SERVICE-SPECIFIC MODULE
MANAGED VULNERABILITY SCANNING SERVICES
Supplementing NCC Group Terms and Conditions for the Supply of Services (UK), General Terms and Conditions

1 Contract Structure and Interpretation

1.1 This Service-Specific Module sets out the terms and conditions applicable to managed security services and is to be read in conjunction with the General Terms and Conditions.

1.2 The General Terms and Conditions apply to this Service-Specific Module and the capitalised terms in this Service-Specific Module shall have the same meaning ascribed to them in the General Terms and Conditions unless stated otherwise herein.

2 Definitions:

"Cyber Essentials" means the self-assessment verification certification issued and governed by the IASME Consortium Limited;

"Cyber Essentials Services" means the Cyber Essentials services detailed in the Statement of Works;

"Cyber Essentials Plus" means the technical audit certification issued and governed by the IASME Consortium Limited;

"Cyber Essentials Plus Services" means the Cyber Essential Plus services detailed in the Statement of Works;

"**Managed Vulnerability Scanning Services**" means the managed vulnerability scanning services provided by NCC Group including PCI ASV Scanning Services, Cyber Essentials Services and Cyber Essentials Plus Services;

"**MVSS Portal**" means any web-based facility through which the Client can access the results of the Managed Vulnerability Scanning Services;

"**PCI**" means Payment Card Industry;

"**PCI ASV**" means Payment Card Industry Approved Scanning Vendors;

"**PCI SSC**" means Payment Card Industry Standards Security Council;

"**PCI ASV Scanning Services**" means a service for carrying out regular PCI ASV scanning on the Client's systems as described in the Statement of Works;

"**Scheduled Days Cost**" means Fees that correspond to the days scheduled by NCC Group for provision of the Services or the relevant Service Portion (as applicable); and

"**System**" means the systems and networks which the Client requires to be security tested or security monitored and/or scanned as part of the Services, together with any software, systems, networks, premises, equipment, data structures, protocols, computers, programs, data, hardware and firmware linked to the same and data passing across or contained in any of the foregoing.

3 Client's Duties:

3.1 The Client agrees:

3.1.1 to obtain consent from its ISP and any third-party suppliers of the System for the Managed Vulnerability Scanning Services to be carried out and, when requested by NCC Group, to provide written evidence of such consent and to notify relevant employees that the Managed Vulnerability Scanning Services are to be carried out and that they may be monitored;

3.1.2 to ensure at least one employee has substantial experience and knowledge of the Systems and project management and will act as liaison between the Client and NCC Group, responding promptly to any queries or requests for information;

3.1.3 to co-operate with NCC Group and to provide it promptly with such information about the System as are reasonably required by NCC Group;

3.1.4 that it shall properly and fully back-up all data and copies of all computer programs and data which are held immediately prior to commencement of the Managed Vulnerability Scanning Services, and which may be affected by the provision of the Managed Vulnerability Scanning Services and, where appropriate, make back-ups not less than daily to enable straightforward recovery and/or reinstatement of any and all data and/or computer programs lost or damaged (whether in whole or part) through performance of the Managed Vulnerability Scanning Services;

3.1.5 that, whilst NCC Group will use reasonable endeavours to avoid disruption to the Client's network disruption to the Systems and/or possible loss of or corruption to data and/or software may occur and the Client agrees to make back-ups pursuant to clause 3.1.4 of this Service-Specific Module;

3.1.6 to notify NCC Group in writing in advance or as soon as possible after becoming aware of any periods during which NCC Group should not perform the Managed Vulnerability Scanning Services or should cease performing the Managed Vulnerability Scanning Services due to critical business processes (such as batch runs) or if any part of the System is business critical to enable NCC Group to modify its testing approach if necessary, with the client's consent;

3.1.7 to use any software and/or hardware which NCC Group (and its Affiliates) supplies to the Client as part of the Managed Vulnerability Scanning Services for lawful purposes, solely to the extent necessary to receive the benefit of the Managed Vulnerability Scanning Services and in accordance with any applicable licence terms and NCC Group's (and its Affiliates) instructions provided from time to time;

