ISO27001: 2017 ISMS
INFORMATION SECURITY MANUAL

Version 1

24th October 2019

1. Introduction

1.1. This manual provides the framework for the policies and procedures which the top management of Time to Reply Ltd have adopted to implement an information security management system which complies with ISO/IEC 27001:2017 ("the ISMS").

1.2. This manual explains Time to Reply Ltd's approach to information security and contains both the management policy statement on information security in Time to Reply Ltd and, because it identifies which of the controls identified in Annex A of ISO27001:2017 apply to Time to Reply Ltd, it is also Time to Reply Ltd's Statement of Applicability.

ISO27000:2012 provided definitions that are used in this ISMS.

ISO27002:2013 provided guidance on the selection and implementation of controls.

1.3. Time to Reply Ltd's document control procedures (section 4.10 and 4.11) apply to this manual and to all other documents within the ISMS.

2. Change history

Details of changes to this manual are recorded in section 13.

Issue of this manual is authorised by:

Signature of the Managing Director

On: 24th October 2019

3. Scope

3.1. Scope of the ISMS

The ISMS will encompass all functions of Time to Reply Ltd. Specifically, this will incorporate:

- All Administrative functions, including the management of employee and contractor records.
- All Sales functions, including the management of customer commercial records.
- All Operational functions, including the management of customer operational records, sub-contractor records and services conducted by staff and contractors.
- All sub-contractors that hold or process information related to staff, customers, sub-contractors, contractors, customers or subjects of customers and any other sensitive information held or processed by Time to Reply Ltd.

All aspects of Time to Reply Ltd are within the scope of this system

3.2. Definitions

Where terms which are used in ISO27001:2017 or ISO27002:2013 are used here, the definitions provided in ISO27000:2012 are applied.

In particular, the **Information Security Management System** ("ISMS") is defined as the part (which includes organisational structure, policies, planning activities, plans, responsibilities, working practices, procedures, processes and resources) of Time to Reply Ltd's overall management system which, based on a business risk approach, enables management to establish, implement, operate, monitor, review, maintain and improve information security within Time to Reply Ltd.

4. Documentation

4.1. Time to Reply Ltd's ISMS documentation consists of:
4.2. The scope statement (section 3 above), information security management system (section 5 below), and Statement of Applicability (RM-ISMS_DOC_6.1.3d). This manual is, together with any separately published policies, Time to Reply Ltd's Tier 1 ISMS documentation.
4.3. The control objectives described in this manual are achieved by controls that include policies (which provide Board of Directors approved guidelines on specific control areas) and procedures. These policies are either included in, or referenced from, this manual (ISO27001 7.5.1).
4.4. The separate, version-controlled risk assessment report and risk treatment plan, whose preparation follows the methodology described in section 6 (below) of this manual (ISO27001 6.1.2 and 6.1.3).
4.5. Records of how Time to Reply Ltd applied (and continues to apply) its continual improvement process, which is described in section 3 (above) of this manual, in improving the suitability, adequacy and effectiveness of its ISMS (ISO27001 4.4 and 10).
4.6. Those procedures, which describe how the policies are implemented, and which are identified in this manual but are separate from it, are Tier 2 documents (ISO27001 7.5.2 and 7.5.3).
4.7. Work Instructions and Operations Work Instructions, which set out specific requirements for the performance or execution of specific tasks, including for the measurement of the effectiveness of the controls, in Time to Reply Ltd generally and in the IT Department specifically, and which are identified in procedures, and similar documents, such as User Agreements and Job descriptions, are Tier 3 documentation.
4.8. Records of Time to Reply Ltd's control of its information security processes, including details of audits, information security incidents and management reviews, are the fourth tier of Time to Reply Ltd's ISMS documentation (ISO27001 7.5.1b and 9.2g).
4.9. Authorisation levels
  4.9.1. Time to Reply Ltd has clearly defined authorisation levels which cannot be delegated.
  4.9.2. The Board of Directors has ultimate authority over the information security policy and ISMS and approves and authorises all changes to the information security policy, the Statement of Applicability, the information security manual and any separate policy statements (tier 1 documents).
  4.9.3. The Chief Information Security Officer (CISO (DIRECTOR)) has lead executive authority for information security and works with the Board of Directors to approve, authorise and issue all tier 2 documents.
  4.9.4. The Information Security Manager and all Department Managers approve and authorise tier 3 documents owned by individuals or entities in their areas of responsibility. Any information security documents personally owned by Department Managers have to be approved and authorised by the Chief Information Security Officer (CISO (DIRECTOR)).
  4.9.5. Owners of information assets (See Annex: Control A.8 of the Manual) are responsible for the security classification of their asset(s), the day-to-day

protection of their asset(s) and for the day-to-day operation of related security processes. The responsibility for carrying out these processes or associated task(s) can be delegated to anyone within the Owner's area of responsibility, provided that:

a. The individual has the necessary skill, competence and resources to carry out the processes or task(s).
b. The Owner retains accountability for ensuring that the process or task is carried out correctly.

4.9.6 Access rights are specified in Annex: Control A.9. Access rights are personal, are set out in individual User Agreements (Annex: Control A.9 below) and cannot be delegated.

4.10 Time to Reply Ltd's ISMS documentation is protected and controlled. There is a documented control procedure (MSS DOC 7.5.3) which takes 3.1 Scope (above) into account and defines the management actions for document control (ISO27001 7.5.3).

4.11 Time to Reply Ltd has a documented procedure for the Control of Records (ISMS-C DOC 18.1.3) which defines the controls for identification, storage, protection, retrieval, retention time and disposal of records. (See Annex: Control A.18, 18.1.3 below) Documents are available to those who need and are authorised to access them in line with these requirements.

