



INCURSION CYBER SECURITY

Incursion Cyber Security Terms and Conditions



Incursion Cyber Security Terms and Conditions

1. Definitions

Business Day – A Day other than a Saturday, Sunday or public holiday in England.

Captured Data – Data (including PII) belonging to the Customer accessed by or discoverable by Incursion Cyber Security (ICS) as a result of testing. This does not include data (including PII) communicated to ICS in the ordinary course of the Contract.

Charges – The amount payable by the Customer to ICS for the provision of services.

Conditions - These terms and conditions as detailed within this document.

Contract - The contract between the Customer and ICS for the supply of Services in accordance with these Terms and Conditions, any Schedules and the Proposal including any additional documents expressly referenced.

Customer - The purchasing party or any party agreeing to purchase Services from ICS.

Customer Materials - all materials, equipment and tools, drawings, specifications and data supplied by the Customer to ICS.

Deliverables – Any documents, products and materials developed by ICS as part of or in relation to the Services in any form.

Party – Either ICS or the Customer when referenced as individual entities.

Parties – Both ICS and the Customer when referenced as a single entity.

Personal Data – Personal Data as per Data Protection Legislation. It related only to Personal Data or any part of such Personal Data to which either party may be granted access in the course of the provision of Services.

Proprietary Information – All information of a confidential or proprietary nature in any form be it provided orally or in an electronic format, and which is either marked as or reasonably believed to be confidential (or some similar legend) be it registered or unregistered.

Proposal – A document and any referenced sub document detailing the services offered to the Customer including a description of work, pre-requisite information, timescales and cost to carry out the requested services.

ICS – Incursion Cyber Security Ltd, registered in England under company number 14303576 at the registered office address of 9c Shears Drive, Amesbury, Wiltshire, SP4 7XU.

Services – Services, including without limitation any Deliverables, to be provided by the ICS pursuant to the Terms and Conditions and Proposal.

System – The target of ICS testing as defined by the Customer.

Test Start Date – The day on which ICS is to start test, as set out in the Proposal.

Test End Date – The day on which ICS is to cease testing. Reporting will continue after this date; ICS will not attempt to access Customer Material after this date without express written permission from the Customer.

Testing – All and any security reviews and assessments performed by ICS on the Customer's System.

2. SUPPLY OF SERVICES

2.1 ICS shall perform the Services (see section 15. Service Offerings for a list of services) in accordance with these terms and conditions. They shall govern the Contract to the entire exclusion of all other terms and conditions (including any terms or conditions which the Customer purports to apply under any purchase order, confirmation of order, specification or other document).

2.2 Each order made by the Customer for Services supplied by ICS shall be deemed as an offer by the Customer to purchase Services pursuant to these terms and conditions.

2.3 The Customer acknowledges and accepts that during the performance of Testing, the System will be exposed to simulated hacking activity via whatever means of connectivity provided to ICS. While unlikely,



Incursion Cyber Security Terms and Conditions

Testing may cause interruptions to System functionality, cause damage and/or corruption to the Customer's computer systems. The Customer shall seek to enable Testing at times selected to minimise potential detrimental impact. The Customer shall also make full back-up copies of all data on the System in advance of any Testing.

2.4 Where ICS is required to provide Services on a Customer's or third-party premises, the Customer shall be responsible for arranging, permits, licences or other permissions necessary to enable ICS's employees and representatives to gain access to, and perform testing on such premises. ICS's employees and representatives working on the Customer's premises shall abide by such regulations detailed in advance of arrival to such premises.

3. CUSTOMER OBLIGATIONS

3.1 To enable ICS to provide the agreed upon Services, the Customer shall, prior to test commencement, obtain appropriate instructions, licences and authorisations including third party licences, approvals and consent. This is to include but is not limited to authorisations required for compliance within the provisions of the Computer Misuse Act 1990.

3.2 The Customer is requested to notify ICS of any changes to the System between beginning pre-test negotiations and 2 working days prior to the test start date. If changes are made, ICS reserve the right to change the proposal to accommodate the testing or reschedule the date of testing. ICS will not be liable for any loss, damage or expense suffered by the Customer because of actions taken by ICS due to changes made prior to Test Start Date.

