National Cyber Security Centre

CYBER-SECURITY INFORMATION SHARING PARTNERSHIP

Terms and Conditions

V5.0

Synopsis

This document contains the Cyber-Security Information Sharing Partnership (CiSP) terms and conditions that each member organisation must agree to and sign in order to participate within the CiSP Collaboration Environment.

The Terms and Conditions are the primary means by which information sharing, handling, confidentiality, liability and appropriate behaviour are established and managed by the CiSP community of organisations.

CYBER-SECURITY INFORMATION SHARING PARTNERSHIP

(CiSP) COLLABORATION ENVIRONMENT

TERMS & CONDITIONS

These terms and conditions govern the exchange of cyber threat and vulnerability information between the companies and other legal entities who become members ("Members") of a technical information sharing platform known as the CiSP Collaboration Environment. The parties to it are the Members for the time being of the CiSP Collaboration Environment and the National Cyber Security Centre.

By accessing the CiSP Collaboration Environment you are indicating that you are an Individual Participant as defined below and are acting on behalf of a "Member" of the CiSP Collaboration Environment who agrees to comply with these terms and conditions.

1 DEFINITIONS

In these terms and conditions, the following definitions apply:

1.1 "**Admin Access**" means the permissions allocated to NCSC staff members who are responsible for the administration of the CiSP Collaboration Environment. This access includes administrative rights that allow those staff members to make changes to content hosted on the CiSP Collaboration Environment in order to discharge their administrative responsibilities and to moderate that content.

1.2 **"CiSP"** means the Cyber-Security Information Sharing Partnership

1.3 "**CiSP Collaboration Environment**" means a uniquely hosted technical system that enables online relationships and connections between a set of Members (acting by Individual Participants) to allow them to share cyber threat and vulnerability information. The CiSP Collaboration Environment is based on the principle that, as far as possible, there should be openness and transparency between Members.

1.4 "**CiSP Collaboration Tool**" means customised and specially configured commercial social network software that provides the technical basis of the CiSP Collaboration Environment. It facilitates the sharing of cyber threat, vulnerability and other information between Members in a controlled and trusted manner.

1.5 "**Corporate Device**" means a Secure Device that is approved for use on the Member organisation's corporate network. The operation and use of the

Corporate Device should comply with a Member's corporate controls and procedures and with good practice.

1.6 "**CiSP Fusion Cell**" means a joint government and industry organisation of analysts, based in NCSC's Operations Unit, who examine cyber information and data feeds, conduct analysis and provide contextual cyber threat and vulnerability assessments to produce a coherent view in the CiSP Collaboration Environment for the benefit of Members.

1.7 "**Elevated Viewing Privileges**" means the permissions allocated to analysts within the NCSC and to industry members of the CiSP Fusion Cell. Elevated Viewing Privileges do not include any right to modify content.

1.8 "**Embed**" means an individual who is assigned to work for NCSC on a part time basis whilst being employed by, and continuing to receive salary from, an employer outside government.

1.9 "**Group**" means a voluntary organisation of two or more Members who have a specific interest in sharing Information with each other as a result of their industry organisation, industry sector, level of cyber maturity or any other shared interest.

1.10 "**Group Owner**" means a Member who applies to the CiSP Service Desk with a reasoned case supporting the creation of a Private Group or a Secret Group and who determines which other Members may join the Group and which content should be made available within the Group.

1.11 "**Individual Participant**" means an individual within a Member who has been provided with personal access to the CiSP Collaboration Environment and who operates on behalf of the Member.

1.12 "**Information**" means any information (of whatever nature and whatever form or format) that is exchanged and shared between Members in the CiSP Collaboration Environment and includes information which is received in writing, electronically or orally from or pursuant to discussions between Members.

1.13 **"Information Handling Levels**" means the application of privacy control measures on Information which details how the Information shall be handled within the CiSP Collaboration Environment. The four levels take the form of a traffic light protocol (or TLP) and are described in clause 5.

1.14 "**Managed Security Service Provider**" means an organisation that provides a Member with support to its network security management which may include virus blocking, spam blocking, intrusion detection, firewalls, log & packet inspection and virtual private network (VPN) management. The Managed Security Service Provider may also manage and implement system changes, modifications, and

upgrades.

1.15 "**Member**" means a company or other legal entity that which meets the criteria for membership contained in clause 2.

1.16 "**NCSC**" means the Secretary of State for Foreign and Commonwealth Affairs acting through the National Cyber Security Centre, a part of the Government Communications Headquarters.

