Terms and Conditions of the Security Procedures the Data Receiver Must Implement to Protect the Confidentiality and Integrity of Data

Definitions:

"Data" means any files or other information that is downloaded from the Portal.

"Data Receiver" is the individual or entity that downloads Data from the Portal.

"Data User" means an individual who is a member of the staff or other personnel of the Data Receiver, and any other individuals nominated by the Data Receiver to be a Data User. Such persons will only be considered a Data User after being provided with dedicated identification credentials from the Data Receiver to allow on-site access at the Data Receiver or remote access from a secure desktop environment in order to perform local data analysis.

"Identified Person" means a Data User whose current work-related responsibilities require access to the Data.

"Data Provider" is the individual or entity that uploads to, modifies or retracts Data from the Portal.

"Data Manager" means the person(s) engaged by the Data Receiver who is, for the term of all use of the downloaded Data, responsible for:

a) acknowledging receipt of all Data downloaded from the Portal and maintaining a register for the Data that contains the following information:
    i. date downloaded;
    ii. file name and reference period (or other information to distinguish different files of the Data, if appropriate);
    iii. Identified Person who downloaded the Data;
    iv. the identity of the Data Provider;
    v. Identified Person responsible for safekeeping of the Data (if appropriate); and
    vi. date the Data is destroyed (if appropriate);
b) communicating the security requirements of these terms and conditions and providing training, if required, to all Identified Persons prior to them downloading the Data as described in clause 5 of these terms and conditions;
c) maintaining a record of access to the Data by Identified Persons as described in clause 9 of these terms and conditions; and
d) monitoring and ensuring compliance with the requirements of these terms and conditions and promptly notifying the Data Receiver of any non-conformity so that the Data Receiver may immediately inform the Data Provider and the Parties can agree on the appropriate action to take.

"Identity Management" means the user identity and password as the primary form of authentication for all Data Users. These identities are managed through a central directory maintained by the Data Receiver. All passwords will meet the following complexity rules:

i. Be at least 8 characters in length;
ii. Use both upper and lower case letters;
iii. Include at least one number or special character;
iv. Not include your username; and
v. May not be one of your last three passwords.

"Portable Storage Devices" or "PSDs" means devices that are portable and contain storage or memory into which users can store information, including, but not limited to, laptops, CD-ROMs, flash memory sticks, backup media and removable hard disks.

"Portal" means the online interface enabling upload, download, modification and retraction of the Data.

"Research Project" means the project for which the Data is downloaded from the Portal, which may include publicly disseminating the results of the project via online websites and peer-reviewed publications.

"Secure Location" means anywhere on the Data Receiver's premises that requires either badge or key access by authorized Data Users.

"System" means any electronic or physical system (regardless of the technology used) that, for or on behalf of the Data Receiver, or a third party with which the Data Receiver has a contractual relationship, transmits, stores, analyses, disseminates or disposes of Data, establishes access control(s) and management of the downloaded Data, defines who Data Manager(s), Data User(s) and Identified Person(s) of the Data are, and how the Data will be logged, monitored and audited, to ensure that the Data has appropriate confidentiality, integrity and availability, irrespective of the Data's location. This includes, but is not limited to, personal computers, servers, laptops, tablets, smart phones, virtual computers and cloud based virtual systems.

"Visitor" means an individual, other than a Data User, who has been invited into the secure area by a Data User, as permitted by the Data Receiver's access policies.

Data Ownership and Use

1. The Data remains the property of the Data Provider and are made available to the Data Receiver solely in connection with and for the purpose of the Research Project.

2. The Data Receiver will not process or transfer the Data except within the Data Receiver itself and between it and Identified Persons without the prior written consent of the Data Provider.

3. The Data Receiver will not seek to reverse engineer or de-anonymize the Data in any way whatsoever.

4. The Data Receiver agrees to keep the Data in confidence, except for Data that: (a) are publicly known, or available from other sources which are not under a confidentiality obligation to the source; (b) have been made available by its owners without a confidentiality obligation; (c) are otherwise already known by or available to the Data Receiver without a confidentiality obligation; or (d) are required to be disclosed by operation of law, provided that the Data Receiver takes all reasonable actions to avoid and/or minimize such disclosure.

