# Information Security Data Assurance Request Evaluation

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Project Title/Topic:** |  | | |  |  |  |
| **Principal Investigator:** |  | | |  |  |  |
| **Researcher(s):** |  | | |  |  |  |
| **Authority Requesting Assurance:** |  | | |  |  |  |
| **Institution (if not LSE):** |  |  |  | | |  |
| **Date received by InfoSec** |  |  |  | | |  |
| **Reviewed by:** |  |  |  | | |  |

|  |
| --- |
| **Governance / Behavioural requirements in the data assurance request that the project must observe:** |
| **Main behavioural requirements – 1**  **Information Security Awareness Training**  You can self-enrol on the *Information Security Awareness Training* course via <https://moodle.lse.ac.uk/course/view.php?id=5242>  Training taken?  Yes  No  Date of course completion:  Are all sessions complete?  Yes  No  *Please note that taking the training course is mandatory. Please be aware that the course completion can be spot checked by InfoSec, the research data provider, and the research funder.* |
| **Main behavioural requirements – 2 Device level security, storage, physical format of data**  Device level security  Please indicate below whether the following can be achieved?  1. Any mobile device (e.g. laptop, phone, external storage device) that’s used to store, access, or transcribe the data must have full drive encryption applied (e.g. FileVault on Mac, BitLocker for Windows, VeraCrypt for Windows Home Edition).  Please refer to the encryption guideline at:  <https://info.lse.ac.uk/staff/divisions/imt/assets/documents/infosec/encryption-matrix.pdf>  2. Strong encryption key (meeting password policy [<https://info.lse.ac.uk/staff/divisions/imt/services/infosec/resouces/passwords>] at least)  3. Strong logon password (meeting password policy)  4. Actively operate anti-virus software with regular scans  5. Actively operate a software firewall (enable the built-in firewall option in the operating system)  6. Keep the operating systems up to date by installing security patches as soon as they are released  7. Keep other software up to date by implementing security patches as soon as they are released  8. Apply a screen saver that automatically locks after 5 minutes’ inactivity  9. Enable the ‘remotely wipe data’ option for laptop  MAC <https://support.apple.com/kb/PH2701?locale=en_US>  Windows – can use software like Prey  10. Apply a ‘privacy screen’ for laptop if working in public area (e.g. 3M laptop privacy screens)  11. Any external storage device if containing personally identifying data must be encrypted  *Note: By default for LSE desktop patches are pushed out but you’ll need to reboot in order to apply them; files by default are saved on H space; the log-in is via standard LSE network account; Sophos anti-virus is installed. If there are any deviations from above, or if further measures are required (e.g. encryption of hard drive), please then contact the IMT Service Desk <It.Servicedesk@lse.ac.uk>*  Data storage   1. School provided data storage options – H: space, One Drive for Business, SharePoint, departmental shared folder (for staff) 2. If data are stored on departmental shared folder, or SharePoint, then please indicate below whether the following can be achieved:   ‘least privilege’ and ‘need to know’ are observed, i.e. only the right personnel has the right access to the right resources  The access is ‘role based’ (i.e. access is assigned via user groups) instead of being assigned to individuals  Indicate you understand the regular folder permission review requirements (e.g. every 6 months) to make sure only the right people have access to the right resources.  *If the data are stored in other locations than above, please note below:*  ­­­­­­­­­­­­­­   1. Other identifying information e.g. completed consent form, interview notes, personal information of survey respondents /research participants etc. are encrypted while saved outside LSE-provided storage place (e.g. while locally residing on the personal laptop, external storage device, etc.) Please refer to the encryption guideline at: <https://info.lse.ac.uk/staff/divisions/imt/assets/documents/infosec/encryption-matrix.pdf>   Can above be achieved?  Yes  No  Physical format of data   1. Physical format of identifying data are kept in a locked file cabinet and are securely destroyed when no longer in use   Can above be achieved?  Yes  No |
| **Main behavioural requirements – 3**  **Backups**  If the data are stored locally on a laptop, or on external storage device, how are you ensuring data are backed up? (e.g. what would happen if the laptop is lost/stolen and the data stored there locally are no longer available) |

