensure that any material downloaded is virus checked.

9.6. The Client acknowledges and agrees that:

9.6.1. no services of the kinds comprised in the Services or any of them offers 100% certainty of either problem prevention or problem detection or accurate identification of the causes of problems. Although Jisc will comply with industry practice in providing Services it will not have any liability for and will not be responsible for meeting any part of the costs of a failure by Jisc to prevent, detect or provide any causal understanding of any problem including where the Services are tasked specifically with so doing;

9.6.2. the Services may identify problems which do not exist or may misidentify problems (and Jisc shall have no liability for the same);

9.6.3. although Jisc will use reasonable care and skill, it is possible that the Services may cause harm to the Client Environment or wider IT system or the Users' IT systems and Jisc will have no liability for and will not be responsible for meeting any part of the costs of any such harm caused or any failure by Jisc to prevent, detect or limit any such harm including where the Services are tasked specifically with so doing;

9.6.4. Jisc's liability in relation to any open source software and any third party software or services used in the Services may be further limited under the terms of the relevant licence, supply contract or terms of use notified to the Client from time to time and such limitations will apply to Jisc's liability to the Client in respect of such open source software or third party services;

9.6.5. complex software is never wholly free from defects, errors and bugs, and Jisc gives no warranty or representation that the Services will be wholly free from such defects, errors and bugs.

9.7. All of the parties' warranties and representations in respect of the subject matter of the Contract are expressly set out in the terms of the Contract. To the maximum extent permitted by applicable law, no other warranties or representations concerning the subject matter of the Contract will be implied into the Contract.

10. INTELLECTUAL PROPERTY

10.1. All Intellectual Property Rights in respect of the Services will, as between the parties, remain owned by Jisc. Except as expressly stated in the Contract, the Client is not granted any rights to, or in, any such Intellectual Property Rights in respect of the Services or any related software, documentation or apparatus.

10.2. Without prejudice to Clause 10.1:

10.2.1. Jisc now grants the Client a non-exclusive, perpetual, royalty-free licence to access and download the Deliverables in order to enjoy the benefit of the Services for its own internal business purposes; and

10.2.2. in respect of the Consultancy Services, the Client may be granted access to use open source or third party proprietary software tools which will be subject to their own terms of use.

11. CONFIDENTIALITY

11.1. Each Party agrees to keep confidential and, subject to Clause 11.2, not to disclose to any third party any Confidential Information (excluding information which is or becomes public knowledge other than as a result of the default of the recipient) and to use any such Confidential Information only for the purposes of and in accordance with the Contract or as required by law.

11.2. Nothing in the Contract will prohibit or limit either Party's use of Confidential Information (i) previously known to it without obligation of confidence, (ii) independently developed by or for it, (iii) acquired by it from a third party which is not, to its knowledge, under an obligation of confidence with respect to such information, (iv) which is or becomes publicly available through no breach of the Contract, (v) where such use/disclosure is required by Applicable Law or by a court with the relevant jurisdiction if, to the extent not prohibited by Applicable Law, the recipient Party notifies the disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure, (vi) on a confidential basis, to its auditors, or (vii) on a confidential basis, to its professional advisers or others within its Group, on a need-to-know basis.

11.3. Each Party agrees to immediately notify the disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

11.4. Notwithstanding Clause 11.1 the Client agrees that Jisc may disclose data derived from the performance of the Services on an aggregated or un-aggregated basis, provided such disclosure does not identify the Client.

12. DATA PROTECTION

12.1. Both Jisc and the Client shall comply with the provisions of Schedule 2.

12.2. In the event of any conflict between Schedule 2 and any other provision of these Terms, the relevant provision of Schedule 2 shall take precedence.

13. FREEDOM OF INFORMATION

13.1. Jisc is not subject to the requirements of the FOIA and the Environmental Information Regulations. However, Jisc will endeavour to respond to any request in the spirit of the FOIA where reasonably able to do so. The parties will assist and cooperate with each other if a request is received by Jisc.

14. TERM AND TERMINATION

14.1. The Contract will commence on the Effective Date and will, subject to earlier termination under the Contract, continue until completion of all the Services.