5. The Data Manager will communicate the security requirements in these terms and conditions to all Identified Persons prior to them accessing the Data and be available for assistance, as required. The Data Manager will also deliver training to Identified Persons if required.

6. The Data Receiver will notify the Data Provider in writing immediately upon becoming aware of non-conformity with any provision of these terms and conditions. Upon

such notification, the Data Provider and the Data Receiver will agree on the appropriate action to take.

7. The Data Receiver will provide such information as is reasonably necessary to enable the Data Provider to satisfy itself of the Data Receiver's compliance with these terms and conditions.

Physical Access

8. The Data will be stored at all times in a Secure Location. All Visitors to the Secure Location will be escorted by a Data User at all times.

9. Access to the Data is limited to Identified Persons. Unless otherwise agreed between the Data Provider and the Data Receiver, a record of access to the Data by Identified Persons will be maintained and record the following:

    a) Data reference;
    b) name of employee or contractor to whom access is given;
    c) justification for access;
    d) name of delegated manager who authorized access and date of authorization; and
    e) start and end dates of the period for which access is authorized.

10. Under no circumstances will Visitors be permitted to access the Data without an authorized Data User present.

Storage and Transmission

11. All Systems with access to the Data will employ Identity Management at the device and network level.

12. All Systems will have up-to-date antivirus software and security patches installed and managed by the Data Receiver.

13. Data will not be electronically transmitted, except as described in clauses 15, 16, 17 and 18 of these terms and conditions. Electronic transmission includes, without being limited to, transmittal of the Data by e-mail.

14. All the Data Receiver's servers where the Data will be stored will be centrally managed to ensure the latest security patches are applied, antivirus software is up-to-date and the appropriate access controls are in place in order to protect the confidentiality, integrity and availability of the Data.

15. The Data can be accessed using the Data Receiver's secure Virtual Private Network (VPN) platform which relies on the access controls to secure the Data. Logs of all user connections will be retained by the Data Receiver.

16. The Data Receiver will apply physical and logical segregation of different networks and the use of modern firewalls and routers to ensure the security of the different parts of its network. The Data will be stored on equipment in secure areas of the network which are not accessible from unsecured networks and where appropriate firewall rules are in place to create targeted access controls.

17. Network firewall rules will be in place such that no system processing the Data can

communicate at the network layer with any system that can be accessed by non-Identified Persons. Network firewall rules will also be in place such that no system processing the Data can be accessed at the network layer by a system outside of the secure area. Data may be stored on and transmitted over networks not meeting these requirements, provided that it is encrypted, except when at rest and in use by an Identified Person. Alternatively, the Data may be stored on a stand-alone computer in a secure area with no external connections, or on a closed network within the secure area.

18. If agreed between the Data Provider and the Data Receiver, all transmission of the Data into and out of a System will use Transport Layer Security encryption. When Data is transmitted outside a Secure Location, the Data will be encrypted at all times (including on a PSD or laptop) using the 256-bit Advanced Encryption Standard (AES-256) both at rest as well as in all backups of the Data. The Data can be analyzed within a Secure Location in an unencrypted state

Physical Storage

19. The Data will not be removed from the Secure Location (as described in clause 8 of these terms and conditions) in any format (e.g., printouts, PSDs, etc.), except as described in clauses 15, 16, 17 and 18 of these terms and conditions.

20. When not in use, printed documents containing original Data will always be stored in secure containers in a Secure Location.

Data Copying and Retention & Record Management

21. The Data must be backed up regularly, when Data is required to be encrypted, all backups of that Data will also be encrypted. Backups of the Data will be stored in a secondary Secure Location area respecting the same access controls as of the primary Secure Location.

22. The Data Receiver will make extracts of the Data and produce copies of this only for the purposes of carrying out work in accordance with the Research Project. When no longer needed, the Data and any such copies or extracts, including all back-up, PSDs, photocopiers and other electronic media where the Data have been electronically stored will be sanitized or disposed of as appropriate.