|  |
| --- |
| **Main behavioural requirements – 4**  **If you are conducting interviews, are they recorded?**  Yes  No  **If Yes** –additional security measures are applied as follows  Recording device – dictation device   * If dictation device is used (this is the ideal option) – The recording device is kept in a safe place when unattended. * Models with real-time encryption capabilities include:   Olympus DS -7000  Olympus DS -3500  Phillips DPM 8000/00   * For video recording, there’s no proven devices that support real-time video encryption capabilities. Video recording represents a higher risk around personally identifiable data; any video recording files should be imported to a computer with adequate protection at first instance.   Recording device – smart device   * If smart device is used for audio/video recording, the following should be applied:   Full device encryption  Keep iOS or Android up to date  Keep all apps up to date  Only download apps from apple store or google play store  Enable the ‘remotely wipe data’ option  Recording apps   * If recording apps are used, ensure the recording files are not automatically synced into a third party cloud service, and that any locally stored recording files are in an encrypted folder (or reside on an encrypted drive).   Recording files   * Original recordings must be imported from the recording device to the computer at first instance, and be deleted from the recording device as soon as these are imported. * Original recordings are kept encrypted while residing outside LSE provided storage (e.g. while locally residing on the personal laptop, external storage device, etc.)   Transcription   * If a third party transcription service is involved then non-disclosure agreement should exist. LSE can supply model NDA templates. * Cloud based automatic transcription software is not advised if the recorded contents are sensitive, or if the interviewee’s identity is sensitive. If a cloud based transcription software has to be used, then please indicate below that the following are followed and understood:   Check the terms of services  Be aware of what the provider does with the voice, what data they store, where the data are physically stored, how long the data are stored for, and what the data are used for by the provider (any use outside the transcription, for example using the data for improving their voice recognition accuracy, is in breach of GDPR)  The transcription of voice data has to be within the EEA or countries with equivalent level of protections (for an official list of such countries please refer to <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>)  Can all of the above be achieved?  Yes  No  Audio and Video Recording guideline at:  <https://info.lse.ac.uk/staff/divisions/imt/assets/documents/policies/AV-Recording-Guidelines.pdf> |
| **Main behavioural requirements – 5**  **Third party survey solutions**  School preferred survey providers:  Qualtrics, survey monkey  If other providers are used, please note below, and indicate if you have checked their terms and usage and ensure that the usage of such tool meets GDPR requirements. If unsure please contact [secdiv.gdpr@lse.ac.uk](mailto:secdiv.gdpr@lse.ac.uk)  Yes  No |
| **Main behavioural requirements – 6**  **Content scrapers**  It is technically not illegal to use content scrapers.  If a content scraper is used, please check the terms of service of the contents provider.    The content provider might have set conditions of using a content scraper, or might require the explicit consent of their users in order for the content scraper to be used.  If it is unclear from the terms of service whether the tool is permitted, or under which conditions, then get in touch with the content provider to ensure permission is obtained.  Has above been followed?  Yes  No |
| **Main behavioural requirements – 7**  **Applicable Policies/regulations:**   1. The EU General Data Protection Regulation (GDPR) should be complied with from 25th May 2018. Any data breach of the identifying data would subject the School to a financial fine of 4% of the global turnover or € 20 million, whichever is higher. Please refer to the School’s GDPR page at:   <https://info.lse.ac.uk/staff/divisions/Secretarys-Division/Information-Rights-and-Management/GDPR>   1. Comply with the School’s Information Security Policy <https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/infSecPol.pdf> 2. Comply with the School’s Conditions of User of IT Facilities <https://info.lse.ac.uk/staff/services/Policies-and-procedures/Assets/Documents/conOfUseOfITFacAtLSE.pdf?from_serp=1> |

|  |
| --- |
| **Any other issues requiring action?** |
| Please provide additional details and get in touch with [imt.infosec@lse.ac.uk](mailto:imt.infosec@lse.ac.uk) if your research involves additional areas that are not covered by above |

|  |  |  |
| --- | --- | --- |
| **Technical controls requiring implementation** | | |
| **Control description** | **Who will implement?** | **Team contacted/Job no.** |
|  |  |  |
| **Date for information security follow-up** | | |
|  | | |