3.3 The Customer is requested not to modify or change the System between the Test Start Date and Test End Date. If any such change is made to the System, the Customer shall communicate the nature of the change to ICS immediately. ICS reserve the right to change the proposal to accommodate the testing or reschedule the date of testing. ICS will not be liable for any loss, damage or expense suffered by the Customer because of actions taken by ICS due to changes made between Test Start Date and Test End Date.

3.4 The Customer shall make available relevant personnel and undertake monitoring of the Testing.

4. PRICE AND PAYMENT TERMS

4.1 ICS shall invoice the Customer following receipt by the Customer of all Deliverables. The Customer shall pay ICS the Charges by bank transfer to a bank account nominated by ICS within 30 days of submission of an invoice by ICS. Should payment of undisputed invoices become 7 calendar days overdue, a 10% charge will be added to the due amount. Should payment of undisputed invoices become 30 calendar days overdue the amount will be passed to a debt collection agency.

4.2 Unless otherwise stated, Charges are exclusive of any Value Added Tax, sales tax or similar, and any taxes, duties or imposts chargeable thereon shall be payable by the Customer as an additional charge. All payments due from the Customer shall be made without deduction of any setoffs, taxes, charges and other duties (including withholdings or income taxes).

4.3 If the Customer disputes any invoice or part thereof, the Customer shall immediately notify ICS in writing of the reasons. The Parties shall seek to resolve the dispute within 14 days of notification, the Customer shall pay the undisputed portion of the Charges within 30 days of submission of the invoice as per Clause 4.1. In the absence of a resolution the provisions of Clause 12 (Dispute Resolution) shall apply. Upon resolution of the dispute, an agreed upon sum shall be alongside the undisputed charge or, in instances in which the undisputed charge has been paid, immediately to ICS, together with any interest due under Clause 4.4.

4.4 If the Customer fails to pay ICS any sum due, the Customer will be liable to pay interest to ICS on such sums from the due date for payment at an annual rate equivalent to the Bank of England base lending rate plus 4 percentage points, accruing on a daily basis from the date the original Charges were due payment as per Clause 4.1

5. WARRANTY

5.1 ICS Testing is intended to aid in the verification of the Customer System's through a combination of automated and manual simulated attacks. Testing does not guarantee that a System is or will be immune to attack or unauthorised access by malicious actors.

5.2 ICS warrants that it will provide the Services with reasonable care and skill. Furthermore, ICS will conduct testing and provide the Deliverables in accordance with the standards set down by NCSC

5.3 Subject to Clause 5.4, if any Deliverable is found to not meet Clause 5.2 resulting from the performance of the Services, ICS shall at its option either re-perform the relevant Services or part thereof or refund such proportion of the Charges paid to ICS by the Customer for the Services as is reasonable.

5.4 ICS shall have no liability of any kind for breach of its warranty in Clause 5.2 where such breach is due to a failure of the Customer to comply with its obligations under the Contract, or any defect in, or failure of, the



Incursion Cyber Security Terms and Conditions

Customer's (or a third party's) System, or a failure by the Customer to follow ICS's reasonable oral or written instructions in connection with the performance of the Services.

5.5 The Customer acknowledges and accepts that the warranties at Clause 5.2 and associated remedies at Clause 5.3 are its sole and entire warranties and remedies in connection with the performance by ICS of the Services under this Contract. All other representations and warranties which may otherwise be implied (by statute or otherwise) in relation to the Services are excluded to the fullest extent permitted by law.

6. LIMITATION OF LIABILITY

6.1 The following provisions set out the entire financial liability of ICS (including any liability for the acts or omissions of its employees, agents and sub-contractors) to the Customer arising under or in connection with the Contract in respect of any breach of the Contract and any representation, statement or tortious act or omission including negligence.

6.2 Nothing in the Contract shall exclude or limit the liability of ICS for death or personal injury caused by ICS's negligence, fraud committed by ICS (including fraudulent misrepresentation) or any other matter it would be illegal, or a breach of a statutory provision, for ICS to exclude or attempt to exclude liability.