5. Information security management system

Time to Reply Ltd has established, implemented, maintained and continually improves the ISMS (ISO27001 4.4 and 10).

5.1 Establish the ISMS

a. Time to Reply Ltd defined the scope of the ISMS in section 1.
b. Time to Reply Ltd has defined its information security policy, which is set out in section 5, to apply throughout Time to Reply Ltd as defined in the scope (section 1 above). The policy includes:
   b1. A framework for setting information security objectives for the ISMS ("in order to preserve its competitive edge, cash-flow, profitability, and commercial image" and "an enabling mechanism for information sharing, for electronic operations") and an overall sense of direction ("will continue to be aligned with Organisational goals") and principles ("are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets") for action with regard to information security (ISO27001 5.1.a).
   b2. The requirement for "legal, regulatory and contractual compliance" (ISO27001 5.2.c).
   b3. The strategic organisational and risk management context for the establishment and maintenance of the ISMS ("the Organisation's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks") (ISO27001 5.2.b).
   b4. Reference to a systematic approach to risk assessment, the risk management framework (8.1 below) in which the criteria for risk evaluation are described and the structure of the risk assessment is defined (8.5 below) (ISO27001 6.1.2.a.2).
   b5. The policy and this manual have been approved by top management (ISO27001 5.2).
c. Time to Reply Ltd has identified a suitable, systematic approach to and framework for risk assessment that produces consistent, valid and comparable results and that is appropriate for its business, legal, regulatory and contractual requirements, and this is described in section 8 below (ISO27001 6.1.2.b).
d. Identification of risks is carried out in line with the process set out in section 8 below (ISO27001 6.1.2.c.1).
e. Assessment (the analysis and evaluation) of risks is carried out in line with the process set out in section 8 below (ISO27001 6.1.2.d and 6.1.2.e).
f. Options for risk treatment are identified and evaluated in line with the process set out in section 8 below (ISO27001 6.1.3.a).
g. Control objectives and controls are selected from any appropriate source to meet the criteria and requirements of the risk management framework, take into account the risk acceptance criteria (see section 8 below) and legal and regulatory requirements and contractual obligations, have been compared with the controls listed at ISO27001:2017 Annex A (see ISO website) and are contained in the Statement of Applicability (ISO27001 6.1.3.d).

h. The Statement of Applicability records whether the organisation is applying the controls of Annex A, along with the justification for or against this decision, as well as details of those controls selected that are not listed in Annex A (ISO27001 6.1.3.d).
i. The Statement of Applicability is contained in sections five to eighteen of this manual and the work instruction RM-ISMS DOC 6.1.3d in approving this manual the risk owners accept the residual risks (see section 8.6.3 below also) (ISO27001 6.1.3.f).
j. Top management authorises implementation of the ISMS and any changes to this manual (ISO27001 5.1).

5.2 Implement the ISMS

a. Time to Reply Ltd's risk treatment plan (RM-ISMS REC 6.1.3 Pt1, Part 2, Part 3, Part 4, Part 5, Part 6)reflects the decisions made in 5.1 above, and identifies the management action, responsibilities and priorities for managing the identified information security risks (ISO27001 6.1.3.e).
b. Appropriate funding and resources are, as described in the risk treatment plan, allocated to its implementation (ISO27001 6.2.g).
c. The selected controls are implemented (and their implementation is co-ordinated across Time to Reply Ltd) to meet the identified control objectives (ISO27001 8.3).
d. Time to Reply Ltd has defined how it evaluates the performance of the ISMS and measures the effectiveness of its controls and has specified how to use these measurements to improve control effectiveness to produce comparable and reproducible results, and this is set out in (MSS DOC 9.1), monitoring, measurement, analysis, evaluation procedure (ISO27001 9.1).
e. Awareness programmes, applicable to people doing work within the scope of the ISMS and under the control of Time to Reply Ltd, are implemented as required in the risk treatment plan, (RM-ISMS REC 6.1.3 Pt1, Part 2, Part 3, Part 4, Part 5, Part 6), quality management system awareness procedure (ISO27001 7.3).
f. Time to Reply Ltd has identified competence requirements in respect of the ISMS and has taken appropriate action to ensure that relevant roles have relevant competences, (MSS DOC 7.2), competence procedure (ISO27001 7.2).
g. Top management uses its Internal Audit process to ensure that the operational management procedures and work instructions required in this manual are implemented (ISO27001 8.1).
h. Time to Reply Ltd has committed specific resources to the effective management of the ISMS, including the appointment of a Chief Information Security Officer (CISO (DIRECTOR)), , recruitment of additional training/technical staff, inclusion of information security in all job descriptions as well as investing in information security products and services as required by the risk treatment plan (RM-ISMS REC 6.1.3 Pt1, Part 2, Part 3, Part 4, Part 5, Part 6) (ISO27001 7.1).

i. Time to Reply Ltd has implemented measurement and monitoring procedures and controls as described in Annex: Control A12.4 and A16.1 (below) (ISO27001 8.1).