14.2. Without prejudice to any other rights or remedies that may be available, either Party may at any time give a written notice of termination to the other Party if:

14.2.1. the other Party is in material breach of the Contract which is incapable of remedy; or

14.2.2. the other Party is in material breach of the Contract which is capable of remedy, but is not remedied within 30 days of receipt of a written notice from the first Party, specifying the breach and requesting remedy; or

14.2.3. the other Party becomes insolvent, subject to a winding up petition,

ceases trading or undergoes a similar event.

15. CONSEQUENCES OF TERMINATION

15.1. On any termination or expiry of the Contract for any reason:

15.1.1. each Party will return all hardware or other equipment, software, property, materials and other items (and all copies of them) belonging to the other Party and, at the disclosing Party's option, return or destroy any copies of the disclosing Party's Confidential Information; and

15.1.2. the provision of the Services will immediately cease.

15.2. Subject to Clauses 15.1, 15.3 and 15.4, any expiry or termination of the Contract for any reason, will be without prejudice to any other rights or remedies of either Party under the Contract or at law, and will not affect any accrued rights or liabilities of either Party.

15.3. Where the Client has terminated the Contract pursuant to Clause 14.2.2 Jisc will reimburse the Client for any monies paid in advance and in relation to Services yet to be provided.

15.4. The provisions of Clause 1 (Definitions), 6.2 (Client Warranties), 8.9 (Limitation of Liability), 10 (Intellectual Property), 11 (Confidentiality), 13 (Freedom of Information), 15 (Consequences of Termination), 16 (Dispute Resolution) and 25 (Governing Law and Jurisdiction) will survive termination (however caused) or expiry.

16. DISPUTE RESOLUTION

16.1. The Parties agree that in the event of a dispute they will first attempt to resolve the matter through good faith discussions and the production of an agreed improvement plan. If the matter is not resolved it will be escalated to higher levels of management via the management contacts as agreed between the Parties in writing. If the dispute is not resolved through discussion the Parties will use a mutually agreed alternative dispute resolution process prior to resorting to litigation as a last resort.

17. GENERAL VARIATION

17.1. No variation to the Contract will be effective unless it is agreed in writing and signed by authorised signatories for both Parties.

18. FORCE MAJEURE.

18.1. Neither Party will be liable to the other as a result of any delay or failure to perform its obligations under the Contract, if and to the extent such delay or failure is caused by an event or circumstance which is beyond the reasonable control of that Party. If such event or circumstances prevent a Party from performing any of its obligations under the Contract for more than 30 days continuously, the other Party will have the right, without limiting its other rights or remedies, to terminate the Contract with immediate effect by giving written notice to the first Party. For the avoidance of doubt, the failure or delay of any obligations of any sub-contractor will not be deemed to be beyond the reasonable control of a Party unless the delay or failure is a result of an event beyond the reasonable control of the sub-contractor.

19. ASSIGNMENT

19.1. Subject to Clause 19.2, neither Party will at any time assign or transfer all or any of its rights or obligations under the Contract, without the prior written consent of the other Party (such consent not to be unreasonably withheld or delayed).

19.2. Jisc may at any time by written notice assign or transfer all or any of its rights or obligations under the Contract to another member of its Group. Jisc will be entitled to sub-contract any of its obligations, and sub-licence any of its rights under the Contract without the Customer's consent.

20. SUB-CONTRACTORS

20.1. Where Jisc sub-contracts any of its rights or obligations under these Terms (in whole or in part) to any third party, Jisc will remain primarily liable for all acts and omissions of any such sub-contractor and will ensure that any sub-contractor complies with Jisc's confidentiality obligations in these Terms.

21. NOTICES

21.1. Any notices given in relation to the Contract will be given for the attention of the relevant person set out in the Statement of Work, which may include email, and sent to the address or email address of the recipient set out in the Statement of Work or another address or email address which the recipient may designate by notice given in accordance with the provisions of this Clause, with, in the case of Jisc, a copy by email to legal@jisc.ac.uk.

21.2. A notice will be deemed to have been received: if delivered personally, at the time of delivery; in the case of pre-paid first-class post, 3 Business Days from the date of posting; and in the case of email, upon the email reaching the recipient's server.

21.3. Where notices are to be served by email, the email must contain the following wording in the subject matter field: “Notice served in accordance with Jisc Cyber Incident Response Services General Terms and Conditions”.