6.3 The Customer acknowledges that, by its nature, Testing may cause damage to hardware, software, data and systems or parts thereof (including but not limited to the System). By agreeing to Testing, the Customer accepts that ICS's liability to the Customer shall be excluded in respect to any damage caused by or arising from Testing, except where the damage is caused by ICS's negligence or wilful misconduct.

6.4 Subject to Clause 6.2, ICS's aggregate liability in contract, tort (including negligence or breach of statutory duty), misrepresentation or otherwise, arising in connection with the performance or contemplated performance of this Contract shall be limited to the lesser of 100% of the Charges and £100,000.

6.5 Subject to Clause 6.2, ICS shall not be liable to the Customer for any indirect, special or consequential loss or damage; any loss of profit, loss of business, depletion of goodwill or like loss; any loss, damage or liability to the extent caused by the negligence, wilful misconduct or other fault of the Customer, its employees, agents or contractors or a breach by the Customer of this Contract; in each case howsoever caused, including without limitation negligence or breach of statutory duty or misrepresentation, arising out of or in connection with the Contract.

7. CONFIDENTIALITY

7.1 Without prejudice to the Parties rights elsewhere in this Contract, all Proprietary Information exchanged between the Customer and ICS shall be handled as COMMERCIAL-IN-CONFIDENCE in accordance with this Clause unless an alternate protective marking is expressly assigned.

7.2 Neither Party shall use, disclose or knowingly permit to be disclosed to any person (except those employees, agents or sub-contractors who have a need to know for the purpose of supplying agreed upon Services) any Proprietary Information of the other Party without written consent of the other Party. Both Parties shall ensure that employees, agents or sub-contractors are subject to obligations of confidentiality to a minimum standard as that between the two Parties.

7.3 The obligations of confidentiality owed by the Parties to each other as set out in this Clause shall remain in force upon completion (or earlier determination) of the Contract but shall not apply to information which is in or enters the public domain (otherwise than by a breach of the receiving Party's confidentiality obligations); is known without restriction to the receiving Party at the time of disclosure without breach of any obligation of confidentiality; becomes known to the receiving Party without restriction from an independent source having the right to convey it; is shown to the reasonable satisfaction of the originating Party to have been generated independently by the receiving Party; or is required to be disclosed by law or a competent regulatory body.

8. DATA PROTECTION

8.1 Each Party warrants to the other that it will process any Personal Data in compliance with the General Data Protection Regulation (EU/2016/279) the Privacy and Electronic Communications (EC Directive) Regulations 2003 the Data Protection Act 2018 the Computer Misuse Act 1990 and all applicable laws and regulations effective in the UK relating to the processing of personal data and privacy each as may be updated, amended, re-enacted or replaced ("Data Protection Legislation").

8.2 ICS will only process Captured Data for purposes expressly authorised by the Customer.

8.3 As part of the provision of Services, ICS will analyse and process Captured Data in the creation of the agreed upon Deliverable. Deliverables will not include personal data unless expressly requested by the Customer. Upon the Customer's acceptance of the Deliverables, ICS will securely delete Captured Data. ICS will store deliverables in



Incursion Cyber Security Terms and Conditions

a secure archive to facilitate the provision of future Services. Unless expressly requested by the Customer, deliverables will be deleted within 10 years.

8.4 The Customer shall ensure that it has obtained and will maintain all necessary consents and authority required under Data Protection Legislation to allow ICS to carry out its obligations under the Contract.

8.5 The Customer will immediately inform ICS if any of the consents required under Clause 3.1 or Clause 8.4 is revoked or changed in any way which impacts on ICS's rights or obligations to provide agreed upon Services.

8.6 When processing Personal Data, The Parties will:

8.6.1 process Personal Data no further than is necessary to carry out its obligations under the Contract;

8.6.2 ensure that its staff are subject to a duty of confidence with respect to such Personal Data;

8.6.3 not cause or permit such Personal Data to be transferred outside of the European Economic Area;

8.6.4 not use Customer Personal Data for marketing or promotion purposes;

8.6.5 not disclose Personal Data to third parties without the express consent of the other Party.