1.17 "**Originator**" means the Member that first discloses any particular Information using the CiSP Collaboration Environment.

1.18 "**Personal Data**" has the meaning given in the Data Protection Act 1998.

1.19 "**Private Group**" means a group whose existence can be discovered by a search on the CiSP platform and to which any Member may apply to join.

1.20 "**Purpose**" means the improvement of the collective cyber security capabilities of the Members (or any subset of them that forms a Group) through the exchange of actionable information on cyber threats and vulnerabilities.

1.21 "**Recipient**" means a Member that receives Information pursuant to these terms and conditions from an Originator. A Member is still a Recipient for the purposes of these terms and conditions even when the Information is received by an Individual Participant who acts on behalf of that Member under a marking contained in clause 5 that prevents disclosure more widely within the Member organisation.

1.22 "**Secret Group**" means a group whose existence cannot be discovered by a search on the CiSP platform, and to which membership is only by invitation of the Group Owner.

1.23 "**Secure Device**" means a device with the following characteristics as a minimum where applicable:

1.23.1 an operating system and all applications with up-to-date software patches from their respective manufacturers;

1.23.2 an up-to-date browser;

1.23.3 an installed fully operational anti-virus product with up-to-date configuration data;

1.23.4 an installed fully operational anti-spyware product with up-to-date configuration data; and

1.23.5 an installed operational firewall.

1.24 "**Service Desk**" means the part of NCSC which provides management and administration of the CiSP Collaboration Environment in order that it can successfully meet the Purpose. The Service Desk provides a helpdesk facility and is the point of escalation for all Member issues associated with the effective operation of the CiSP Collaboration Environment. The Service Desk administers the terms and conditions for the CiSP Collaboration Environment.

2 MEMBERSHIP

2.1 Any UK registered company or other legal entity which is responsible for the administration of an electronic communications network in the UK, a UK Crown Dependency, or a UK Overseas Territory and which has a sponsor is eligible to become a Member provided that it is able to confirm that it complies and is willing to continue to comply with clause 2.2.

2.2 Members must have appropriate measures in place to protect the confidentiality of any Information received via the CiSP Collaboration Environment.

2.3 Membership of the CiSP Collaboration Environment is exclusive to the legal entity to whom it is granted and does not extend to any related or associated company. Companies that are a holding company or a subsidiary of a Member are required to apply for membership in their own right in order to participate in the CiSP Collaboration Environment.

2.4 **Groups**: Members are able to request the creation of two kinds of groups on CiSP: Private Groups and Secret Groups. The criteria for establishing Groups is as follows:

2.4.1 **Private Groups**: Any Member or Members who wish to form a Private Group must apply to the Service Desk with a reasoned case supporting their existence;

2.4.2 **Secret Groups**: Any Member or Members who wish to create a Secret Group must apply to the Service Desk with a reasoned case supporting their existence and must also demonstrate that there are exceptional circumstances whereby users wish to share sensitive information and have such a high degree of concern about the information that they need to prevent Embeds within the CiSP Fusion Cell from having access to the information other than by invitation. Secret Groups will be subject to regular audit by the Service Desk to ensure that their secret status remains appropriate.

2.5 Members understand and agree that Group Owners hold the right to admit, invite, and remove content from Members of their Groups, in order to ensure appropriate

activity in accordance with the Purpose of the CiSP Collaboration Environment. In addition, all activity on the CiSP Collaboration Environment is monitored by Service Desk staff in order to moderate content, membership, and privacy levels where required.

2.6 Membership of the CiSP Collaboration Environment is dependent on user interaction and contribution, and a condition of continued membership is that the Member is using their account regularly. Inactive accounts will be subject to the following procedure for deactivation

2.6.1 After one month of inactivity (defined as the Member not logging in to CiSP), the Member will be sent a notification email, prompting a return to CiSP;

2.6.2 If the inactivity continues for a further month after the first notification email, the Member will be sent the notification email again;

2.6.3. If the inactivity continues for a further month after the second notification email, the Member will be sent the notification email for a third time;

2.6.4 After a failure to log in for a period of one week after the third email, the Member's account will be suspended. If the account is not reactivated by the Member during the following month, the account will be automatically deactivated;

2.6.5 The Member will then be notified directly by email when their account has been deactivated.

3 MEMBER RESPONSIBILITIES

3.1 A Individual Participant put forward by a Member must:

3.1.1.1 have a role within the Member's organisation which is such that their participation in the CiSP Collaboration Environment promotes the Purpose.