22. INDEPENDENT CONTRACTOR

22.1. Nothing in the Contract will be construed as constituting or evidencing any partnership, contract of employment or joint venture of any kind between either of the Parties or as authorising either Party to act as agent for the other. Neither Party will have authority to make representations for, act in the name of or on behalf of, or otherwise to bind the other Party in any way.

23. ENTIRE CONTRACT

23.1. The Contract constitutes the entire agreement between the Parties and supersedes all prior agreements, understandings or arrangements (both oral and written) relating to the subject matter of the Contract. Each of the parties acknowledges and agrees that it does not enter into the Contract on the basis of and does not rely, and has not relied upon, and will have no remedy in respect of, any statement or representation or warranty or other provision made, given or agreed to by the other Party to the Contract (whether negligently or innocently made) except those expressly repeated or referred to in these Terms and the Call-Off Terms and the only remedy available in respect of any misrepresentation or untrue statement made to it will be a claim for breach of contract under the Contract. Nothing in this Clause will operate to limit or exclude liability for fraud.

24. THIRD PARTY RIGHTS

24.1. Subject to Clause 24.2, no third party is entitled to the benefit of the Contract under the Contracts (Rights of Third Parties) Act 1999. The right of either Party to vary or terminate the Contract will not be subject to the consent of any third party.

24.2. Jisc may enforce any rights of Jisc under these Terms in accordance with the Contracts (Rights of Third parties) Act 1999.

25. GOVERNING LAW AND JURISDICTION

25.1. The Contract will be governed by English law, and the English Courts will have exclusive jurisdiction to deal with disputes arising out of or in connection with the Contract.

26. COUNTERPARTS

26.1. The Contract may be entered into by the Parties on separate counterparts, which taken together will constitute one single agreement between the Parties.

27. TOOLING AND SOFTWARE

27.1. In support of an engagement, Jisc may recommend that the Client deploys certain software to the Client network for a limited period.

27.2. In addition to the licence terms set out in the Contract such software is made available to the Client: for the Client’s internal use only in relation to, and for the duration of, the agreed engagement; and on an ‘as-is’ basis and the Client acknowledges that Jisc does not make any warranty or representation in relation to such hardware or software or any results they may produce..

27.3. The Client shall uninstall all such software within 30 days of completion of the engagement, unless it is otherwise agreed in writing to keep such software installed for a longer period in readiness for potential use on future tasks.

28. NCSC POST-INCIDENT REPORTING

28.1. The Client acknowledges that Jisc is an NCSC-assured Cyber Incident Response provider under the National Cyber Security Centre’s certified Cyber Incident Response (CIR) scheme. In accordance with the requirements of that scheme, Jisc may be required to provide a copy of the Post-Incident Report to the National Cyber Security Centre on a confidential basis.

28.2. Jisc shall consult with the Client in advance of any such disclosure and shall, to the extent permitted under the terms of the CIR scheme, co-operate with the Client to minimise the scope of the information disclosed to the extent reasonably practicable, including by redacting sections of the report where appropriate.

29. COMMUNITY THREAT INTELLIGENCE SHARING

29.1. The Client acknowledges that anonymised cyber threat intelligence, including IoCs, TTPs, and lessons learned arising from incidents, may be shared by Jisc with the Education and Research community via trusted community channels, threat reports, and security platforms.

29.2. Jisc shall ensure that all such information is sanitised, anonymised, and presented in a manner that prevents direct or indirect attribution to the Client, the Client’s systems, or any individual cyber incident.