8.7 The Parties do not intend ICS to act as Data Processor on behalf of the Customer except to the extent required to meet obligations as set out in Clauses 8.2 and 8.3. For the purposes of those obligations, the Parties agree that:

8.7.1 the scope, nature and purpose of the processing is as described in this Contract;

8.7.2 the duration of the processing shall not exceed that required to comply with obligations set out in Clause 8.3;

8.7.3 the types of and category of Personal Data may be of any type contained within the systems subject to ICS Testing;

8.7.4 ICS will not use a third party to process Personal Data;

8.7.5 the Parties will provide each other with assistance and cooperation to enable compliance with obligations under the Data Protection Legislation; and

8.7.6 the Parties will inform each other if it is thought that the other Party's instructions could breach Data Protection Legislation.

8.8 each Party will accept, at its own cost, the inclusion of any reasonable data protection clause into this Contract in order to comply with Data Protection Legislation.

8.9 In exceptional circumstances ICS may be required to report information relating to the Captured Data to a public authority in order to comply with legal and regulatory obligations. In such circumstances ICS will where possible inform the Customer in advance and take reasonable account of the Customer's representations in respect of any required disclosure.

8.10 The Customer shall, to the extent permitted by law, at all times during and after the term of the Contract, indemnify ICS against all losses, fines, damages, costs, expenses and other liabilities (including legal fees) incurred by, awarded against or agreed to be paid by ICS arising from any processing of Captured Data by ICS if carried out in accordance with the Contract and arising from the Customer's instructions.

9. CANCELLATION OR RESCHEDULING

9.1 The Customer acknowledges that Services will be carried out on the dates offered to and accepted by the Customer by ICS.

9.2 In accordance with Clause 9.3, the Customer may at any time prior to the Test Start Date, cancel or reschedule all or some of the Services by notice in writing.

9.3 The Customer acknowledges that cancellation or rescheduling of the provision of Services at short notice would make reallocation of ICS's committed resources to alternative tasks impractical likely resulting in financial loss for ICS. As a result, the Customer agrees that, for any notice of cancellation or rescheduling received by ICS prior to the Test Start Date, ICS shall have the right to charge a percentage of the Charges for the cancelled or rescheduled Services in accordance with the following table:



Incursion Cyber Security Terms and Conditions

Working days before scheduled provision of the Services that notice is received by ICS:	ICS entitled to charge (% of Charges for cancelled or rescheduled Services)
≥ 10	0%
5-10	50%
<5	100

9.4 On receipt of written notice given of cancellation or rescheduling of Service in accordance with Clause 9, ICS shall, if requested by the Customer, reschedule the provision of Services as soon as reasonably practicable.

10. TERMINATION FOR BREACH

10.1 Without prejudice to any rights of action or remedy which have accrued or shall accrue, either Party may at any time by written notice terminate the Contract if:

10.1.1 the other Party is in breach of any material obligation under the Contract and where the breach is capable of remedy, the other Party has failed to remedy within 30 days of written notice of a requirement of remediation

10.1.2 any distress, execution or other process is levied upon any of the assets of the other Party

10.1.3 the other Party enters into any compromise or arrangement with its creditors, commits any act of bankruptcy or if an order is made or an effective resolution is passed for its winding up (except for the purposes of amalgamation or reconstruction as a solvent company) or if a petition is presented to court, or if a receiver and/or manager, administrative receiver or administrator is appointed in respect of the whole or any part of the other Party's undertaking or assets

10.1.4 the other Party ceases or threatens to cease to carry on its business

10.1.5 the financial position of the other Party deteriorates to such an extent that in the opinion of the terminating Party the capability of the other Party adequately to fulfil its obligations under the Contract has been placed in jeopardy.

