2) Protection of PII.	17	100	70	2 sheets (4 sides) of A4 sheets inclusive of any graphs, figures and tables.

Please provide details of how your organisation will meet each of the requirements for **Protection of PII** outlined in Framework Schedule 6 Order Form, Special Clauses and Call-Off Schedule 20, Call-Off Specification, Security - Protection of PII.

[redacted]

Tender Response (Please input your tender response to this question)

We have an integrated system for the management of information security in line with ISO 27001 covering the safety, security and prevention of risks due to information security breaches. We have held Cyber Essentials at Cyber Essentials Plus level since July 2018.

The systems and procedures in place to support these standards means that the Authority can have total confidence in the security of our communications and in the electronic transfer of documents.

We therefore place a great emphasis on security, both within our head office facility and within our translator population, and this drives all our core functions. Security is embedded in all processes and employees undergo annual awareness and training to ensure their - and our - ongoing adherence to the ISO standard.

To ensure the continuing relevance and appropriateness of our approach to security, we have an advisory board which is headed up by the Managing Director of the company, Urwi Patel. The Managing Director assumes responsibility for the implementation and of governance and security approaches including the ongoing adherence to the ISO27001:2013 standard.

REDACTED Under FOIA Section 43 Commercial Interest

Security when recruiting translators

Our recruitment process is designed to ensure we recruit only the best (we reject over 60% of applicants). The vetting procedure followed for linguists includes first verifying that they comply with Baseline Personnel Security Standards (BPSS) by checking the following:

REDACTED Under FOIA Section 43 Commercial Interest

Information collected is reviewed and assessed, and recorded on the BPSS Verification Record. Subject to GDPR, any information collected as part of the vetting process will be available to the Authority's authorised personnel, should they wish to undertake audits at any time during the contract term.

Data security during document translation

REDACTED Under FOIA Section 43 Commercial Interest

All translators are required to sign our security policy and confidentiality policy and are provided with training on data security such as data protection, information governance and information security guidelines. This is done via e-learning CPD certified training. The team assigned to the current Authority contract have also all undertaken bespoke training requirements relating to the Authority contract, to ensure that the translators are provided with the correct level of training to ensure data is kept secure at all times and destroyed when required.

REDACTED Under FOIA Section 43 Commercial Interest

When they are at our office, documents are stored securely in an alarmed storage room.

REDACTED Under FOIA Section 43 Commercial Interest

In addition, all translators are required to treat the information they read and translate as confidential and must conform to the requirements of the Data Protection Act (2018).

Data Protection Impact Assessments (DPIA), are completed by the project management team when processing personal data, with information passed to our continuous improvement team.

Staff training and procedure

Translators undergo induction training and annual awareness and training on our information security policies and procedures to ensure their - and our - ongoing adherence to these standards.

All Language Empire staff sign a non-disclosure/confidentiality agreement for each organisation they work on behalf of and this is kept in their HR file. This agreement states that staff/linguists must not "disclose any personal information about service users, other than to the public sector professionals directly responsible for the specific aspect of service delivery to which the assignment relates, and to act in accordance with the relevant guidelines of the public sector body with whom the Provider is under contract."

Our translators are also bound by a non-disclosure agreement. This mandates that the translator does not record details or retain any confidential documents relating to the assignment. Also, all translators must adhere to national codes of conduct which have elements of Information Security and Data Protection awareness embedded.

For this contract, translators will also have completed the Defence Information Management Passport.

REDACTED Under FOIA Section 43 Commercial Interest

Vulnerability testing

To ensure that our information systems are not being misused and have been secured in a manner that reduces or eliminates potential threats, Language Empire's IT support team conduct periodic vulnerability testing. Our network is subject to annual penetration tests and regular surveillance audits by the accrediting body as part of our certification. All data is stored in a certified and tested environment and sensitive data is encrypted when sent electronically. Security logging and monitoring tools ensure compliance and alert to any deviation from policy. Sensitive data is encrypted both in transit and at rest.

REDACTED Under FOIA Section 43 Commercial Interest

Once risks have been identified for an information system or application, the Information Owner must determine whether to accept the risk (provided the risk is low and the cost to control the risk is not cost effective for Language Empire), mitigate the risk, or defer each risk to other parties, such as insurers. Before any risks are analysed we ensure we have identified interested parties and their risk requirements. Each vulnerability alert and patch release is checked against existing Language Empire systems and services prior to taking any action, in order to avoid unnecessary patching. The decision to apply a patch, and within what timeframe, is taken following the guidelines presented in the Language Empire Patch Priority Matrix.

All patches are downloaded from the relevant system vendor or other trusted sources. Each patch's source must be authenticated and the integrity of the patch verified. All patches are submitted to an anti-virus scan upon download. New servers and desktops are fully patched before coming online, and new software is fully patched when installed on Language Empire resources, in order to limit the introduction of risk. Patches are tested prior to full implementation. A back out plan that allows safe restoration of systems to their pre-patch state is devised prior to any patch rollout in the event that the patch has unforeseen effects. All configuration and inventory documentation is immediately updated in order to reflect applied patches.

Monitoring network logs

We have a dedicated in-house IT team who have provision in place to monitor network logs in real time. We ensure that all security logs are monitored weekly and management reports are sent on a monthly basis as part of our IT security monitoring for ISO27001.

Penetration testing

In addition to internal reviews, we engage the services of an external penetration test company who conduct a six-monthly assessment of the environment to determine if any new IT vulnerabilities have been discovered. The testing is scoped to ensure tests include assessments of external attacks and malicious insiders / compromised hosts. Should the testing discover problems, these are addressed immediately with a risk-management based remediation process.

REDACTED Under FOIA Section 43 Commercial Interest

Information disposal

REDACTED Under FOIA Section 43 Commercial Interest