5.3 Maintain the ISMS

a. The controls implemented to meet control objectives (Annex: Control A12.4 and A16.1) below are operated to promptly detect processing errors and detect security

events, to identify failed and successful security breaches and incidents, enable management to assess whether security activities are performed in line with the criteria set for them, and take action to resolve any breach of security in a way that reflects Time to Reply Ltd's priorities, also see section 5.4 below (ISO27001 9.1).

b. Time to Reply Ltd and its management regularly review the effectiveness of the ISMS, in line with the policy and procedures identified, seek to continuously improve the effectiveness of the ISMS through analysing audit results, and monitoring events and activity, all in the context of the business goals and risk treatment plan, and at least once a year (ISO27001 9.2 and 9.3).
c. Time to Reply Ltd evaluates the performance of the ISMS, as set out in MSS DOC 9.1, to verify that security requirements have been met (ISO27001 9.1).
d. At planned intervals as well as whenever there are significant changes in Time to Reply Ltd, technology, business objectives and processes, identified threats or external (legal, regulatory, social) changes, Time to Reply Ltd reviews those aspects of its risk assessment and risk treatment plan, including levels of residual risk and acceptable risk (taking into account changes in the effectiveness of controls), that are affected by the changes, or carries out additional assessments of specific risks in relation to new technologies, and system or any other changes that affect Organisational information or information assets (ISO27001 8.2).
e. Management ensures that Time to Reply Ltd carries out regular internal ISMS audits in accordance with the Internal Audit Procedure (MSS DOC 9.2) and Internal Audit Schedule (MSS REC 9.2.1).
f. Other audits are conducted as required (See Annex: Controls 12.7.1 and 18.2 below) and the results of these audits inform the reviews identified in 5.3b) above (ISO27001 5.1.e and 9.2.c).
g. Actions or events that could impact the effectiveness of the ISMS are recorded in line with the controls (See Annex: Controls 12.4 and 16 below) (ISO27001 6.2.e and 9.3) and are reviewed at management review.
h. The risk treatment plan (RM-ISMS REC 6.1.3 Pt1, Part 2, Part 3, Part 4, Part 5, Part 6) is updated to take into account the findings of monitoring and reviewing activities.

5.4 Continually improve the ISMS

a. Where improvement opportunities for the ISMS are identified during the maintenance phase (see 5.1 b) and d) above), they are implemented if they meet the criteria of the risk treatment plan (ISO27001 10.2).
b. Time to Reply Ltd has the documented Non Conformity and Corrective Action procedure (MSS DOC 10.1) which is complemented by other procedures (including but not limited to those in Annex: controls 15.1, 16 and 18.2 of this manual; and these include evaluating the need for action in response to non-conformities (ISO27001 10.1).
c. The results of reviews are communicated to everyone involved and action delegated to the appropriate people, in line with the documented Non Conformity and Corrective Action procedure (MSS DOC 10.1) and Annex: Controls 6.1.1 and 16.1 below (ISO27001 7.4).
d. The implemented improvements are subject to monitoring and audit (Internal Audit Procedure (MSS DOC 9.2) and Annex: Control 8) to ensure that their intended objectives have been achieved (ISO27001 10.1.d).

6 Context of organisation

Time to Reply Ltd provides software, consultancy and services to various UK sectors. The company was established in 2006 to provide IT application and consultancy solutions.
The company uses sub-contractors to provide both core and non-core services, these include:

- Google and Microsoft for cloud applications;
- Other cloud application providers;
- Our-sourced hosted data centres;
- Out-sources support services, for example accountants.

Any sub-contractor will either be certified to ISO 27001 or will be managed to ensure that they adhere to all relevant Time to Reply Ltd policies, processes and procedures. In this way it is the company's intention to encompass the entire UK operation within its ISO27001 certification.

- **7 Leadership**
-

7.1 Leadership and commitment

7.1.1 Time to Reply Ltd's (ISMS DOC5.2) Information Security Policy demonstrates top management's commitment to information security and the ISMS.

7.1.2 This commitment extends to all objectives, processes and controls defined within the scope of the ISMS.

7.2 Information Security Policy

The information security policy is developed in accordance with both clause 5.2 of ISO 27001.

Control objective: The organisation provides management direction and support for information security in accordance with business requirements and relevant laws and regulations

7.2.1 Information security policy document

The management team and the Board of Directors have approved and authorised an information security policy for Time to Reply Ltd. This policy is set out in ISMS DOC 5.2 and is authorised for separate distribution under the Managing Director's signature. A current version of this document is available to all staff and contractors on the corporate intranet, and to external parties on request.

7.2.2 Review of the information security policy

Time to Reply Ltd's information security policies are reviewed at planned intervals, or when and if significant changes occur, to ensure their continuing suitability, adequacy, and effectiveness.

7.2.3 The Information Security Manager is the Owner of the information security policies and has approved management responsibility for the development, review and evaluation of the policies.

7.2.3.1 Time to Reply Ltd has a defined procedure (MSS DOC 9.3) for the management review of the information security policies, and this includes continual improvement, and assessing policy changes that might be necessary in response to significant changes in the organisational environment, business circumstances, legal conditions, technical environment or requirements of interested parties.

All changes to the information security policy are subject to approval by Time to Reply Ltd's Board of Directors.

7.3 Organisational roles, responsibilities and authorities

7.3.1 Relevant roles and responsibilities with regard to information security and the ISMS are defined in 3 Roles and Responsibilities Document Management Tool (ISMS REC 5.3).

7.3.2 These roles and responsibilities are determined by top management on the basis of ensuring that the ISMS conforms to the requirements of ISO 27001:2017.

- **8 Planning**

8.1 **Risk Management Framework**

Time to Reply Ltd's approach to risk, which has been specifically approved and authorised by management, is contained in the risk management framework which it applies to its overall strategic planning process. The risk management framework is designed to identify and assess risks (including information security risk) in the business plan, to identify and evaluate options for the treatment of those risks, and to select control objectives and controls that will reduce those risks to acceptable levels within the context of the business plan, operational requirements, constraints and objectives and national and international legislation and regulation (ISO27001 4.1, and ISO27002 6.1 and 6.2).