SCHEDULE 1: DATA PROTECTION

1. DEFINITONS

1.1. The following definitions apply to this Data Protection Schedule

Agreement	means the agreement between Jisc and the Client for the provision of the Service;
Applicable Law	means all applicable laws, statutes, regulations, decree directives, legislative enactments, orders, binding decisions of a competent Court or Tribunal, rule, regulatory policies, guidelines, codes, other binding restriction, regulatory permits and licences applicable under law which are in force from time to time during the term of this Agreement to which a Party and/or any Processing of Personal Data is subject from time to time;
Controller, Processor and Data Subject	shall have the meaning given to those terms in the UK GDPR;
Data Protection Legislation	means (a) any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject for the purposes of this Agreement, including the Data Protection Act 2018 and the General Data Protection Regulation 2016/679 (**EU GDPR**) as each is amended in accordance with the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (as amended by SI 2020 no. 1586) and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, as amended to be referred to as **DPA 2018** and the **UK GDPR** respectively; and (b) any code of practice or guidance published by the Regulator or European Data Protection Board from time to time;
Data Protection Particulars	means, in relation to any Processing under this Agreement: (a) the subject matter and duration of the Processing; (b) the nature and purpose of the Processing; (c) the type of Personal Data being Processed; and (d) the categories of Data Subjects.
Data Subject Request	means an actual or purported subject access request or notice or complaint from (or on behalf of) a Data Subject exercising his rights under the Data Protection Legislation;
Data Transfer	means transferring the Personal Data to, and / or accessing the Personal Data from and / or Processing the Personal Data within, a jurisdiction or territory that is not a Permitted Country;
ICO	means the UK Information Commissioner (including any successor or replacement);
Permitted Country	means a country, territory or jurisdiction that is either: (a) within the UK or the European Economic Area; or (b) outside of the UK or European Economic Area but which is the subject of an adequacy determination by the UK Secretary of State or the European Commission (as applicable);
Permitted Purpose	means the purpose of the Processing as specified in the Data Processing Particulars;
Personal Data	has the meaning given to it in the UK GDPR and for the purposes of this Agreement includes Sensitive Personal Data;
Personal Data Breach	has the meaning given to it in the UK GDPR and, for the avoidance of doubt, includes a breach of Clause 4.1.3;
Personnel	means all persons engaged or employed from time to time by Jisc in connection with this Agreement, including employees, consultants, contractors and permitted agents;

Processing	has the meaning given to it in the UK GDPR (and **Process** and **Processed** shall be construed accordingly);
Regulator	means the ICO and any other independent public authority which has jurisdiction over a Party, including any regulator or supervisory authority which is responsible for the monitoring and application of the Data Protection Legislation;
Regulator Correspondence	means any correspondence from a Regulator in relation to the Processing of Jisc Data under or in connection with this Agreement;
Security Requirements	means the requirements regarding the security of the Personal Data, as set out in the Data Protection Legislation (including, in particular, the measures set out in Article 32(1) of the UK GDPR (taking due account of the matters described in Article 32(2) of the UK GDPR));
Sensitive Personal Data	means Personal Data that reveals such categories of data as are listed in Article 9(1) of the UK GDPR and Personal Data relating to criminal convictions and offences;
Service	means the Cyber Incident Response Service provided by Jisc;
Schedule	means this schedule which forms part of the Agreement; and
Third Party Request	means a written request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by law or regulation;

2. ARRANGEMENT BETWEEN THE PARTIES

2.1. The Parties shall each Process the Personal Data in accordance with the terms of this Schedule. The Parties acknowledge that the factual arrangement between them dictates the classification of each Party in respect of the Data Protection Legislation. Notwithstanding the foregoing, the Parties anticipate and agree that the Client shall act as Controller and Jisc shall act as Processor, as follows:

2.1.1 The Client shall be a Controller where it is Processing the Personal Data in relation to the services being supplied by Jisc; and

2.1.2 Jisc shall be a Processor where it is Processing the Personal Data in relation to the Permitted Purpose in connection with the performance of its obligations under these service terms.

2.2. Each of the Parties acknowledges and agrees that the following table sets out an accurate description of the Data Protection Particulars:

The subject matter and duration of the Processing	The subject matter of the Processing is the provision of cyber incident response and digital forensics services, including investigation, containment, eradication, recovery, and post-incident reporting activities following a cyber security incident. Processing shall commence upon notification of an incident by the Client and shall continue for the duration of the incident response engagement, including any agreed follow-up forensic analysis and reporting. Personal Data shall be retained only for as long as is necessary to fulfil the purposes of the Services, comply with applicable legal or regulatory obligations, or as otherwise agreed with the Client.
The nature and purpose of the Processing	The nature of the Processing includes the collection, access, analysis, storage, and secure handling of data required to investigate and respond to a cyber security incident. This may include technical analysis of systems, networks, logs, endpoints, and compromised accounts, as well as

	digital forensic examination of affected environments. The purpose of the Processing is to enable the detection, investigation, containment, mitigation, and remediation of cyber security incidents, to determine root cause and impact, to support recovery activities, and to produce incident and forensic reports for the Client and, where applicable, relevant authorities or assurance bodies.
The type of Personal Data being Processed	The Personal Data processed may include, where present within affected systems or logs: • User identifiers (such as usernames, email addresses, and account IDs) • Device and system identifiers (such as hostnames, IP addresses, and device IDs) • Authentication and access data (such as login timestamps and access logs) • Business contact information contained within systems or communications • Limited content data incidentally captured within forensic artefacts, logs, or system images The Processing is not intended to include special category data; however, such data may be incidentally processed where it is stored within systems affected by the incident.
The categories of Data Subjects	The categories of Data Subjects may include: • Employees, contractors, and temporary staff of the Client • Students, researchers, or other end users of the Client's systems • Third parties whose data is processed within the Client's environment, including collaborators or service users