3.1.1.2 have successfully passed the security background check as defined in the CiSP Collaboration Tool Operating Procedures and the security check has been verified by the sponsor and passed to the Service Desk before any account is activated for the Individual Participant;

3.1.1.3 consent to the processing of their Personal Data in accordance with clause 13;

3.1.1.4 have agreed to comply with these terms and conditions.

3.2 A Member must inform the Service Desk as soon as possible if it wishes to replace

one of its Individual Participants or if any Individual Participant ceases to be employed by it or if there are any changes to their personal details.

3.3 A Member may not supply information through the CiSP Collaboration Environment except in so far as the Member considers that supplying the information is necessary to further the Purpose. Members shall only use and disclose Information supplied by other Members for the Purpose and in a manner consistent with the Information Handling Level that applies to it.

3.4 Members shall ensure that their supply and receipt of Information through the CiSP Collaboration Environment, and also their use and disclosure of Information, comply with any applicable legal obligation including those contained in these terms and conditions. Members shall not supply confidential information about their own or other Members' prices, discounts or other terms offered to customers or future changes to or plans for prices, discounts and other terms and conditions; recent or forecast sales figures; territories or markets; proposed responses to invitations to tender; or commercial or marketing strategy.

3.5 To minimise the commercial sensitivity of Information within the CiSP Collaboration Environment, Members shall ensure that the Information that is shared relates to cyber incidents, on technical indicators and mitigations and does not extend to impacts or damage assessments.

3.6 Members shall not solicit, advertise, endorse or oppose a product or service in the CiSP Collaboration Environment for any commercial gain for themselves, another Member, or any third party.

3.7 Members shall not use the platform as a recruitment or business lead generation tool that may yield any commercial gain for themselves, another Member or any third party.

3.8 Members shall endeavour to ensure that any Information shared within the CiSP Collaboration Environment is accurate. However, all Members understand and accept that Information shared is provided “as-is” and the Originator excludes all representations, warranties, obligations and liabilities in relation to the Information to the maximum extent permitted by law. The Originator shall not be liable for any errors or omissions in the Information and shall not be liable for any loss, injury or damage of any kind arising from or in connection with its use.

3.9 Members will ensure that any Individual Participant who represents them is fully familiar with, and understands and complies with the requirements of the CiSP Terms and Conditions.

3.10 In the event of a Member’s organisation splitting up into two or more organisations, it is the responsibility of the Member to inform the Service Desk, so that details can be reviewed and amended accordingly and the new organisations can become

Members if appropriate.

4 PRIVACY CONTROLS

4.1 Members are able to set privacy controls and Information Handling Levels on the sharing of Information within and outside the CiSP Collaboration Environment in accordance with clause 5.

4.2 A Member may not disclose another Member's Information except in accordance with the applicable Information Handling Level or with the prior written consent of the Originator.

4.3 Members understand and accept that the NCSC staff with Admin Access are able to access all posts on the CiSP Collaboration Environment, regardless of privacy controls and Information Handling Levels.

5 INFORMATION HANDLING.

5.1 Members posting Information on the CiSP Collaboration Environment must use the Traffic Light Protocol (TLP) set out below. Any government information must be rebranded and reclassified using the TLP by the Originator.

5.2 The Originator must assign one of four Information Handling Levels to every piece of Information shared within the CiSP Collaboration Environment. The four levels are as follows:

5.2.1 **RED.** Disclosure of Information that is marked as RED is restricted to the Individual Participants that have been explicitly identified and named by the Originator and the CiSP Fusion Cell. Information shared in this manner must not be disclosed to other Individual Participants. The Originator will not be identified for Information disclosed at Red.

Information released at RED shall be marked as "*Red – May be shared with named participant(s) only"*

5.2.2 **AMBER**. Disclosure of Information that is marked as AMBER is restricted, in the first instance, to Individual Participants, identified and named by the Originator and to the CiSP Fusion Cell analysts with Admin Access. Disclosure may subsequently be made to: other Individual Participants who represent the same Recipient as the identified Individual Participant; other individuals within the same Recipient organisation (including the same organisation overseas); the Individual Participants of other Members who are Members of the same Group as the Recipient; and to other individuals within those Members. Disclosure of Information beyond the identified and named Individual Participants shall be on a "need-to-know" basis and only disseminated

as is necessary to act on that Information in accordance with the Purpose. The default setting for Information disclosed at this level is non-attribution (i.e. the Originator identity is anonymous) although the Originator has the option to give their permission to be named as the source of the disclosure which must always be in writing stating their name, their organisation and the fact they are prepared to be identified as the Originator.

Information released at AMBER shall be marked as "*Amber – May be shared with identified groups/participants within their organisation. The source of the information is always RED"*

5.2.3 **GREEN.** Member Information marked as GREEN can be disclosed by Recipients to any Member and Non-Members within a Member organisation. The default setting for Information disclosed at this level is non-attribution (i.e. the Originator identity is anonymous) although the Originator has the option to disclose its identity if desired.

Information released at GREEN shall be marked as "*GREEN – May be shared with any participant in the CiSP Collaboration Environment."*

5.2.4 **WHITE**. Subject to the laws of copyright and any other restrictions on disclosure which arise as a matter of law, Information marked as WHITE may be published and distributed freely without restriction within and outside the CiSP Collaboration Environment. The default setting for Information disclosed at this level is non-attribution (i.e. the Originator identity is anonymous) although the Originator has the option to disclose their identity if desired.

Information released at WHITE shall be marked as "*WHITE) – May be shared with anyone (no restrictions / public information).""*

5.2.5 Information marked as AMBER or GREEN may, additionally, be disclosed by a Member to its Managed Security Service Provider(s), providing, and only to the extent that:

5.2.5.1 it is necessary for the Member to make such disclosure in order to improve its cyber-security capability (consistent with the Purpose); and

5.2.5.2 disclosure to that Managed Security Service Provider has not been prohibited by the Originator.

6 ADMIN ACCESS AND ELEVATED VIEWING RIGHTS

6.1 Members understand and agree that NCSC will permit some selected NCSC staff to have Admin Access to the CiSP Collaboration Environment. Staff with Admin Access shall be required to use it strictly for the purposes of administering these terms and conditions and moderating content. Staff given Admin Access will be limited to the minimum number necessary to enable effective administration and subject to regular audit.

6.2 Members understand and agree that, except as set out in clause 6.3, NCSC analysts and Embeds who are part of the CiSP Fusion Cell will have Elevated Viewing Privileges which provide them the same viewing rights over content as a Member of any Group and the ability to see the author of anonymous posts. Individuals with Elevated Viewing Rights shall be required to use them strictly for the purpose of developing increased situational awareness and analytics across all data feeds in support of the Purpose and to ensure that NCSC's role as moderator can be properly executed. Individuals working within the CiSP Fusion Cell shall be subject to additional non-disclosure restrictions in recognition of their enhanced data access and the increased sensitivity of Information.

6.3 Only NCSC staff and CiSP Service Desk staff have Elevated Viewing Rights that extend to Secret Groups. Industry and law enforcement Embeds will not have any viewing or other access to Secret Groups unless specifically invited to join the Group by the Group Owner.

7 MALWARE SAMPLES

7.1 The CiSP Collaboration Environment is only for the dissemination of threat Intelligence not for the upload of malware samples. Controls are in place to stop the upload of samples and will be removed by Service Desk moderators. Malware samples should be sent to incidents@ncsc.gov.uk where the incident handling team will analyse the sample and post its findings via the CiSP Collaboration Environment.

8 IDENTITY PROFILE

8.1 Each Individual Participant shall have an identity profile in the CiSP Collaboration Environment, as follows;

8.2 A **public profile** viewable by all Individual Participants in the CiSP Collaboration Environment. The public profile shall consist of the following details:

8.2.1 Name of Member represented by the Individual Participant, in the format 'name@organisation'.

8.2.2 High level summary of activity (to include number of incident reports submitted and number of contributions); and

8.2.3 Number of connections with other Individual Participants

8.3 A **private profile** viewable only by another Individual Participant(s) where permission has been granted for them to do so. The private profile shall consist of the following details:

8.3.1 Public Profile information;

8.3.2 Name;

8.3.3 Job title and role within Organisation;

8.3.4 Telephone Number;

8.3.5 Corporate E-mail Address;

8.3.6 Recommendations;

8.3.7 Likes and dislikes; and

8.3.8 Activity details.

8.4 Members and Individual Participants shall be responsible for ensuring that profiles are up to date and accurate at all times. Individual Participants are able to control the visibility of their private profile information and make elements of their profile available for viewing by all Individual Participants as part of their public profile.