8.2 Time to Reply Ltd's risk management framework is set out in RM-ISMS DOC 6.1.1 (ISO27001 5.1, 5.2 and 6.1.2, ISO27002 0.2).

8.3 Information security risk management

8.3.1 Controls which are required to meet contractual, legal or regulatory requirements are identified at the point of identifying requirements of interested parties, and these controls are implemented. Time to Reply Ltd maintains a legal, regulatory and contractual compliance database which enables it to identify which controls are implemented in relation to which requirements, and these controls are, where appropriate, included in the Statement of Applicability (RM-ISMS DOC 6.1.3d).

8.3.2 Time to Reply Ltd has established and maintains its ISMS, and identifies and assesses information related risks, and evaluates options for their treatment, within the context of the risk management framework described in RM-ISMS DOC 6.1.1 and performs risk assessments in line with RM-ISMS DOC 6.1.2, using the tool selected following the procedure documented in RM-ISMS DOC 6.1.2a.

8.3.3 Control objectives and controls are selected from any suitable source, and then compared to the controls offered in Annex A of ISO27001:2017 on the basis of the conclusions to step 8.3.2 above. All control objectives and controls are documented in the Statement of Applicability (RM-ISMS DOC 6.1.3d) and tool (RM-ISMS Rec SoA).

8.3.4 A consolidated, corporate level risk treatment plan (RM-ISMS REC 6.1.3 Pt1, Part 2, Part 3, Part 4, Part 5, Part 6) is formulated in order to implement the selected controls.

8.3.5 The implementation is reviewed for effectiveness and, where possible, improvements are identified and these, within the context of the overall ISMS, are implemented, using a process of continual improvement.

8.3.6 This process is followed irrespective of whether a single risk is being considered, or multiple risks.

8.4 Risk assessment tool

Time to Reply Ltd's method for risk assessment is risk assessment tool vsRisk. This tool is suitable for the scope of Time to Reply Ltd's ISMS (section 1), the business objectives (3.1 b1. above)), the security, contractual obligations, legal and regulatory requirements (3.1 b2.) above) and risk management framework that were identified earlier. The selection criteria are set out in RM-ISMS DOC 6.1.2a ISO27001 6.1.2 and the risk assessment procedure itself is carried out as described in RM-ISMS DOC 6.1.2.

8.5 Systematic approach to risk assessment

8.5.1 Time to Reply Ltd has a documented approach; framework (RM-ISMS DOC 6.1.1), tool (RM-ISMS DOC 6.1.2a) and procedure/methodology (RM-ISMS DOC 6.1.2) to risk assessment.

8.6 Prepare a Statement of Applicability

8.6.1 The control objectives and controls selected in line with 8.5 above, and as a result of carrying out the procedure identified in RM-ISMS DOC 6.1.2 Risk Assessment Procedure, are documented in a Statement of Applicability (RM-ISMS DOC 6.1.3d) (which forms sections 5 to 18 of this Manual and which is made available as a separate, standalone document, Statement of Applicability) in support of the ISO27001 compliance certificate.

8.6.2 Controls or control objectives in Annex A of ISO27001:2017 are documented, whether included or excluded on the basis of the risk assessment, together with the justification for their inclusion or exclusion; any additional controls or control objectives that may be required are also documented in the Statement of Applicability and are included in this Manual as additional points following Control A.18.

8.6.3 The remaining residual risks are highlighted in the risk treatment plan (RM-ISMS REC 6.1.3 Pt1, Part 2, Part 3, Part 4, Part 5, Part 6) as required by RM-ISMS DOC 6.1.1, approved by the risk owners, and management authorisation is obtained for implementation of the ISMS.

Any changes to the risk treatment plan (RM-ISMS REC 6.1.3 Pt1, Part 2, Part 3, Part 4, Part 5, Part 6), which lead to a change in the ISMS, are subject to authorisation by top management.

8.7 Establish information security objectives

8.7.1 **Time to Reply Ltd** has a documented procedure for setting information security objectives and developing plans to achieve them (ISMS DOC 6.2), including the identification of appropriate inputs.

8.7.2 A summary of the objectives and plans to achieve them is recorded in ISMS REC 6.2, and individual plans are recorded separately.

-
- **9Support**

9.1 Time to Reply Ltd has determined and provides the resources necessary for the establishment, implementation, maintenance and continual improvement of the ISMS.

9.2 Competence

9.2.1 Time to Reply Ltd identifies the necessary competencies and related procedures for procuring and developing these competencies, in accordance with MSS DOC 7.2.

9.2.2 The information security competence required for a given role within Time to Reply Ltd is recorded in the competence matrix (MSS REC 7.2) and included in the job description (example: MSS REC 7.2.1).

9.2.3 Time to Reply Ltd has developed a procedure to assess new/prospective employees for competence (MSS DOC 7.2.2).

9.2.4 Time to Reply Ltd has developed a procedure governing the provision of training for the purposes of the ISMS (MSS DOC 7.2.3).

9.2.5 Time to Reply Ltd retains evidence of acquired competence (MSS REC 7.2.3).

9.3 Awareness

9.3.1 Awareness of the Information Security Policy, how it relates to an individual's role, and the implications of non-conformance with the ISMS applies to all persons doing work under the organisation's control.

9.3.2 Internal communications relating to the ISMS are governed by the procedure detailed in MSS DOC 7.4.

9.3.3 Time to Reply Ltd's induction checklist (MSS REC 7.2.2) requires all new starters to be informed of the relevant information security policies and procedures.