3. CONTROLLER OBLIGATIONS

3.1 As the Controller in respect of the Processing of the Personal Data, the Client shall ensure that:

3.1.1 it is not subject to any prohibition or restriction which would prevent or restrict it from disclosing or transferring the Personal Data to Jisc in accordance with the terms of this Schedule; and

3.1.2 all fair processing notices have been given (and/ or, as applicable, consents obtained) and are sufficient in scope to allow the Client to disclose the Personal Data (including any Sensitive Personal Data) to Jisc for the delivery of the Service in accordance with the Data Protection Legislation.

4. PROCESSOR OBLIGATIONS

4.1 Jisc (as a Processor in relation to any Personal Data Processed by (or on behalf of) the Client pursuant to the Agreement) undertakes to the Client that it shall:

4.1.1 Process the Personal Data for and on behalf of the Client in connection with the performance of the Service only and for no other purpose in accordance with the terms of this Agreement and any instructions from the Client;

4.1.2 unless prohibited by law, promptly notify the Client (and in any event within forty-eight (48) hours of becoming aware of the same) if it considers, in its opinion (acting reasonably) that it is required by Applicable Law to act other than in accordance with the instructions of the Client, including where it believes that any of the Client's instructions under Clause 4.1.1 infringes any of the Data Protection Legislation;

4.1.3 implement and maintain appropriate technical and organisational security measures to comply with at least the obligations imposed on a Controller by the Security Requirements. If requested by the Client, Jisc will provide a description of the technical and organisational security measures that Jisc will implement and maintain;

4.1.4 take all reasonable steps to ensure the reliability and integrity of any of the Personnel who shall have access to the Personal Data, and ensure that each member of Personnel shall have entered into appropriate contractually-binding confidentiality undertakings;

4.1.5 notify the Client promptly, and in any event within forty-eight (48) hours, upon becoming aware of any actual or suspected, threatened or 'near miss' Personal Data Breach, and:

(a) implement any measures necessary to restore the security of compromised Personal Data;

(b) assist the Client to make any notifications to the Regulator and affected Data Subjects;

4.1.6 notify the Client promptly (and in any event within ninety-six (96) hours) following its receipt of any Data Subject Request or Regulator Correspondence and shall:

(a) not disclose any Personal Data in response to any Data Subject Request or Regulator Correspondence without the Client's prior written consent; and

(b) provide the Client with all reasonable co-operation and assistance required by the Client in relation to any such Data Subject Request or Regulator Correspondence;

4.1.7 not disclose Personal Data to a third party in any circumstances without the Client's prior written consent, other than:

(a) in relation to Third Party Requests where Jisc is required by law to make such a disclosure, in which case it shall use reasonable endeavours to advise the Client in advance of such disclosure and in any event as soon as practicable thereafter, unless prohibited by law or regulation from notifying the Client;

(b) to Jisc's employees, officers, representatives and advisers who need to know such information for the purposes of Jisc performing its obligations under this Agreement and in this respect Jisc shall ensure that its employees, officers, representatives and advisers to whom it discloses the Personal Data are made aware of their obligations with regard to the use and security of Personal Data under this Agreement; and

(c) to a sub-contractor appointed in accordance with Clause 5.

