3) Incident Reporting.	17	100	70	2 sheets (4 sides) of A4 sheets inclusive of any graphs, figures and tables.

Please provide detail of your organisation's proposed **Incident Reporting** Process in line with Framework Schedule 6 Order Form, Special Clauses and Call-Off Schedule 20, Call-Off Specification, Security - Incident Reporting.

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

Language Empire has a Business Continuity Policy and plan under which the company can continue to deliver services in the event of any disruption, including a security incident. This runs alongside our Risk Assessments/Register.

In order to ensure full compliance and that the planning is robust, this policy has been developed in accordance with the following standards:

REDACTED Under FOIA Section 43 Commercial Interest

The policy provides a clear commitment to business continuity planning which enable us to reduce the period of disruption, improve the resilience of the infrastructure to reduce the likelihood of disruption, and reduce the operational and financial impact of any disruption. It fully meets the Authority's requirements included at call off schedule 8.

REDACTED Under FOIA Section 43 Commercial Interest

Each process within Language Empire is owned by a specific individual.

We produce a bespoke Information Security Management System (ISMS) for each new contract we are awarded – this will be shared with the Authority for approval during implementation.

Language Empire defines a security breach / incident as any unauthorised access to goods, services, sites or data. In the event any security breach occurs, we have robust Incident Response & Reporting Processes (covered by the ISO27001:2013 SOA) to detect, confirm, contain and investigate incidents.

REDACTED Under FOIA Section 43 Commercial Interest

Language Empire will notify the Authority Integrated Assurance Team immediately if a breach is confirmed.

Our post-incident investigation process will look to identify the root cause of the breach and provide preventative action guidance to our leadership team.

Full updates will be provided to the Authority until the breach is deemed fully resolved.

All staff have individual roles and responsibilities and each role has a clearly defined expectation regarding data an information security and information governance. This makes up part of their job descriptions and any breach would be deemed gross misconduct in our disciplinary procedures and practice.

REDACTED Under FOIA Section 43 Commercial Interest