SUPPLIER RESILIENCY REQUIREMENTS

These Supplier Resiliency Requirements apply to a service provider or supplier providing goods or services deemed critical to RELX ("Supplier"). "RELX" means RELX Group plc and any of its partially or wholly-owned direct or indirect subsidiaries receiving goods or services from Supplier.

Supplier must account for known and reasonably anticipated risks and threats and monitor and adapt to new threats.

Supplier shall be prepared to provide RELX a current, independent report (or a substitute report, accepted within the reasonable discretion of RELX, identifying Supplier's compliant testing activities, any discovered issues, and any applicable remediation steps) demonstrating Supplier's compliance with its resiliency obligations for relevant goods and services set forth herein. Such report should arise from a third party auditor accredited by ANSI, ANAB, or a similar accrediting body. Supplier shall promptly provide RELX such report upon a reasonable likelihood of, or an actual event of, a material disruption or upon reasonable request not more than annually.

"Business Continuity Program" means documented policies and procedures for sustaining Supplier business operations upon disruption to ensure consistency, sustained performance, and provision of goods or services to RELX.

"IT Disaster Recovery / Technical Resiliency Program**"** means documented policies and procedures for getting important Supplier information technology infrastructure and business operations up and running again if a disruption affects RELX.

Supplier's goods and services must actively meet or exceed one or more of the following:

□ be FedRAMP designated;

□ current ISO 22301 standards for Supplier's Business Continuity Program (and for the IT Disaster Recovery / Technical Resiliency Program, meet or exceed other listed requirements);

□ Supplier's own superseding written requirements, as mutually agreed upon by Supplier and an authorized representative of RELX; or

□ the RELX Minimum Requirements below, as approved by Supplier senior management, sufficiently documented, and regularly reviewed or tested.

For internal RELX review purposes, Supplier should check its applicable requirements or standards above. A change to this selection may be provided to RELX upon written notice.

RELX Minimum Requirements

1. BUSINESS CONTINUITY PROGRAM

1.1 Supplier's Business Continuity Program shall address the following:

1.1.1 management commitment to established policies and objectives;

1.1.2 integration into the Supplier's business processes;

1.1.3 a process that ensures achievement of intended outcome(s);

1.1.4 established roles and responsibilities;

1.1.5 criteria for accepting risks as well as the acceptable levels of risk;

1.1.6 review at planned intervals and when significant changes occur (i.e. environment changes, or change of Supplier's business and structure);

1.1.7 awareness through an ongoing education and information program for relevant staff and establish a process for evaluating the effectiveness of the awareness delivery;

1.1.8 exercising and testing, including alternate and redundant communication methods for internal and external parties; and

1.1.9 prompt remediation of identified deficiencies.

Supplier's Business Continuity Program shall have protection and mitigation for identified risks, including proactive measures that reduce the likelihood of disruption, shorten the period of disruption, and limit the impact of disruption on the Supplier's key products and services.

1.2 Supplier will conduct a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident, or emergency ("Business Impact Analysis").

1.2.1 The Supplier shall establish, implement and maintain a formal and documented process for Business Impact Analysis and risk assessment that establishes the context of the assessment, defines criteria and evaluates the potential impact of a disruptive incident.

1.2.2 Based on recovery objectives identified in the Business Impact Analysis, Supplier shall establish, document, implement, and maintain business continuity procedures (the "**Procedures**") as part of its Business

Continuity Program. The Procedures must be regularly reviewed by management and tested to manage a disruptive incident and continue Supplier operations.

2. IT DISASTER RECOVERY / TECHNICAL RESILIENCY PROGRAM

2.1 Supplier’s IT Disaster Recovery Program shall address the following:

2.1.1 Supplier's disaster recovery objectives;

2.1.2 the scope of the IT Disaster Recovery / Technical Resiliency Program, including limitations and exclusions;

2.1.3 review at planned intervals and when significant changes occur, such as environmental changes, or change of a Supplier's business and structure;

2.1.4 roles and responsibilities set by management and a person with appropriate seniority and authority to be accountable for the IT Disaster Recovery / Technical Resiliency Program’s policy and implementation;

2.1.5 awareness through an ongoing education and information program for relevant staff and establish a process for evaluating the effectiveness of the awareness delivery; and

2.1.6 prompt remediation of identified deficiencies in the IT Disaster Recovery / Technical Resiliency Program.

2.2 Supplier shall ensure that any services that are required to enable disaster recovery to occur have:

2.2.1 documented Recovery Time Objectives (RTO) and Recovery Point Objectives (RPOs), as defined herein;

2.2.1.1 “Recovery Time Objective” is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

2.2.1.2 “Recovery Point Objective” concerns the amount of data at risk. RPO is determined by the amount of time between data protection events and reflects the amount of data that potentially could be lost during a disaster recovery.

2.2.2 regular review from a prevention perspective to assess risks of service interruption or degradation;

2.2.3 periodic review to improve service resilience and lower the likelihood and/or impact disruption to Supplier's goods and/or services;

2.2.4 a management notification procedure for gaps between critical disaster recovery capability and business continuity requirements; and

2.2.5 strategies for reducing the impact of the unavailability of the normal facilities, technologies, data, and suppliers.

3. INCIDENT RESPONSE

3.1 The Business Continuity Program and IT Disaster Recovery / Technical Resiliency Program shall each establish, document, and implement procedures and a management structure to respond to a disruptive incident using personnel with the necessary responsibility, authority and competence to properly manage an incident (“Incident Response Procedure”). The Incident Response Procedure must, at a minimum:

3.1.1 confirm the nature and extent of the incident;

3.1.2 take control of the situation;

3.1.3 contain the incident;

3.1.4 promptly communicate with RELX and/or Affiliate stakeholders and SupplierIncidents@RELX.com;

3.1.5 Provide regular status updates and as requested by RELX.

Additionally, the Incident Response Procedure should trigger appropriate Business Continuity Program or IT Disaster Recovery / Technical Resiliency Program action(s). This response should integrate with overall Incident Response Procedures. Those responsible for incident management should have plans for the activation, operation, coordination and communication of the incident response including how to communicate to RELX.