4.1.8 not make (nor instruct or permit a third party to make) a Data Transfer without putting in place measures to ensure the Client's compliance with Data Protection Legislation;

4.1.9 on the written request of the Client, and with reasonable notice, allow representatives of the Client to audit Jisc in order to ascertain compliance with the terms of this Clause 4 and/ or to provide the Client with reasonable information to demonstrate compliance with the requirements of this Clause 4, provided that:

(a) the Client shall only be permitted to exercise its rights under this Clause 4.1.9 no more frequently than once per year (other than where an audit is being undertaken by a Client in connection with an actual or 'near miss' Personal Data Breach, in which case, an additional audit may be undertaken each year by the Client within thirty (30) days of the Client having been notified of actual or 'near miss' Personal Data Breach);

(b) each such audit shall be performed at the sole expense of the Client;

(c) the Client shall not, in its performance of each such audit, unreasonably disrupt the business operations of Jisc;

(d) the Client shall comply with Jisc's health and safety, security, conduct and other rules, procedures and requirements in relation to Jisc's property and systems which have been notified by Jisc to the Client in advance; and

(e) in no case shall the Client be permitted to access any data, information or records relating to any other Client of Jisc.

4.1.10 except to the extent required by Applicable Law, on the earlier of:

(a) the date of termination or expiry of the Agreement (as applicable); and/or

(b) the date on which the Personal Data is no longer relevant to, or necessary for, the performance of the Service,

cease Processing any of the Personal Data and, within sixty (60) days of the date being applicable under this Clause 4.1.10, return or destroy (as directed, in writing, by the Client) the Personal Data belonging to, or under the control of, the Client and ensure that all such data is securely and permanently deleted from its systems, provided that Jisc shall be entitled to retain copies of the Personal Data for evidential purposes and to comply with legal and/or regulatory requirements;

4.1.11 comply with the obligations imposed upon a Processor under the Data Protection Legislation; and

4.1.12 assist the Client in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the UK GDPR taking into account the nature of Processing and the information available to Jisc, provided that Jisc shall be entitled to charge a fee to the Client (on a time and materials basis and at such rate notified by Jisc to the Client from time to time) in respect of providing any such assistance to the Client.

4.2 Notwithstanding anything in this Agreement to the contrary, this Clause 4 shall continue in full force and effect for so long as Jisc Processes any Personal Data on behalf of the Client.

5. SUB-CONTRACTORS

5.1 Jisc may from time to time use sub-contractors to perform all or any part of its obligations under this schedule. Jisc shall notify the Client prior to appointing a sub-contractor. The Client may object to the appointment of any sub-contractor and Jisc shall reasonably take into account the views of the Client in appointing any such sub-contractor, but for the avoidance of doubt the appointment of any sub-contractor shall be at Jisc's absolute discretion and Jisc shall have no obligation to act in accordance with any objection raised by the Client. Information regarding the sub-contractors Jisc uses from time to time in connection with the performance of the Service can be found on the Service website.

5.2 Jisc may from time to time disclose Personal Data to its sub-contractors (or allow its sub-contractors to access Personal Data) for Processing solely in connection with the fulfilment of the Permitted Purpose.

5.3 Where Jisc uses a sub-contractor to Process Personal Data for or on its behalf, it will ensure that the sub-contractor contract (as it relates to the Processing of Personal Data) is on terms which are substantially the same as, and in any case no less onerous than, the terms set out in Clause 4 of this schedule.

5.4 Jisc shall remain liable to the Client for the acts, errors and omissions of any of its sub-contractors to whom it discloses Personal Data, and shall be responsible to the Client for the acts, errors and omissions of such sub-contractor as if they were Jisc’s own acts, errors and omissions to the extent that Jisc would be liable to the Client under this Agreement for those acts and omissions.

SCHEDULE 2: STATEMENT OF WORK TEMPLATE

Document Release

Version	Date	Change	Author (s)
0.1		Initial Draft	
0.2		Security Specialist Review	
1.0		Document Released	

Engagement Schedule

Jisc Reference Number	Start and end date
Ref:	Date from and To

Charges

- Refer to day rate card for applicable pricing
- Where out-of-hours support is required, a multiplier of 1.5 shall be applied to the applicable day rate

Charges Payment Profile
[insert anticipated invoicing profile]

Contacts

Client Contacts

Contact 1	Contact 2
Name	Name
Job Description	Job Description
Email address	Email address
Telephone Number	Telephone Number

Jisc Contacts

Contact 1	Contact 2
Name	Name
Job Description	Job Description
Email address	Email address
Telephone Number	Telephone Number

Service description

Summary

This Statement of Works defines the scope, deliverables, responsibilities, and pricing for Enhanced level incident response support provided by Jisc CSIRT to **Client Name**.

The objective is to support **Client Name** through all phases of a ransomware incident**,** analysis, containment, eradication, and recovery**,** leveraging Jisc's education-sector expertise and NCSC-aligned methodology.