3.1.8 to assume all liability and to indemnify, keep indemnified and hold harmless NCC Group, its Affiliates and its and their respective officers, employees, agents, contractors and sub-contractors in full and on demand from and against any and all third party claims (including claims for alleged or actual infringement of Intellectual Property Rights), losses, damages, demands, costs, expenses, fees (including court and legal fees) and liabilities (in each case whether direct, indirect or consequential) of whatever nature suffered, incurred or sustained by NCC Group (or its Affiliates) as a result of the provision of the Managed Vulnerability Scanning Services, save to the extent that any such losses, damages, demands, costs, expenses, fees or liabilities are incurred as a direct result of NCC Group's breach of the Contract;

3.1.9 to ensure there is sufficient bandwidth to enable NCC Group to perform the Managed Vulnerability Scanning Services;

3.1.10 that NCC Group may be obliged to disclose assessment results to PCI SSC or any then current member of PCI SSC, for any PCI work carried out by NCC Group for the Client;

3.1.11 that, in respect of Cyber Essentials Services and Cyber Essentials Plus Services:

3.1.11

3.1.11.1 NCC Group may be obliged to disclose assessment results to IASME and/or the National Cyber Security Centre; and

3.1.11.2 other than as set out in a Statement of Works, NCC Group will not audit or otherwise test or verify the information provided to it by the Client or on behalf of the Client in the course of the Cyber Essentials Services and Cyber Essentials Plus Services. NCC Group shall be entitled to rely on all information provided to it by the Client and on the Client's decisions and approvals in connection with the Cyber Essentials Services and Cyber Essentials Plus Services and to assume that all such information provided to NCC Group from whatever sources is accurate, complete and not misleading.

3.1.12 that ownership of all Intellectual Property Rights in the MVSS Portal remains with NCC Group;

3.1.13 that nothing in this Contract will operate to transfer to the Client or to grant to the Client any licence or other right to use the MVSS Portal except to the extent necessary to enjoy the benefit of the Managed Vulnerability Scanning Services and in compliance with NCC Group's acceptable use policy in respect of the MVSS Portal in force from time to time. NCC Group may at its absolute discretion suspend the Client's access to the MVSS Portal if the Client uses the MVSS Portal in breach of the Contract or acceptable use policy;

3.1.14 that if NCC Group (or its Affiliates) requires any of the Client's Intellectual Property Rights to be used in connection with the MVSS Portal the Client shall grant to NCC Group a non-exclusive, royalty free, licence to use such Intellectual Property Rights solely for the purposes of providing the MVSS Portal;

3.1.15 to ensure that its access credentials for the MVSS Portal are stored securely and only used by those employees of the Client that are expressly authorized by the Client to access the MVSS Portal and are not shared with any other person. The Client shall take all reasonable steps to prevent any unauthorized access to the MVSS Portal and will immediately notify NCC Group if it becomes aware of any such access; and

3.1.16 that, by signing the Authorisation Form, the Client consents, for itself and on behalf of all Affiliates, to NCC Group (or its Affiliates) performing the Managed Vulnerability Scanning Services and confirms that it has procured, where necessary, the consent of all its (and its Affiliates') third party service providers (including ISPs), relevant third party software vendors and equipment owners, employees, agents and sub-contractors to NCC Group carrying out the Managed Vulnerability Scanning Services. Such consent includes authorisation for the purposes of Section 3 of the Computer Misuse Act 1990 that NCC Group, its Affiliates and their respective employees, agents and sub-contractors may perform Managed Vulnerability Scanning Services which may;

3.1.16.1 impair the operation of the System;

3.1.16.2 hinder access to the System; and

3.1.16.3 impair the operation of any program and/or the reliability of any data relating to the System.

