CPNI
Centre for the Protection of National Infrastructure

CPNI EXTRANET TERMS AND CONDITIONS

1. General Terms of Use

1.1 The Centre for the Protection of National Infrastructure ("**CPNI**") is the UK national technical authority that provides integrated protective security advice to organisations. CPNI owns and manages a restricted-access extranet that provides CPNI guidance and materials (the "**Extranet**"). This page sets out the terms of use which you agree to when you using the Extranet and gives guidance on handling extranet material (the "**Terms and Conditions**"). By using the Extranet, you indicate that you accept these Terms and Conditions and that you agree to abide by them.

1.2 The Extranet contains material with handling caveats and/or Government Security Classifications up to OFFICIAL-SENSITIVE. It is the primary means by which CPNI shares published guidance with you.

1.3 Access to certain areas of the Extranet is provided on the basis of individual permissions for only. You will only be able to access designated areas if you have the appropriate permissions.

1.4 Material is published on the Extranet in order to limit its circulation to those who 'need to know'.

1.5 If you are not a UK citizen you must indicate this on the application form and complete the additional information requested. Without this, your application will not be accepted.

1.6 If it comes to the attention of CPNI that you have entered any incorrect information onto the application form, or that you have failed to

comply with these terms and conditions, your access will be terminated.

2. Access to the Extranet

What you need to know

2.1 Access to the Extranet is provided on a goodwill basis and is determined on a named, individual basis by CPNI. CPNI has the right in its sole discretion to determine and approve who will have access to the Extranet and reserves the right to terminate access at any time at its absolute discretion including, for example, non-use over a prolonged period of time despite email reminders. Termination of access may be without notice or explanation if necessary. There is no right of appeal against such a decision and CPNI will not be liable for any losses (direct, indirect or consequential) that may be suffered by any person as a result. CPNI does not publish a list externally of those organisations or individuals who have access.

2.2 Access criteria are based around role, organisation and national security interests. If you leave your organisation or change roles within it, you must tell CPNI immediately.

2.3 Extranet users will have their details checked against our organizational records.

2.4 Your access criteria to the Extranet will be reassessed on an annual basis.

2.5 To access the site you need a unique username, password, followed by a One Time Password (OTP). Full guidance on access will be given to users.

2.6 You must never share your username or password, either within your organisation or outside.

2.7 You can access the Extranet via any modern internet browser, and from any secured (current anti-virus and spyware, personal firewall and patched) corporate device (e.g. desktop, laptop or appropriately accredited tablet or smartphone). You do not need a dedicated laptop or other device. We recommend against access via a personal desktop, personal mobile device or personal laptop unless accredited for use by your organisation, or access via another private network (e.g. internet café).

2.8 If you intend to access the Extranet outside the UK you must indicate this on the application form where requested, indicating the country/countries you will be visiting and/or accessing from.

2.9 You may not attempt to gain unauthorised access to any portion or feature of the Extranet to which you have not been given access.

2.10 You may not probe, scan or test the vulnerability of the Extranet, or breach, or attempt to breach the security or authentication measures on the Extranet.

2.11 You may not use the Extranet or its content for any purpose that is unlawful or prohibited by this agreement.

2.12 If you need to write down your password then this record must be kept separate from your username and OTP. The password should be secured as best you can, preferably in a locked cupboard or drawer. If you are on the move it may be written in a way that disguises or obscures its purpose.

2.13 Once you are logged onto the Extranet, if you intend to leave your PC or device unattended you must log out of your account.

Inactivity

2.14 An account is deemed 'inactive' if it has not been logged in to for a period of 90 consecutive days. If this occurs, you will be notified via email that you need to log on within a further 90 days. If you fail to do so, having not logged in for 180 consecutive days, your access will be terminated with no further communication.

2.15 If you are unable to use your account within the timeframes specified in 2.14, CPNI must be informed by emailing information@cpni.gov.uk in order to avoid access termination.

3. Classification of Materials

3.1 The Extranet aggregates a substantial amount of sensitive information, which may be of interest to terrorists or hostile foreign states. Its unauthorised disclosure could have implications for UK national security. You must handle it in accordance with guidance set out in this section.