About the service

Organisations across the education and research sectors face an increasingly complex and fast-paced cyber threat landscape. Timely detection, expert guidance, and effective response to cyber incidents are now essential components of organisational resilience. As one of the UK's NCSC-Assured Cyber Incident Response (CIR) providers for the education and research

community, Jisc delivers a comprehensive incident response service designed to help members prepare for, withstand, and recover from cyber attacks.

The Jisc Cyber Incident Response Service provides expert, assured support throughout the full incident lifecycle; Protect, Detect, Respond, and Recover, leveraging unique national-level capabilities to mitigate the impact of cyber incidents and strengthen long-term security posture.

Jisc operates Janet, the UK's National Research and Education Network (NREN). This infrastructure provides visibility and intelligence at a national scale, enabling Jisc to identify emerging threats and hostile activity targeting the sector. Through live network telemetry, primary threat intelligence feeds, and industry-leading analysis, the service delivers insights and containment options unavailable to traditional commercial providers.

This positions Jisc as the only NCSC-Assured CIR provider with:

- Access to nationwide education and research threat intelligence
- Enhanced network-level containment capabilities via the Janet Network
- Deep integration with sector-specific behaviours, infrastructure, and threat actors
- A long-established Cyber Incident Response Team trusted across UK academia

Together, these capabilities enable faster detection, more contextualised response actions, and more effective containment of active threats.

Service eligibility criteria

To utilise the Jisc Cyber Incident Response service, the following eligibility criteria must be met, and must continue to be met during the term of the service:

- **Janet Network Connection**: Clients wishing to purchase Jisc's Cyber Incident Response service must have a Janet Network IP Connection.

Service Scope

Initial Incident Assessment

As part of its enhanced service offering, Jisc CSIRT provides a rapid and structured initial incident assessment to help organisations understand the nature and impact of a ransomware event. This includes quickly identifying any signs of encryption activity, evidence of attacker access, and the overall scope of the compromise. The team conducts a focused review of SIEM and EDR/XDR outputs, network telemetry, and other relevant log sources to build an accurate picture of the incident. Jisc CSIRT also draws on insights from its in-house Cyber Threat Intelligence (CTI) team to assess potential indicators of data exfiltration and to evaluate threat actor behaviour, enabling more informed and targeted response actions during the early stages of the incident.

Deployment of Endpoint Detection & Response (EDR)

As part of its service, Jisc CSIRT provides comprehensive support for the deployment of Endpoint Detection and Response (EDR) to strengthen containment, eradication, and recovery efforts, while reducing the risk of re-compromise. This includes deploying, or assisting with the rapid deployment of, Jisc-approved EDR tooling across affected or high-risk systems. The team validates EDR coverage to ensure effective visibility across all key endpoints and uses the tooling to identify signs of persistence, unauthorised accounts, lateral movement, and the presence of malicious tools. Jisc CSIRT also leverages EDR capabilities to support quarantine and isolation actions and to continuously monitor for reinfection attempts. The deployment of EDR forms a critical element of the overall technical containment strategy.

Enhanced Network-Level Containment

Jisc CSIRT will utilise Jisc's network-level security capabilities provided as part of the Janet connection to enhance containment efforts:

- Support implementation of network-level blocks for C2 infrastructure, malicious IPs/domains, and ransomware distribution channels.
- Leverage Jisc's network architecture to limit lateral movement or continued threat actor access.
- Apply emergency network controls (where feasible) to prevent reinfection or outgoing traffic linked to data exfiltration.
- Provide recommendations for segmentation and temporary access restrictions.

Containment Support

Jisc CSIRT provides comprehensive containment support to help limit attacker activity and stabilise the environment during an incident. This includes advising on and assisting with endpoint isolation through EDR, as well as coordinating credential resets and the enforcement of multi-factor authentication to reduce the risk of further compromise. The team supports the removal of malicious tools, scripts, and persistence mechanisms, and guides organisations in improving account hygiene to restrict additional attacker movement. Where required, Jisc CSIRT also implements network isolation measures using Jisc's network-level containment capabilities to further protect affected systems and prevent ongoing intrusion.