10.2 Where ICS terminates the Contract under Clause 10.1, the Customer shall within 7 days' pay to ICS all outstanding Charges invoiced by ICS under the Contract at the date of termination plus a fair and reasonable price for work done or in progress but not invoiced for at the date of termination, all costs (including overheads) and liabilities incurred by ICS arising out of or resulting from termination, including but not limited to suppliers' and sub-contractors' cancellation charges and a sum in respect of the profits which ICS would have made under the Contract but for its termination.

10.3 All Clauses which are implicitly intended to survive termination of this Contract shall remain in force after termination.

11. FORCE MAJEURE

11.1 ICS shall not be liable for any failure or delay in conducting Testing, producing Deliverables or any other obligation under the Contract if the failure or delay is due directly or indirectly to any cause beyond the reasonable control of ICS. Causes beyond ICS control shall include but not are not limited to any act of God, accident, civil disturbance, emergency, explosion, fire, flood, governmental actions, strikes, war ; any major plant or equipment or power failure or shortage which has a material effect on the operations of a facility; failure of any telecommunication facility such as but not limited to telephone or internet connection; or the postponement of any trial or test as a result of unsafe conditions ("Force Majeure Event").

11.2 Either Party affected by a Force Majeure Event will provide notice to the other Party within a reasonable timeframe specifying the nature of the Force Majeure Event, its expected duration and details of steps being taken



Incursion Cyber Security Terms and Conditions

to mitigate it. The time for performance of the obligations of the affected Party shall be extended by a period equivalent to that during which performance is prevented or delayed. If a Force Majeure Event persists for longer than 30 days from the date of service of notice either Party may terminate the Contract with 7 days written notice.

11.3 Termination for Force Majeure shall be without prejudice to any right or remedy accrued under the Contract prior to termination.

12. DISPUTE RESOLUTION

12.1 If any dispute arises out of or in connection with this Contract ("Dispute") the Parties undertake that, prior to the commencement of any legal proceedings pursuant to Clause 13, they will seek to have the Dispute resolved amicably by use of an alternative dispute resolution procedure acceptable to both Parties. Either Party will be entitled to initiate the process by written notice to the other.

12.2 If the Dispute has not been resolved to the satisfaction of either Party within 30 days of initiation of the procedure pursuant to Clause 12.1 or if either Party fails or refuses to participate in or withdraws from participating in the procedure then either Party may deal with the Dispute through legal proceedings issued in accordance with Clause 13.

13. MISCELLANEOUS

13.1 A notice given under or in connection with the Contract must be in writing and may be delivered by email, hand or sent by post using a signed for recorded delivery service to the ICS Project Manager or registered business address or to the address of the Customer as set out in the Contract or to any such other address as either ICS or the Customer may substitute by notice to the other Party. Notice shall be deemed given if sent by a signed for recorded delivery service once the Royal Mail confirm delivery; by email at the time of transmission (unless a delivery failure notification is received); or delivered by hand on the day of delivery. This Clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

13.2 A person who is not a Party to this Contract shall have no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Contract. This Clause does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

13.3 Failure by either Party to enforce, at any time or for any period, any one or more of the terms or conditions of the Contract shall not be a waiver of them or of the right at any time subsequently to enforce all terms and conditions of the Contract.

13.4 The Contract constitutes the entire communications not superseded by later communication or written document between the parties in connection with its subject matter and neither Party has relied on any representation or promise except as expressly set out in the Contract.

13.5 If any provision of these terms and conditions is held by any competent authority to be illegal, void, voidable, invalid, unenforceable or unreasonable in whole or in part ("Void") it shall, to the extent it is Void be deemed severable and the validity of the other provisions of these terms and conditions and the remainder of the provision in question shall not be affected.

14. GOVERNING LAW AND JURISDICTION

14.1 The Contract shall be governed by and construed in accordance with the law of England and Wales.

14.2 Each Party hereby irrevocably submits to the exclusive jurisdiction of the courts of England and Wales provided that each Party shall have the right to enforce a judgment of the courts of England and Wales in a jurisdiction in which the other Party is incorporated or in which any assets of the other Party may be situated.



Incursion Cyber Security Terms and Conditions

15. ICS SERVICE OFFERINGS

15.1 ICS offer the following services:

15.1.1 Internal Infrastructure assessments. An evaluation of an organisation's internal networks with the aim to identify vulnerabilities, obtain sensitive information and gain control of the assets.