9.3.4 Time to Reply Ltd describes other ISMS awareness programmes in MSS DOC 7.3.

9.3.5 Time to Reply Ltd describes procedures for promoting awareness in contractors and other non-staff working under Time to Reply Ltd's control in MSS DOC 7.3

9.4 Communication

Time to Reply Ltd's internal and external communications relating to the ISMS are governed by the procedure in MSS DOC 7.4.

9.5 Documented information

9.5.1 Time to Reply Ltd maintains documented information required by ISO 27001:2017, and documented information determined to be necessary for the effectiveness of the ISMS.

9.5.2 Time to Reply Ltd operates document control for all documents within the scope of the ISMS, as described in Protection & Control of ISMS Documentation MSS DOC 7.5.3.

• 10 Operation

This manual contains references to all of the policies and procedures that describe Time to Reply Ltd's ISMS, its risk assessment programme and its risk treatment programme. These policies and procedures are implemented, and records are retained to the extent necessary to ensure that the ISMS processes have been carried out. Operations are controlled in accordance with Operational Control (MSS DOC 8.1).

• 11 Performance evaluation

11.1 Monitoring, measurement, analysis and evaluation

11.1.1 Time to Reply Ltd monitors, measures, analyses and evaluates the performance of the ISMS, as described in MSS DOC 9.1.

11.1.2 This procedure covers all processes within the scope of the ISMS, including controls selected as part of the risk treatment.

11.1.3 This procedure is conducted at least [annually].

11.2 Internal audit

11.2.1 Time to Reply Ltd conducts internal audits of the ISMS, as described in MSS DOC 9.2.

11.2.2 The internal audit is conducted at least annually, in line with Time to Reply Ltd's defined audit schedule (MSS REC 9.2.1).

11.3 Management review

Time to Reply Ltd conducts management reviews of the ISMS, as described in MSS DOC 9.3.

This review is conducted at least annually, in accordance with the information security policy (ISMS DOC 5.2).

• 12 Improvement

As noted in 12.2 of this document, Time to Reply Ltd continually improves the ISMS.

12.1 Nonconformity and corrective action

12.1.1 Time to Reply Ltd seeks to correct errors and nonconformities within the ISMS following the procedure described in MSS DOC 10.1.

12.1.2 This procedure may be invoked at regular intervals in line with the results of the monitoring (MSS DOC 9.1), internal audit (MSS DOC 9.2) or management review (MSS DOC 9.3), or when a change occurs and a nonconformity is identified.

12.2 Continual improvement

12.2.1 Continual improvement of the ISMS is driven by the continual improvement procedure MSS DOC 10.2.

- **13**

- **Document Owner & Approval**

The Information Security Manager is the Owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of staff on the corporate intranet

This manual was approved by the Board of Directors on 24th October 2019 and is issued on a version-controlled basis under the signature of the Managing Director.

Signature: Date: 24/10/2019

Change History

Issue	Description of Changes	Issue Date
1	Initial Issue	24/10/2019

- **Annex A – Control Objectives and Controls**

- **Control A.6 Organisation of Information Security**

6.1 Internal Organisation

Control objective: establishment of a management framework for the initiation, implementation and operation of information security within the organisation.

6.1.1 Information security roles and responsibilities
Time to Reply Ltd has clearly defined and allocated all information security responsibilities.

6.1.1.1 Responsibilities for specific information security procedures are clearly defined throughout the ISMS and are documented in individual job descriptions.

6.1.1.2 The Director (CISO) is responsible for ensuring that Time to Reply Ltd has standard job descriptions for all roles, that contain defined security roles and responsibilities, and that these apply to all users of organisational information assets. Job descriptions are provided to all prospective users prior to their recruitment.

6.1.1.3 The Information Security Manager is responsible for ensuring that information security and IT staff have specific information security responsibilities and that these are detailed in their job descriptions.

6.1.1.4 The IT Manager is responsible for ensuring that all users sign User Agreements (see 9.2 below) before they are allowed to access Organisational information assets; these User Agreements contain specific information security responsibilities.

6.1.1.5 The Chief Information Security Officer (CISO (DIRECTOR)), who has lead responsibility in the management team for information security, is responsible for the development, implementation and maintenance of the ISMS.

6.1.1.6 The Information Security Manager is also the Chief Information Security Officer (CISO (DIRECTOR)).

6.1.1.7 The Information Security Manager's responsibilities are documented in his/her job description and include the day-to-day responsibility for the implementation, co-ordination and maintenance of the ISMS.

6.1.1.8 All staff (and certain third-party contractors) have accepted their specific responsibilities in the User Agreements which they sign before they are authorised to access organisational information assets.

6.1.1.9 All information assets including those within composite information systems have been identified (see 8.1.1 below) and the security processes associated with each asset have been defined following a risk assessment (see section 6 above) and documented on the asset inventory schedules (see Control A.8 below).

6.1.1.10 All assets have identified Owners (see 8.1.2 below) whose responsibility for the day-to-day maintenance of the controls applied to their asset is documented in their job descriptions and elsewhere through the ISMS.

6.1.1.11 All risks have identified Owners (identified during the risk assessment in section 6 above) whose responsibility for the acceptance of the treatment of their risk and any residual risk is documented in their job descriptions and risk treatment plan (see section 6 above).

6.1.1.12 Each site has an identified individual the Site Manager who is responsible for co-ordinating information security activities or carrying out specific processes within that site, or facility, in line with the Manual and applicable procedures. The authority of these individuals is documented in their job descriptions. The Information Security Manager maintains a list of the responsible Site Manager's.