Digital Forensics & Incident Response (DFIR)

Where required and for major incidents only, specialist Digital Forensics and Incident Response (DFIR) support is provided to investigate and analyse cybersecurity incidents in depth. This includes forensic evidence collection and preservation, analysis of compromised systems, identification of attacker activity, timelines, indicators of compromise (IOCs), and associated tactics, techniques and procedures (TTPs). DFIR findings support incident scoping, regulatory or legal requirements, root cause analysis, and inform remediation and post-incident security hardening activities.

Recovery & Eradication Guidance

Jisc CSIRT provides structured recovery and eradication guidance to help organisations safely restore operations following an incident. This support includes advising on safe restore

processes using known-clean backups and ensuring that appropriate validation is carried out before systems are reintroduced to the network. The team uses EDR tooling to assist with the eradication of attacker artefacts and confirms that systems are free from malicious activity. Jisc CSIRT also offers recommendations to prevent reinfection during the recovery phase, helping to ensure a stable and secure return to normal operations.

Post-Incident Security Hardening

Following stabilisation, Jisc CSIRT will provide comprehensive hardening guidance including:

- **Active Directory Hardening**
  - Review of privileged accounts and administrative tiering.
  - Identification of insecure configurations enabling lateral movement.
  - Recommendations for identity hygiene, MFA enforcement, and privileged access restructuring.
  - Guidance to align with the AD Tiering Model and Jisc/NCSC best practice.
- **Infrastructure & Endpoint Hardening**
  - Review patching posture, EDR coverage, and endpoint configuration.
  - Network segmentation recommendations.
  - Improvements to logging, monitoring, detection coverage, and SOC readiness.
  - Ransomware Resilience Recommendations
  - Backup protection improvements.
  - Credential handling hygiene.
  - Long-term mitigation actions aligned to NCSC Cyber Assessment Framework.

Reporting & Documentation

Jisc CSIRT provides structured reporting and documentation throughout the engagement to ensure clear visibility of incident progress. This includes daily status update calls supported by a presentation outlining the current state of containment, known attacker activity, immediate risks, active work items, progress made, and the required next steps. At the conclusion of the engagement, Jisc CSIRT supplies a final incident report summarising the response activities and outcomes. This report is advisory in nature and is not intended to serve as a formal forensic report.

Exclusions

- Malware reverse engineering
- Legal advice
- System administration or engineering work beyond guidance

Client Responsibilities

- Provide access to technical teams and systems.
- Deploy or assist deployment of EDR tooling as required.
- Implement recommended network and endpoint controls.
- Coordinate with third-party forensic provider.
- Maintain communication through a designated incident lead.

Jisc Responsibilities

- Provide qualified incident responders with sector-specific expertise.
- Use intelligence and tools available through the Janet connection.
- Act in accordance with NCSC best practice.
- Maintain confidentiality and handle data responsibly.
- Collaborate with the Client, Jisc SOC (if subscribed), and third parties.

Assumptions

- Support will be provided remotely.
- Support will be required during business hours (Mon-Fri 8am to 6pm), where agreed additional out of hours support can be provided at an additional cost.

Acceptance Criteria

- Containment measures applied
- Recovery guidance delivered
- Hardening guidance provided
- Final report issued

Special Conditions

- Special Condition 1

Client Environment

Captured during an initial scoping call, and updated as the incident response engagement progresses.

How to contact us

The following contact details are available for organisations to contact the relevant teams at Jisc.

 	Cyber Security Incident Response Team	Telephone: +44 (0) 300 999 2340 Email: **IRT@jisc.ac.uk** URL: **https://www.jisc.ac.uk/csirt**
	Relationship Manager	**https://www.jisc.ac.uk/contact/your-relationship-manager**
	Complaints	Email: **help@jisc.ac.uk** URL: **https://www.jisc.ac.uk/contact/complaints-and-escalations**
 	L1 Jisc Service Desk	Telephone: +44 (0) 300 300 2212 Email: **OPS@jisc.ac.uk**

Acceptance of this Statement of Work

The Statement of Work covers the breadth of engagement that will take place between Jisc and **Client Name**.

The Services to be provided by Jisc under this Statement of Work are subject to the Jisc Cyber Incident Response General Terms and Conditions.

By signing below, the Client confirms its acceptance of this Statement of Work and agrees to be bound by the Jisc Cyber Incident Response General Terms and Conditions.

Signed by a duly authorised officer/ representative for and on behalf of the Client:

……

Name:

Title:

Date: