NCC GROUP TERMS AND CONDITIONS FOR THE SUPPLY OF SERVICES

Services Module (Managed Vulnerability Scanning Services)

1 Agreement Structure and Interpretation

1.1 This Services Module sets out the terms and conditions applicable to managed security services, and is to be read in conjunction with NCC's General Terms and Conditions.

1.2 NCC's General Terms and Conditions apply to this Service Module.

1.3 Capitalised terms in this Services Module shall have the same meaning ascribed to them in NCC's General Terms and Conditions unless stated otherwise herein. A reference to "Related Body Corporate" includes "Related Corporation" as defined in NCC's General Terms and Conditions (where applicable).

2 Definitions:

"**ISP**" means Internet Service Provider;

"**Managed Vulnerability Scanning Services**" means the managed vulnerability scanning services provided by NCC including PCI ASV Scanning 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 Work; and

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

"**Service Portion**" means a phase, subproject, or similar portion of the total Managed Vulnerability Scanning Services as described in the Statement of Work or otherwise agreed between the Parties; 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 Managed Vulnerability Scanning 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, 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, responding promptly to any queries or requests for information;

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

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 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 Module;

3.1.6 to notify NCC in writing in advance or as soon as possible after becoming aware of any periods during which NCC 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 to modify its testing approach if necessary, with the client's consent;

3.1.7 to use any software and/or hardware which NCC (and its Related Bodies Corporate) 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's (and its Related Bodies Corporate) instructions provided from time to time;

3.1.8 to assume all liability and to indemnify, keep indemnified and hold harmless NCC, its Related Bodies Corporate 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 (or its Related Bodies Corporate) as a result of the provision of the Managed Vulnerability Scanning Services, except to the extent that any such losses, damages, demands, costs, expenses, fees or liabilities are incurred as a direct result of NCC's breach of the Agreement;

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

3.1.10 that NCC 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 for the Client;

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

3.1.12 that nothing in this Agreement 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's acceptable use policy in respect of the MVSS Portal in force from time to time. NCC 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 Agreement or acceptable use policy;

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

3.1.14 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 if it becomes aware of any such access; and

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

3.1.15.1 impair the operation of the System;

3.1.15.2 hinder access to the System; and

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

3.2 The Client acknowledges that there is a risk that the Managed Vulnerability Scanning Services may lead to the loss or corruption of the Client's data and/or Personal Information affected by such Managed Vulnerability Scanning 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 Service Start Date as described in clause 3.1.4 above. Subject to clause 23.6 of NCC's General Terms and Conditions, NCC will not be liable for any such loss of data.

4 NCC's Duties

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

4.2 NCC will use reasonable efforts 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's control for which, subject to clause23.6 of NCC's General Terms and Conditions, NCC shall not be liable, for example a lack of availability of the backbone internet infrastructure in the UK or other locations. NCC may also need to perform maintenance of its own hardware and software, which may interrupt provision of the Managed Vulnerability Scanning Services. NCC will endeavour to execute such maintenance with the minimum of disruption to the Managed Vulnerability Scanning Services and will, where feasible, provide prior notice to the Client.

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

5 Fees and Payment

5.1 The Fees payable under this Agreement for Managed Vulnerability Scanning Services shall be invoiced on or after the Service Start Date. Any additional expenses 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 Managed Vulnerability Scanning Services or, if applicable, each Service Portion will commence on the date set out in the Statement of Work unless otherwise agreed in writing between NCC and the Client (the "**Scheduled Date**").

7.2 The Client accepts and acknowledges that NCC often allocates Personnel weeks or months in advance and would suffer a loss should the Managed Vulnerability Scanning Services or any Service Portion be postponed or cancelled at short notice. As such, the Client agrees that:

7.2.1 it shall pay to NCC a Cancellation Fee (as genuinely pre-estimated liquidated damages) in the amount calculated in accordance with clause 7.3 below; and

7.2.2 the Cancellation Fee reflects the losses which NCC will incur if such cancellation or rescheduling is requested within a set number of days of the Scheduled Date.

7.3 The Cancellation Fee shall be calculated as follows:

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

7.4 The Parties agree that any Fees paid or payable in relation to the Managed Vulnerability Scanning Services are non-refundable. Accordingly, if the Agreement is terminated or the Managed Vulnerability Scanning Services are cancelled, NCC 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.

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

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

8 Liability

8.1 Subject to clause 23.6 of NCC's General Terms and Conditions, NCC excludes all liability 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.