3.2 Some Extranet pages and documents will be marked either with a Government Security Classification (e.g. OFFICIAL-SENSITIVE) or with a marking from the Traffic Light Protocol (e.g. AMBER, GREEN) which dictates how information may be shared within an organisation. There is no equivalence between a Government Security Classification which is based on an assessment of the impact of loss of data and the Traffic Light Protocol which is specific about how widely data may be shared.

3.3 CPNI accepts no liability for issues which arise from the incorrect marking of documents.

Government Security Classifications

3.4 The Government Security Classifications describe how the UK Government classifies information assets to ensure they are appropriately protected. It applies to all information that government collects, stores, processes, generates or shares to deliver services and conduct business. Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats.

3.5 You are likely to come across pages and documents on this Extranet which are marked OFFICIAL-SENSITIVE. This means that the information on that page or document should be held securely and not widely shared. It may be passed to management and security advisers on a 'need to know' basis. If you print an OFFICIAL-SENSITIVE page or document off the Extranet it should be destroyed securely when it is no longer required. See also the sections on Printing and Downloading.

3.6 Full details of the Government Security Classifications and their definitions can be found on the Extranet and on gov.uk at https://www.gov.uk/government/publications/government-security-classifications

Traffic Light Protocol (TLP)

3.7 The TLP is the information sharing tool used within Information Exchanges. It is used to allocate a sensitivity category to information.

There are four information sharing levels: RED, AMBER, GREEN and WHITE.

3.8 On this Extranet you are likely to come across pages which are marked up to AMBER. You are expected to respect the levels applied to information within the site:

- RED – Non-disclosable information, restricted to representatives present at IE meetings only. Representatives must not disseminate the information outside of the IE. RED information may be discussed during a meeting, where all representatives present have signed up to these rules. Guests and others such as visiting speakers who are not full members will be required to leave before such information is discussed.

- AMBER – Limited disclosure and restricted to members of the IE, and those within their organisation (whether direct employees, consultants, contractors or outsourced staff working in the organisation) who have a need to know in order to take action.

- GREEN – Information can be shared with other organisations, IEs or individuals in the network security, information assurance or CNI community at large, but not published or posted on the internet.

- WHITE – Information that is for public, unrestricted dissemination, publication, web posting, or broadcast. Any member may publish the information, subject to copyright.

Handling Extranet material

3.9 You must ensure you handle any materials on the Extranet in accordance with those instructions and prevent inadvertent disclosure of sensitive material or material carrying a Government Security

Classification by avoiding being overlooked when working with material you have downloaded from this Extranet, and by taking care when printing.

3.10 If you suspect a security breach of either the Extranet or Extranet material has occurred, you must phone your usual CPNI sponsor as soon as practical or email information@cpni.gov.uk, marking your email IMPORTANT – Possible security breach.

Printing

3.11 Documents and information may be printed out using local or networked printers, but care must be taken to ensure documents are collected immediately.

3.12 In the case of OFFICIAL-SENSITIVE documents, once you have printed them you must then turn off and restart the printer to clear the print buffer. Networked printers which cannot be turned off and restarted must not be used to print Extranet material.

3.13 Although you can access the Extranet from your corporate device when travelling abroad (see Section 2.8) you must not print out material from the Extranet when you are outside the UK. You must also avoid printing in non-secure locations in the UK e.g. on potentially non-secure printers such as in internet cafes/hotels or in an office where someone else could easily pick up your printing.

3.14 Hard copies of OFFICIAL-SENSITIVE material must be stored in locked drawers or cupboards and should be destroyed securely in accordance with BS-EN-15713: Secure destruction of confidential material.

Sharing Extranet material

3.15 Hard copies can be shared with those in your organisation you assess may be trusted to protect the information to the required standard and on a 'need to know' basis. It is your responsibility to keep a record of those to whom you have passed copies and for you to ensure they understand the level of protection required.

3.16 Any handling instructions or Government Security Classifications must not be removed.

3.17 Information on the Extranet may include information relating to security and intelligence for the purposes of section one of the Official Secrets Act 1989, and is protected against further disclosure without lawful authority. Users of the material are required to hold such material in confidence. Users are notified that disclosure of information on this Extranet without lawful authority will cause damage to national security. Should users have any doubts as to the effects of the Official Secrets Act 1989 and their obligations under it, they should seek independent legal advice.

3.18 OFFICIAL-SENSITIVE documents must not be emailed over the internet.

Downloading

3.19 OFFICIAL-SENSITIVE documents may not be mailed over or stored on networks which are not accredited to handle OFFICIAL-SENSITIVE data. In addition you should carefully consider the risks associated with storing or mailing any other sensitive data held on the Extranet which may not itself carry a Government Security Classification.

3.20 After using the Extranet you must ensure that you delete the 'Temporary Internet Files' cache on your system. Often this can be set

to occur automatically using 'Internet Options' on the Tools menu in your internet browser, or independently using dedicated deletion software. If possible, please ask your system administrator to delete the 'index.dat' file associated with your internet browser. For more details refer to your browser documentation.

3.21 You must ensure that information downloaded from the Extranet is securely stored or appropriately destroyed.

3.22 Information and documentation you download from the Extranet and hold on your own local systems may be subject to a Subject Access Request under the Data Protection Act and/or the Freedom of Information Act. If you receive a request of this type, please contact CPNI for advice on disclosure.

3.23 The Extranet is a security accredited site. CPNI have made every effort to ensure that information CPNI uploads to the site is screened for malicious content. Downloading information from the Extranet is at your own risk and CPNI accepts no responsibility for any loss or damage caused to your data or computer system which may occur as a result of downloading or using materials derived from this site.

3.24 Please note that when you use forms such as Contact Us (on the public website) to communicate with us you must never include information at OFFICIAL-SENSITIVE. The forms are sent to CPNI via ordinary internet email.

4. Disclaimer

4.1 Materials on the Extranet are provided on an information basis only, and whilst CPNI has used all reasonable care in producing it using the

data sources available to it, CPNI cannot provide any guarantees, conditions or warranties as to the accuracy of the information on the Extranet. CPNI does not warrant that the functions contained in the material on the Extranet will be uninterrupted or error free, that defects will be corrected, or that the Extranet or the server that makes it available are free of viruses or represent the full functionality, accuracy and reliability of the material.

4.2 Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this extranet shall not be used for advertising or product endorsement purposes.

4.3 To the fullest extent permitted by law, CPNI accepts 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) incurred by any person and howsoever caused arising from or connected with any error or omission in information, including all documents, and their references, in this Extranet or from any person acting, omitting to act or refraining from acting upon, otherwise using the information contained in this Extranet, including any documents or their references. You should make your own judgement as regards use of information on this Extranet and seek independent professional advice on your particular circumstances and security requirements.

4.4 This disclaimer applies to any damages, liability or injuries caused by any failure of performance, error, omission, interruption, deletion, defect, delay in operation or transmission, computer virus, communication line failure, theft or destruction of or unauthorised access to, alteration of, or use of the Extranet.

4.5 Whilst CPNI shall make reasonable efforts to ensure that information on the Extranet is up to date, it has no obligation to do so and CPNI makes no legal commitment to update the information.

4.6 CPNI reserves the right to modify, suspend or terminate operation of or access to the Extranet, to modify or change the Extranet, and to interrupt the operation of the Extranet as necessary to perform routine or non-routine maintenance, error correction, or other changes.

Virus Protection

4.7 Whilst CPNI takes reasonable efforts to check and test material in production, you must take your own precautions to ensure that the processes which you employ for accessing the Extranet do not expose you to the risk of viruses, malicious computer code or other forms of interference which may damage your own computer system. CPNI recommends the use of anti-virus program on all material downloaded from the Internet. We cannot accept any responsibility for any loss, disruption or damage to your data or your computer system which may occur whilst using material derived from this website.