6.1.1.13 Other responsibilities are identified as necessary throughout the ISMS.

6.1.1.14 Authorisation levels are clearly defined and documented (see manual section 2.2) and enforce segregation of duties (see Control A.6, 6.1.2).

6.1.2 Segregation of duties

Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of organisational assets.

6.1.2.1 As far as is practicable and possible, Time to Reply Ltd segregates duties and areas of responsibility. In particular, the following functions are segregated:

Risk assessment	Director
Authorisation of controls	Director
Change initiation	Department Managers
Change Management	Director
Network Management	Department Managers
Network Administration	Department Managers
IT Operations	Department Managers
Software development	Department Managers
System testing	Department Managers
Employee Administration	Department Managers
Asset Purchase	Director
Site/Secure Area security	Director
Security Audit	Director

6.1.2.2 Segregation of duties is built into procedures, including the requirement that that the Owner of a procedure or process cannot authorise its modification, withdrawal or release.

6.1.2.3 Activity monitoring, audit trails and management supervision are used to support duty segregation.

6.1.3 Contact with authorities

Time to Reply Ltd maintains appropriate contacts with relevant authorities.

6.1.3.1 The Information Security Manager is responsible for identifying (ISMS-C DOC 6.1.3) those authorities with whom Time to Reply Ltd needs to maintain contacts, to support information security incident management (Control A.16 below), business continuity management (Control A.17 below), and continuous improvement.

6.1.4 Contact with special interest groups

Time to Reply Ltd maintains appropriate contact with special interest groups and other specialist security forums and professional associations.

6.1.4.1 The Information Security Manager is responsible, on behalf of Time to Reply Ltd, for identifying and joining those forums and special interest groups which s/he considers will enable him/her to effectively meet the responsibilities contained in his/her job description.

6.1.4.2 The Information Security Manager is required to ensure Time to Reply Ltd has up-to-date information security knowledge, including about the changing malware threat environment.
Time to Reply Ltd's Information Security Incident Management procedure see Control A.16 below) requires Information Security Manager to have suitable liaison for dealing with incidents.

6.1.5 Information security in project management
Information security is addressed in project management, regardless of the type or nature of project.

6.1.5.1 The project management methodology is PRINCE-II

6.1.5.2 The Information Security Manager, in conjunction with the Project Manager is required to ensure that information security objectives are included in project objectives.

6.1.5.3 The project is subject to an information security risk assessment at the initiation of the project, in order to identify necessary controls.

6.2 Mobile devices and teleworking

Control objective: to ensure the security of teleworking and use of mobile devices

6.2.1 Mobile device policy
A formal policy (clause 6.2.1.2 below) is in place and appropriate security measures have been adopted to manage the risks introduced by using mobile devices.

6.2.1.1 Time to Reply Ltd's mobile computing policy below covers notebook computers, palmtops, (PDAs), laptops, tablets, smart phones and mobile phones.

6.2.1.2 Time to Reply Ltd provides mobile computing facilities in order to improve the productivity, flexibility, responsiveness and effectiveness of its operations. Time to Reply Ltd also takes appropriate steps for physical protection (User Agreement ISMS-C DOC 9.2.1a), access controls, cryptography, backups and malware protection for mobile devices and also ensures that users receive appropriate training before they are issued with mobile devices. Users are required to accept in writing (ISMS-C DOC 9.2.3b and 9.2.3c) specific responsibilities with regard to backups, malware protection and their use of mobile devices, particularly with regard to working in unprotected environments.

6.2.2 Teleworking
A formal policy is in place (clause 6.2.2.1 below) and appropriate supporting security measures have been adopted to protect information accessed, processed or stored at teleworking sites.

6.2.2.1 Time to Reply Ltd's policy on teleworking is that it provides teleworking facilities in order to improve the productivity, flexibility, responsiveness and effectiveness of its operations. Time to Reply Ltd's policy is to authorise and control teleworking facilities, as set out in ISMS-C DOC 6.2.2, to ensure that information is secure. It carries out a risk assessment (RM-ISMS DOC 6.1.2) to ensure that each teleworking site is secure (ensures that there is adequate equipment and connectivity) physical and logical protection, access controls, cryptography, backups and malware protection for equipment installed in teleworking locations and will also ensure that teleworkers receive appropriate training before they are allowed to commence working. Teleworkers are required to accept in writing (ISMS-C DOC 6.2.2a) specific responsibilities with regard to teleworking activity, including physical protection, backups, malware protection and their use of Time to Reply Ltd's equipment, particularly with regard to allowing unauthorised access by third parties.

- **Control A.7 Human Resource Security**

7.1 Prior to employment

Control objective: to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1 Screening
Background verification checks on all candidates for employment and contractors are carried out in line with ISMS-C DOC 7.1.1 and in accordance with the laws, regulations and ethics of the United Kingdom, and proportional to Time to Reply Ltd's business requirements, the classification of the information to be accessed, and the perceived risks.

7.1.2 Terms and conditions of employment
Employees and contractors must agree and sign the terms and conditions of their employment contract, which state their and Time to Reply Ltd's responsibility for information security.

7.2 During employment

Control objective: to ensure that employees and contractors are aware of and fulfil their information security responsibilities.

7.2.1 Management responsibilities
Management requires employees and contractors to apply security in accordance with the policies and procedures of Time to Reply Ltd's ISMS.

7.2.1.1 Management ensures that employees, contractors and third parties are appropriately briefed prior to being granted access to organisational information assets (see clause 7.2.2 below).

7.2.1.2 Management ensures that employees, contractors and third parties receive guidelines on security expectations (User Agreement, job descriptions and terms and conditions of employment).

