SPECIFIC CONDITIONS N5 – CYBER SECURITY INCIDENT RESPONSE SERVICES

These Specific Conditions govern the Cyber Security Incident Response Services that may be provided by the Company under an Order Form, together with any other document or terms and conditions referred to in the Order Form including but not limited to the General Terms and Conditions for the Supply of Products and/or Services (the "**Conditions**"), which shall be deemed to be incorporated into the Contract for the performance of any Cyber Security Incident Response Services performed under these Specific Conditions.

1 DEFINITIONS

1.1 Capitalised terms used in these Specific Conditions shall have the following meanings for the purposes of these Specific Conditions only:

"Customer Environment"	means the Customer's IT infrastructure, including any systems, equipment, hardware, software, applications and web applications, which is to be subject to the Cyber Security Incident Response Services, as agreed in writing by the parties;
"Cyber Security Incident Response Services"	means the services provided by the Company to the Customer, remotely and/or at the Customer Premises, in response to a suspected and/or confirmed cyber security incident, in accordance with these Specific Conditions and as detailed in an Order Form; and
"Statement of Works"	means the Order Form or any other relevant contractual document setting out the scope of the Cyber Security Incident Response Services as referred to in the Order Form.

1.2 All other capitalised terms, which are not defined in paragraph 1.1 shall have the meanings stated in the Conditions.

2 COMMENCEMENT DATE AND TIME FOR PERFORMANCE

2.1 The Commencement Date of the Cyber Security Incident Response Services shall be the date specified as such in the Order Form or, if no date is specified, the date on which the Company commences provision of the Cyber Security Incident Response Services to the Customer.

2.2 Notwithstanding paragraph 2.1, the Customer shall not be entitled to cancel or terminate any Cyber Security Incident Response Services for convenience unless an express right to do so is set out in the Order Form. Any order for Cyber Security Incident Response Services shall be binding on the Customer from the Commencement Date until the date upon which the Company has delivered the Cyber Security Incident Response Services in full.

2.3 The Company will use its reasonable endeavours to deliver the Cyber Security Incident Response Services during the period (if any) stated in the Order Form or if no such period is stated or other time for performance is specified, the Cyber Security Incident Response Services shall be provided within a reasonable time from the Commencement Date.

3 SUPPLY OF THE CYBER SECURITY INCIDENT RESPONSE SERVICES

3.1 The Company will use its reasonable endeavours to supply the Cyber Security Incident Response Services as set out in the Order Form.

3.2 The Company may at any time without notifying the Customer make any changes to the Cyber Security Incident Response Services which it deems reasonably necessary to comply with any applicable safety or other statutory requirements, or which do not materially affect the nature or quality of the Cyber Security Incident Response Services.

3.3 The incident response hardware and software used by the Company in the performance of the Cyber Security Incident Response Services includes the Company's proprietary software. The Company has taken reasonable steps to validate such hardware and software as being free from malicious software or code.

3.4 The Company will advise the Customer on steps to be taken to help to prevent the Customer Environment being further infected with malicious software originating from the original attack, including both those actions to be undertaken by the Customer and those to be undertaken by Company Personnel on behalf of the Customer.

3.5 The Company will agree with the Customer how information will be removed and archived from both the reporting environment(s) and the attacked platform(s), and which party will be responsible for undertaking these actions. The Company's incident response methodology includes an assessment of the Customer's data retention needs at the conclusion of the incident.

3.6 The Company is a specialist information and cyber-security service provider and complies fully with all local legislation and regulation relating to information and cyber security including reporting requirements. The Company publishes advice on the implications of computer/cyber crime and the actions required to prevent a breach of legislation, and will provide additional advice tailored to the scope of the Customer's operations as appropriate.

3.7 Notwithstanding any other provision in this Contract, including any Statement of Works or other attachment to this Contract, the Company shall be under no express or implied fitness for purpose obligation in relation to the Cyber Security Incident Response Services. The Company's liability (if any) under this Contract shall be limited to the exercise of reasonable skill, care and diligence to be expected of an appropriately qualified person experienced in carrying out activities of a similar nature, size, complexity and value to the scope of the Cyber Security Incident Response Services.

3.8 If, for any reason, any Company Personnel engaged in the Cyber Security Incident Response Services become unavailable for the performance of the Cyber Security Incident Response Services, the Company will as soon as reasonably practicable substitute a suitably skilled and experienced replacement.

3.9 The Customer covenants to the Company that it is the sole owner of, or has legal authority to grant access to, the Customer Environment to be accessed by the Company in providing the Cyber Security Incident Response Services. This includes authority to remotely scan and/or test related systems and all other authority to access systems given by the Customer to the Company through allocated access or account activation.

3.10 The Customer will indemnify the Company for any loss, damages, costs, expenses or other claims, howsoever caused through any breach of clause 3.9.

3.11 The parties agree that nothing in this Contract shall render the Company Personnel an employee, worker, agent or partner of the Customer and the parties agree that this is a contract for services and not of employment or secondment of the Company Personnel.