5. Intellectual Property

5.1 Unless otherwise indicated, all CPNI materials on the Extranet are owned, controlled or licensed by or to CPNI, and are protected by Crown Copyright and may be subject to trademark and other protection. Nothing in these Terms and Conditions affects the ownership of any intellectual property rights in material that you or CPNI already own at the date you accept these terms.

5.2 Unless otherwise set out in these Terms and Conditions, no content may be copied, reproduced, republished, uploaded, posted, publicly

displayed, encoded, translated, transmitted or distributed in any way (including 'mirroring') to any other computer, server, website or other medium for publication or distribution or for any commercial enterprise, without CPNI's express prior written consent.

Logos

5.3 You are not permitted to use logos displayed on this Extranet without the prior written permission of CPNI.

6. Privacy

6.1 By using the Extranet you acknowledge and agree that internet traffic is never completely private or secure.

6.2 CPNI will use your personal data to provide access to the Extranet, access to any other services that you have requested (and which CPNI have accepted) and for CPNI's statutory functions.

6.3 CPNI will not collect any information about you except that required for assessing access criteria, system administration of our web server and to inform our analytics. User IP addresses are automatically recognised and logged by the web server.

7. Links to other websites

7.1 Where the Extranet contains links to other websites then these links are provided for your information only. Unless explicitly stated, linking should not be taken as endorsement of any kind. We have no control over the contents of those sites or resources, and accept no responsibility for them or for any loss or damage that may arise from

your use of them. Where third parties reproduce our information on websites or applications, those applications or websites may use versions of our information that has been edited or cached. The most up-to-date version of our information will always be that available on this website. We don't provide any guarantees, conditions or warranties as to the accuracy of any such third party products and do not accept liability for loss or damage incurred by users of such third party products under any circumstances.

8. Freedom of Information

8.1 CPNI is exempt from the disclosure provisions of the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Where the Freedom of Information Act 2000 is applicable to you, if you receive an information request relating to CPNI or to information supplied by us, please do not respond to it and inform CPNI as soon as possible.

9. General

9.1 Any notice or communication to be given to CPNI under these Terms and Conditions must be in writing and sent toinformation@cpni.gov.uk.

9.2 CPNI may, in its absolute discretion, vary these Terms and Conditions and should it do so you will only be able to continue accessing the Extranet if you agree to the amended Terms and Conditions. You should check these Terms and Conditions frequently to see whether it has been updated. By continuing to access the Extranet, you agree to be bound by the revised terms.

9.3 Should you not agree to any revision made to these Terms and Conditions in accordance with clause 9.2 above you must stop using the Extranet immediately.

9.4 Subject to clause 9.5, these Terms and Conditions constitute the entire agreement between us in relation to your accessing of the Extranet. You acknowledge that you have not relied on any statement, promise, representation, assurance or warranty made or given by or on behalf of us which is not set out in these terms and that you shall have no claim for innocent or negligent misrepresentation or negligent misstatement based on any statement in these Terms and Conditions.

9.5 By using or submitting products for submission in this Catalogue of Security Equipment (the "**Catalogue**"), you must accept the additional terms relating to the Catalogue (the "**Additional CSE Terms**"), and by using that part of the Extranet you agree to abide by them.

9.6 No failure or delay by the CPNI 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 by the CPNI of its rights will not be effective until it is delivered to you in writing.

9.7 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 and Conditions.

10. Disputes

10.1 Subject to Clause 10.2, CPNI may elect to have any claims or disputes with you resolved by way of confidential arbitration in front of a single arbitrator who shall be a Queen's Counsel agreed by the parties or,

failing agreement, appointed by the chairman of the Commercial Bar Association.

10.2 If you are a Central Government Body, in the event that the dispute or claim is not resolved by negotiation, the dispute or claim shall be progressively escalated upwards through an appropriate suitable escalation route within CPNI and the Central Government Body until it is resolved.

11. Governing law

11.1 These Terms and Conditions shall be governed by and construed in accordance with the laws of England and Wales. Any dispute arising under these Terms and Conditions shall be subject to the exclusive jurisdiction of the courts of England and Wales