7.2.1.3 Management provides personal leadership and example in information security and ensures that Time to Reply Ltd's policies and procedures are followed (see clause 18.2.1 below).

7.2.2 Information security awareness, education and training
All employees of Time to Reply Ltd and, where relevant, contractors receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function.

7.2.2.1 The Director (CISO) is responsible for ensuring that all users receive standard information security induction and awareness training before they are allowed to access organisational information assets. This is conducted on the basis of a training needs analysis and includes the incident reporting procedure.

7.2.2.2 The Information Security Manager is responsible for ensuring that all users receive regular updates and alerts on information security issues as and when necessary, and that additional security-related training is made available as and when required.

7.2.2.3 The Information Security Manager is responsible for ensuring that specialised information security staff receive appropriate specialist training in line with their job requirements.

7.2.3 Disciplinary process
Time to Reply Ltd has a formal and communicated disciplinary process for employees who have committed an information security breach.

7.2.3.1 Breaches of Time to Reply Ltd's ISMS may be treated as misconduct in terms of Time to Reply Ltd's disciplinary policy (which is set out in in the Employee Handbook and Company Procedures, which are available on the intranet) and serious breaches may lead to dismissal.

7.3 Termination and change of employment

Control objective: to protect the organisation's interests as part of the process of changing or terminating employment

7.3.1 Termination or change of employment responsibilities
Information security responsibilities and duties that remain valid after termination or change of employment are defined, communicated to the employee or contractor, and enforced.

7.3.1.1 Upon termination or change of employment, complete a termination checklist (ISMS-C REC 7.3.1)

- **Control A.8 Asset Management**

8.1 Responsibility for assets
Control objective: to identify organisational assets and define appropriate protection responsibilities

8.1.1 Inventory of assets
Assets associated with information and information processing facilities are identified and inventoried, and the inventory is maintained in line with the requirements of ISMS-C DOC 8.1.1.

8.1.2 Ownership of assets
All assets identified (clause 8.1.1 above) are 'owned' by a designated individual or part of Time to Reply Ltd, and details of the Owner are identified on the asset inventory in line with ISMS-C DOC 8.1.1.

8.1.3 Acceptable use of assets
Rules for the acceptable use of information and assets associated with information and information processing facilities have been identified, documented and implemented.

8.1.3.1 The IT Manager is responsible for ensuring that all users sign User Agreements (see section 9.2 below), which set out requirements for acceptable use of information assets and in which they also explicitly accept Time to Reply Ltd's Internet Acceptable Use Policy (ISMS-C DOC 8.1.3).

8.1.3.2 These User Agreements (see section 9.2 below) also explicitly accept Time to Reply Ltd's Rules for Use of E-mail (ISMS-C DOC 8.1.3a).

8.1.3.3 The Information Security Manager is responsible for monitoring compliance.

8.1.3.4 Guidelines for the use of mobile devices are included in the 'mobile on the road' annex to the User Agreement (see Control A.9 below and Control A.6 above) for users issued with such devices.

8.1.4 Return of assets
All employees and contractors are required to return all organisational assets in their possession upon termination of their employment, contract or agreement.

8.1.4.1 Upon termination of employment, complete a termination checklist (ISMS-C REC 7.3.1) to confirm that assets have been returned.

8.2 Information classification
Control objective: to ensure that information receives an appropriate level of protection in accordance with its importance to the organisation

8.2.1 Classification of information
Information has been classified in terms of value, legal requirements, criticality and sensitivity to unauthorised disclosure or modification.

8.2.1.1 Time to Reply Ltd has developed guidelines for information classification, which are suited to business needs (including legality, value, criticality and sensitivity) to both restrict and share information, and to the business impacts associated with those needs, and these are contained in ISMS-C DOC 8.2.

8.2.2 Labelling of information

An appropriate set of procedures for information labelling has been developed and implemented in accordance with the classification scheme adopted by Time to Reply Ltd and this is set out in ISMS-C DOC 8.2.

8.2.3 Handling of assets

Procedures for handling assets have been developed and implemented in accordance with the information classification scheme adopted by Time to Reply Ltd, and this is set out in ISMS-C DOC 8.2.

8.3 Media handling

Control objective: to prevent unauthorised disclosure, modification, removal or destruction of information stored on media.

8.3.1 Management of removable media

Procedure ISMS-C DOC 8.3 identifies the controls for the management of removable media in accordance with the information classification scheme laid out in ISMS-C DOC 8.2.

8.3.2 Disposal of media

Media are disposed of securely and safely when no longer required, in line with ISMS-C DOC 11.2.7.

8.3.3 Physical media transfer

ISMS-C DOC 11.2.5 sets out how Time to Reply Ltd ensures that media are protected against unauthorised access, misuse or corruption during transportation.

- **Control A.9 Access Control**

9.1 Business requirements of access control
Control objective: to limit access to information processing facilities

9.1.1 Access control policy
An access control policy has been established, documented in ISMS-C DOC 9.1.1, and is reviewed when required in the light of business and information security needs.

9.1.2 Access to networks and network services
Time to Reply Ltd's policy (in ISMS-C DOC 13.1.3) is that users are only provided with access to the network and network services that they have been specifically authorised to use.

9.2 User access management
Control objective: to ensure authorised user access and to prevent unauthorised access to systems and services

9.2.1 User registration and de-registration
There is a formal user registration and de-registration procedure (ISMS-C DOC 9.2.3 and ISMS-C DOC 9.2.1a) governing assignment of access rights.