9 FEEDBACK

9.1 Members shall be able to provide qualitative feedback on Information received from other Members. The feedback shall be able to be provided against the relevance and usefulness of shared Member Information. Any feedback made or provided by Members or Individual Participants shall be subject to the same limitations and exclusions of liability as are set out in clause 14.

10 CONFIDENTIALITY AND FREEDOM OF INFORMATION

10.1 In consideration of the Information being made available by an Originator, each Member hereby irrevocably undertakes with the Originator and with the other

Members, both for itself and on behalf of its personnel, that the Member and its personnel shall:

10.1.1 only use the Information for the Purpose;

10.1.2 not store in any medium, copy, reproduce or reduce to writing any material part of the Information except as may be reasonably necessary for the Purpose;

10.1.3 use the same care and discretion as it uses with its own proprietary information, but no less than reasonable care, to avoid disclosure, publication, or dissemination otherwise than in accordance with the terms of these terms and conditions; and

10.1.4 ensure that its Individual Participant(s), and any other of its personnel who are permitted to see the Information, are aware of the Information Handling Level that the Originator has attached to it (in accordance with clause 5.1) and that they comply with any confidentiality and non-disclosure obligations which apply.

10.2 The disclosure of Information by any Originator shall in no way be construed to imply any kind of transfer of rights or grant of licence connected with the Information including, without limitation, any intellectual property rights, patents, copyrights trademarks or trade secrets.

10.3 Where a Member stores, copies or reproduces Information in accordance with clause 10.1.2, the Member shall ensure that the copy or reproduction is marked in the same way as the original, in accordance with clause 5.

10.4 The Members acknowledge that NCSC as part of GCHQ is exempt from the disclosure requirements of the Freedom of Information Act 2000 ("FOIA") and as such is under no obligation to comply with the information disclosure requirements therein for as long as such exemption remains in force. In the event that a Member receives a disclosure request from a third party pursuant to FOIA that relates to GCHQ or NCSC or relates to GCHQ or NCSC information disclosed on CiSP, then the Member shall notify NCSC and shall not make any such disclosure whatsoever and under any circumstances unless it receives NCSC's express written consent or otherwise in accordance with NCSC's instructions.

11 NON-DISCLOSURE TO THIRD PARTIES

11.1 Save as otherwise expressly permitted in these terms and conditions, no Member shall at any time without the relevant Originator's prior written consent, disclose Information otherwise than:

11.1.1 in accordance with the applicable Information Handling Level required by clause 5.1; or

11.1.2 if required to do so by law or by the order or ruling of a court or tribunal

or regulatory body or recognised stock exchange of competent jurisdiction.

11.2 Where disclosure is contemplated in accordance with clause 11.1.2, the Member required to make disclosure shall, unless prohibited from doing so, notify the Originator promptly in writing of that fact and, wherever legally possible, prior to making such disclosure. In any event the relevant Member shall only disclose such Information to the extent necessary under the court order or other ruling.

12 UNINTENDED DISCLOSURE

Each Member agrees that, in the event that Information is disclosed or used by them without authorisation, the Member shall immediately notify the relevant Originator of the unauthorised use or disclosure and take steps (including, in particular, any steps which the Originator reasonably requires the Member to take) to prevent further dissemination of the disclosed Information and to prevent further unauthorised use or disclosure. The obligation to notify the Originator of any unauthorised disclosure and to mitigate any damage caused by the unauthorised use or disclosure remains in effect regardless of the termination of any other rights and obligations arising under these terms and conditions.

13 DATA PROTECTION

13.1 The CiSP Collaboration Environment uses cookies for collecting Individual Participant information in order to support session maintenance and user experience. Internet Protocol addresses are automatically recognised and logged by the web server.

13.2 Members agree that the NCSC may store and use any Personal Data provided under clause 8 for the purpose of providing access to and administering the CiSP Collaboration Environment including creating a user profile for the Individual Participant who has supplied it. Any Personal Data received by NCSC will be stored in a database called the CRM and used as set out in this clause.

13.3 NCSC will comply with requests from Members to access, update, correct or delete any Personal Data it holds. In the event that a Member terminates its membership or an Individual Participant ceases to act on behalf of the Member, it will notify the NCSC and the NCSC will delete all and any Personal Data from the CRM.

13.4 Personal Data may not be used by the NCSC or any Member other than in accordance with these terms and conditions. In particular, nothing in these terms and conditions permits any Member to remove Personal Data relating to another Member from the CiSP Collaboration Environment or to use that Personal Data other than for the Purpose.