4 SUPPLY OF THE CYBER SECURITY INCIDENT RESPONSE SERVICES (WITH RETAINER)

4.1 Where stated in the Order Form that the Customer has purchased a retainer, the following terms shall apply in addition to the remainder of these Specific Conditions:

4.1.1 the Minimum Term shall be as set out in the Order Form, or if no Minimum Term is specified, twelve (12) calendar months from and including the Commencement Date;

4.1.2 subject to notification by the Customer by telephone to the incident response telephone number notified in writing by the Company for these purposes, the Company shall use reasonable endeavours to respond to any cyber security incident within:

(a) one (1) hour where stated in the Order Form that the retainer is silver or gold level; or

(b) four (4) hours where stated in the Order Form that the retainer is bronze level; and

4.1.3 any rates or discounts stated in the Order Form shall be held for the duration of the Minimum Term.

5 CUSTOMER OBLIGATIONS

5.1 The Customer shall, at its own expense:

5.1.1 within a sufficient timeframe, make available to the Company all necessary Customer Input Materials and reasonable assistance relating to the Cyber Security Incident Response Services or required by the Company to perform the Cyber Security Incident Response Services;

5.1.2 ensure the accuracy and retain duplicates of any Customer Input Materials;

5.1.3 insure against the accidental loss or damage of any Customer Input Materials and the Customer agrees and acknowledges that the Company shall have no liability for any such loss or damage;

5.1.4 make available to the Company any Customer Representatives familiar with the Customer Environment and/or requirements of the Cyber Security Incident Response Services, ensuring that such Customer Representatives will fully cooperate with the Company Personnel to enable the Cyber Security Incident Response Services to be performed; and

5.1.5 inform the Company of any changes to the Customer Environment which may affect the provision of the Cyber Security Incident Response Services.

5.2 The Company shall have no liability for any failure to provide the Cyber Security Incident Response Services under these Specific Conditions to the extent caused by the Customer's failure to meet any of the obligations set out in paragraph 5.1.

6 CHARGES

6.1 The Charges for the Cyber Security Incident Response Services will be as identified in the Order Form.

6.2 Where stated in the Order Form that the Customer is to pay a retainer fee:

6.2.1 such fee will be invoiced annually in advance or as otherwise stated in the Order Form; and

6.2.2 the Company shall invoice the Customer monthly in arrears for subsequent Charges incurred, including but not limited to any professional services provided, calculated in accordance with any rates or discounts stated in the Order Form.

6.3 Where stated in the Order Form that the Customer is to pay a minimum initial payment:

6.3.1 such payment will be invoiced on or around the Commencement Date and shall be payable by the Customer within 48 hours or as otherwise stated in the Order Form;

6.3.2 such payment shall be used to offset subsequent Charges incurred, including but not limited to any professional services provided, calculated in accordance with any rates or discounts stated in the Order Form;

6.3.3 once such payment has been fully offset in accordance with paragraph 6.3.2, the Company shall invoice the Customer monthly in arrears for any further Charges incurred, including any professional services provided, calculated in accordance with any rates or discounts stated in the Order Form; and

6.3.4 any unused portion of a minimum initial payment shall be non-refundable but may, within a period of six months of the Commencement Date and at the Company's sole discretion, be used to offset subsequent Charges in relation to any future suspected and/or confirmed cyber security incident, or for other cyber security related consultancy services provided by the Company.

6.4 Unless stated otherwise in the Order Form, in addition to the Charges, the Company will invoice the Customer on a monthly basis in arrears, all other fees, disbursements and other expenses including travel and subsistence incurred by the Company under this Contract together with such additional Charges, which in the Company's discretion (acting reasonably and calculated in accordance with the Company's standard rates subject to any discount stated in the Order Form), are chargeable as a result of the Customer's instructions or the Company performing additional services at the Customer's request that were not expressly set out in the Order Form or Statement of Works.

6.5 Any invoices submitted to the Customer in accordance with paragraph 6.4 shall be payable within 15 days of the invoice date.

6.6 The Company will not be obliged to provide the Cyber Security Incident Response Services unless all sums due under this Contract are received as provided for in this Contract.

6.7 Any professional services utilised in the provision of the Cyber Security Incident Response Services shall be tracked daily by the Company in 15 minute allocations, with records available on request.

7 WARRANTIES AND LIABILITY

7.1 The Customer acknowledges that the Company is not guaranteeing that the Customer will have a completely secure Customer Environment as a result of the Cyber Security Incident Response Services, as no test, product or service can offer protection against all possible security breaches. The Customer acknowledges that the Cyber Security Incident Response Services are designed to contribute towards its overall IT security strategy.

7.2 The Company shall not be liable for any loss or damage to the Customer Environment which is caused by any existing weakness (or defect) in the Customer Environment that is discovered or initiated by the provision of the Cyber Security Incident Response Services from the Company.

7.3 The laws of England and Wales apply to the provision of the Cyber Security Incident Response Services . Some of these laws have particular relevance to technical testing engagements, particularly the Computer Misuse Act, Human Rights Act, and Data Protection Act. Through agreement of clause 3.9 of these Specific Conditions, the Customer agrees to indemnify the Company against prosecution for providing the Cyber Security Incident Response Services.