3.1.17 The Client acknowledges that there is a risk that the Services may lead to the loss or corruption of the Client's data and/or Personal Data affected by such Services, and that the same is an inherent risk of Managed Vulnerability Scanning Services even when performed in accordance with Good Industry Practice. The Client is advised to back up its data prior to the Start Date as described in clause 3.1.4 above. Subject to clause 10.4.6 of the General Terms and Conditions, NCC Group will not be liable for any such loss of data.

4 NCC Group's Duties

4.1 Reports shall be uploaded to the MVSS Portal at the frequencies specified in the Statement of Works.

4.2 NCC Group will use reasonable endeavours to ensure the Managed Vulnerability Scanning Services are provided at the agreed frequency without any interruptions and that the information provided is accurate and up to date. However, from time to time the Client may experience disruptions or receive inaccurate information due to circumstances beyond NCC Group's control for which, subject to clause10.2 of NCC Group's General Terms and Conditions, NCC Group shall not be liable, for example a lack of availability of the backbone internet infrastructure in the UK or other locations. NCC Group may also need to perform maintenance of its own hardware and software, which may interrupt provision of the Services. NCC Group will endeavour to execute such maintenance with the minimum of disruption to the Services and will, where feasible, provide prior notice to the Client.

4.3 NCC Group will notify the Client of any bandwidth requirements it may have to enable it to perform the Managed Vulnerability Scanning Services.

4.4 Where NCC Group is performing the Cyber Essential Services or Cyber Essentials Plus Services, the Client accepts and acknowledges that NCC Group can only advise on its interpretation of such rules or standards derived from its experience and expertise in the industry. Specifically, the Client accepts and acknowledges that NCC Group cannot guarantee the Client's compliance with the relevant rules and standards, which is ultimately determined by the IASME Consortium Limited.

5 Fees and Payment

5.1 Any expenses in addition to the basic Fees shall be agreed in advance and shall be reimbursed by the Client.

6 Ownership of System

6.1 Ownership of the System and all Intellectual Property Rights in the System remains at all times with the Client and/or its ISP or other third party supplier (as applicable).

7 Cancellation and Rescheduling

7.1 The Client accepts and acknowledges that NCC Group allocates Consultants weeks or months in advance and would suffer a loss should the Services or any Service Portion be postponed or cancelled at short notice. As such, the Client agrees that it shall pay to NCC Group (as genuinely pre-estimated liquidated damages) the following amount to reflect the losses which NCC Group will incur if such cancellation or rescheduling (the "**Cancellation Fee**"):

7.2 cancellation or rescheduling request within 7 days of the Start Date: 100% of the Scheduled Days Cost.

7.3 Charging of the Cancellation Fee is at NCC Group's discretion. NCC Group will use reasonable commercial efforts to re-deploy Consultants to other projects to mitigate its losses resulting from cancellation or rescheduling. If NCC Group is able to successfully redeploy Consultants, then it shall reduce the Cancellation Fee payable by the Client accordingly.

7.4 If the Client re-books the Services for another date, the Fees for the Services as re-booked will be payable in addition to any Cancellation Fee.

7.5 The parties agree that any Fees paid or payable in relation to the Managed Vulnerability Scanning Services are non-refundable. Accordingly, if the Contract is terminated or the Managed Vulnerability Scanning Services are cancelled, NCC Group will be entitled to retain such Fees (and be paid for all amounts that are as at that date invoiced but unpaid) and no refunds or credits will be given.

8 Liability

8.1 Subject to clause 10.2 of the General Terms and Conditions, NCC Group excludes all liability:

8.1.1 for any use or misuse of information accessed due to another person being informed of or gaining access to the Client's user names and passwords, and

8.1.2 to the Client to the extent that the Cyber Essentials and Cyber Essentials Plus certifications are (i) withdrawn; or (ii) amended by IASME, NCSC (or any other party with authority over them or the Client's participation in them) such that NCC Group is no longer able to perform the Cyber Essentials Services and Cyber Essentials Plus Services.