14 DISCLAIMERS

14.1 References (in Information shared within, or in other communications conducted through, the CiSP Collaboration Environment) to any specific commercial product, process or service by trade name, trade mark, manufacturer, or otherwise, does not imply its endorsement or recommendation. The views and opinions of Individual Participants or the NCSC expressed within the CiSP Collaboration Environment shall not be used for advertising or product endorsement purposes.

14.2 To the fullest extent permitted by law, the NCSC and each and every Member accept no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill and damage to reputation) incurred by any person and howsoever caused arising from or connected with the operation of the CiSP Collaboration Environment in accordance with these terms and conditions, and including loss and damage caused by any error or omission in Information provided through, or information provided in connection with, the CiSP Collaboration Environment or from any person acting, omitting to act or refraining from acting upon, or otherwise using the Information provided through the Collaboration Environment. Members shall make their own judgement as regards use of any Information obtained from the CiSP Collaboration Environment.

14.3 The Service Desk reserves the right to modify, suspend or terminate operation of or access to the CiSP Collaboration Environment, to modify or change the CiSP Collaboration Environment, and to interrupt the operation of the CiSP Collaboration Environment as necessary to perform routine or non-routine maintenance, error correction, or other changes.

15 PUBLICITY

15.1 Membership of the CiSP Collaboration Environment is considered as TLP 'WHITE' as set out in clause 5.2.4 and Members can therefore freely disclose that they are part of the environment.

16.2 Each Member agrees that it shall not use any other Member's or the NCSC's name or logo without consent, or advertise or otherwise publicise the identity of any other Member of the CiSP Collaboration Environment without prior written consent.

16 NOTICES

16.1 Any notice or other communication to be given under these terms and conditions must be in writing and sent to NCSC at cisp@ncsc.gov.

16.2 Any notice shall be deemed served at the time the e-mail is transmitted unless an

error transmission message is received.

16.3 None of the Members shall assign, sub-license or otherwise transfer their rights or obligations under these terms and conditions without the prior written consent of each of the other Members and the NCSC.

16.4 No failure or delay by a Member in exercising any of its rights under these terms and conditions shall operate as a waiver of such rights, nor shall any single or partial exercise preclude any further exercise of such rights. Any waiver must be in writing and signed by the waiving parties to be effective.

16.5 If any clause in these terms and conditions is determined to be invalid in whole or part (for any reason whatsoever) the remaining provisions or parts thereof shall continue to be binding and fully operative.

16.6 These terms and conditions, and the NCSC Industry 100 Non-Disclosure Agreement shall constitute the entire agreement between the Members concerning the Purpose and supersedes all previous arrangements, commitments, understandings and agreements between the Members concerning the subject matter hereof. Nothing in these terms and conditions shall act to exclude or limit any Member's liability to any other Member with respect to any fraudulent misrepresentations.

17 RIGHTS OF THIRD PARTIES

A person who is not a party to these terms and conditions shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any provision of these terms.

18 RELATIONSHIP OF THE MEMBERS

Nothing in these terms and conditions shall constitute or be deemed to constitute any form of employment, partnership, joint venture, agency or other business entity between the Members; nor shall any employees, legal partners or agents of one Member be deemed to be the servants, legal partners or agents of any other Member.

19 COMMENCEMENT, VARIATION AND TERMINATION

19.1 A Member accepts these terms and conditions when they are accepted by an Individual Participant acting on behalf of the Member. If the Member puts forward more than one Individual Participant, they will each be asked to confirm acceptance on behalf of the Member. The terms shall continue to apply until such time as the Member terminates its membership by giving no less than five (5) days notice to the Service Desk or if all the Member's Individual Participants have their

accounts deactivated under clause 2.6. The Service Desk shall promptly inform all remaining Members if any membership is terminated.

19.2 The NCSC may vary the Terms and Conditions from time to time by providing written notice to all Members and a link to the amended terms. The new amendments will take effect five (5) days after they have been notified to Members.

19.3 Notwithstanding a termination of Membership in accordance with clause 19.1, the rights and obligations with respect to the disclosure and use of the Information shall remain in effect for a period of five (5) years from the date of termination or, in relation to particular Information, for such a longer period (not to exceed 20 years) as may be specified in writing, on a case-by-case basis, by each relevant Originator.

20 GOVERNING LAW

These terms and conditions are governed by the laws of England and Wales and subject to the exclusive jurisdiction of the English courts.