15.1.2 External Infrastructure assessments. An evaluation of a organisation's externally facing IT assets with the aim to identify vulnerabilities and routes into a company's internal infrastructure.

15.1.3 Web Application Assessments. An analysis of web applications in order to identify security vulnerabilities that could be exploited to compromise an organisation and its web application user base.

15.1.4 Web Services Assessments. A comprehensive evaluation of web services (APIs), in order to identify security vulnerabilities that could be leveraged to compromise an organisation and its user base.

15.1.5 Cloud Security Reviews. A review of an organisation's cloud infrastructure, focusing on the security configuration of the wider cloud deployment. The aim is to ensure cloud environments align with security best practice to a predefined recommended level.

15.1.6 Windows and Unix Build Reviews. In-depth analysis of the configuration and setup of Windows and Unix systems, focusing on identifying security misconfigurations, unnecessary services, and non-compliance with best practices.

15.1.7 Network Device Configuration Reviews. A detailed examination of the configuration network devices to identify misconfigurations or outdated settings that contradict security best practice or may lead to security vulnerabilities.

15.1.8 Firewall Ruleset Reviews. An analysis of firewall rulesets, aimed at identifying overly permissive rules or configuration errors that could expose the network to risks.

15.1.9 Wi-Fi Assessments. An evaluation of Wi-Fi networks to uncover vulnerabilities and malicious access points. The aim is to ensure that the users of an organisation's wireless networks are secure against eavesdropping and the organisations private networks are protected against unauthorised access.

15.1.10 Physical Security Review. A covert and overt examination of an organisation's physical security measures, including but not limited to access controls, surveillance systems, and environmental safeguards. The aim is to identify potential physical threats to IT infrastructure and data, assessing the effectiveness of current security protocols.

15.1.11 Red Teaming. A proactive approach involving simulated attacks to test the effectiveness of technical and physical security measures including employee awareness. The aim is to as closely as possible replicate the actions of a malicious individual or group targeting an organisation. This is done with as few restrictions in scope as possible and minimal knowledge of the engagement within the organisation.

15.1.12 Incident Response. A combination of proactive preparation and reactive support assisting the company to efficiently manage and mitigate the impact of security breaches and cyber incidents.

15.1.13 Business Continuity Planning. Assistance in developing comprehensive strategies and plans to ensure an organisation's critical business functions can continue during and after disruption, minimising downtime and financial impact.

15.1.14 Training. Tailored training packages aimed at employees in various aspects of IT security, including best practices, threat awareness, and response procedures. The aim is to enhance an organisation's overall security posture by equipping staff with the knowledge and skills necessary to identify, prevent, and respond effectively to potential security threats and incidents.

15.1.14 Cyber Essentials (CE) and Cyber Essentials Plus (CE+) Assessments. Consultancy and Assessment of businesses and companies in line with the IASME/NCSC guidance to award CE and CE+ certification.



Incursion Cyber Security Terms and Conditions

15.2 Our test methodologies constantly evolve to ensure ICS offerings are at the forefront of the IT Security industry. We provide extensive remediation advice for all findings reported following an assessment taking a business risk approach, in which the impact of remediation advice is balanced with the impact to the business.

15.3 The service list above is accurate at the point of issuing this document, however ICS continually review, amend, and add services to offer the greatest value to our customers. The latest service list can be obtained by contacting ICS through your primary point of contact or one of the following mailboxes:

- lewis.lockwood@incursion-security.co.uk
- gareth.paterson@incursion-security.co.uk



Incursion Cyber Security Terms and Conditions

16. DOCUMENT CONTROL

16.1 This is a rolling document, below are the details of the latest revision

Version	Author	Date	Review	Date
1.0	Lewis Lockwood	16/11/2023	Gareth Paterson	16/11/2023
1.1	Lewis Lockwood	27/08/2024	Gareth Paterson	28/08/2024
1.2	Lewis Lockwood	01/10/2024	Gareth Paterson	01/10/2024