9.2.2 User access provisioning
A formal user access provisioning procedure (ISMS-C DOC 9.2.3) has been implemented to assign or revoke access rights for all user types to all systems and services.

9.2.3 Management of privileged access rights
The allocation and use of privileged access rights is restricted and controlled through a formal management process as set out in ISMS-C DOC 9.2.3.

9.2.4 Management of secret authentication information of users
The allocation of secret authentication information is controlled through a formal management process as set out in ISMS-C DOC 9.2.3.

9.2.5 Review of user access rights
Asset owners review users' access rights at regular intervals using the formal process as set out in ISMS-C DOC 9.2.3.

9.2.6 Removal or adjustment of access rights
The access rights of all employees and contractors to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.

9.2.6.1 Upon termination or change of employment, complete a termination checklist (ISMS-C REC 7.3.1) to confirm that all access rights have been removed or adjusted.

9.3 User responsibilities
Control objective: to make users accountable for safeguarding their authentication information

9.3.1 Use of secret authentication information
Users are required (in their User Agreements ISMS-C DOC 9.2.1a) to follow the organisation's practices in use of secret authentication information.

9.4 System and application access control
Control objective: to prevent unauthorised access to systems and applications

9.4.1 Information access restriction

Access to information and application system functions by users and support personnel is restricted in ISMS-C DOC 9.1.2 in accordance with the access control policy in ISMS-C DOC 9.1.1.

9.4.2 Secure log-on procedures

Where required by the Access Control Policy in ISMS-C DOC 9.1.1, access to systems and applications is controlled by the secure log-on procedure set out in ISMS-C DOC 9.4.2.

9.4.3 Password management system

The interactive password management system set out in ISMS-C DOC 9.2.3 ensures quality passwords.

9.4.4 Use of privileged utility programs

The use of utility programs that might be capable of overriding system and application controls is restricted and controlled as specified in ISMS-C DOC 9.4.4.

9.4.5 Access control to program source code

Access to program source code is restricted in line with ISMS-C DOC 8.3.

- **Control A.10 Cryptography**

10.1 Cryptographic controls

Control objective: to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.1.1 Policy on the use of cryptographic controls

Time to Reply Ltd has a policy on its use of cryptographic controls for protection of its information, as set out in clause 10.1.1.1 below.

10.1.1.1 Time to Reply Ltd applies cryptographic controls where required by a risk assessment to secure its confidential communications and information carried beyond its secure logical perimeter, to secure connections from beyond its logical perimeter, and to secure its online business (as required in ISMS-C DOC 14.1.2).

The Information Security Manager is responsible for maintaining ISMS-C REC 10.1.1, which sets out, for each situation in which cryptographic controls are required under this policy, the type and length of the encryption algorithm required, and identifies the precise instructions required to use that cryptographic control.

S/he is responsible for key management and key generation as set out in ISMS-C DOC 10.1.2. Each asset Owner, whose information asset falls within the scope of this policy, is responsible for ensuring that the required cryptographic control is applied. The IT Manager is responsible for configuration of devices as required by this policy.

10.1.2 Key management

Time to Reply Ltd has a policy on the use, protection and lifetime of cryptographic keys, as documented in ISMS-C DOC 10.1.2, which supports Time to Reply Ltd s use of cryptographic techniques.

- **Control A.11 Physical and Environmental Security**[1]

11 Secure areas

Control objective: to prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities

11.1.1 Physical security perimeter
Time to Reply Ltd uses security perimeters to protect areas that contain sensitive or critical information and information processing facilities.

11.1.1.1 Time to Reply Ltd's sites have physical security perimeters. The minimum specification checklist for the physical security perimeter is in ISMS-C DOC 11.1.11 and the Premises Security Manager ensures that each site is checked on a regular basis.

11.1.1.2 The Site Manager of each Organisational site is responsible for maintaining that site's secure perimeter.

11.1.1.3 Time to Reply Ltd's central information processing facilities are within secure areas server room/communications room or data centre, each of which have Owners (see Control A.8 above) that are themselves within a site's secure perimeter.

11.1.1.4 The Information Security Manager has a site map for each site or secure area, together with a current security checklist ISMS-C DOC 11.1.11 that identifies the current state of conformity to the requirements in that checklist.

11.1.2 Physical entry controls
Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

11.1.2.1 A risk assessment (see section 6 above) is used to determine the type of entry controls that might be required for secure areas and these are implemented in line with the requirements of ISMS-C DOC 11.1.2d and ISMS-C DOC 11.1.2.

11.1.2.2 The Site Manager are responsible for maintaining required physical entry controls.

11.1.3 Securing offices, rooms and facilities
Time to Reply Ltd has designed and applied physical security for offices, rooms and facilities.

11.1.3.1 Time to Reply Ltd conducts risk assessments in line with RM-ISMS DOC 6.1.2 of individual offices, rooms and facilities that contain confidential or high risk information assets to identify the controls that might be necessary to secure them. These are implemented in line with ISMS-C DOC 11.1.11. There are no sites where confidential information processing facilities are shared with a third-party organisation, other than under the terms of a contract (see clause 15.1.2 below).

11.1.4 Protecting against external and environmental threats
Time to Reply Ltd has designed and applied physical protection against damage from natural disasters, malicious attack or accidents.

11.1.4.1 Time to Reply Ltd has assessed the risk of external and environmental threats and has applied controls that are included in ISMS-C DOC 11.1.11 or that are part of the Business Continuity Management framework (see Control A.17).

11.1.5 Working in secure areas

[1]

Time to Reply Ltd has designed and applied procedures for working in secure areas and these are contained in ISMS-C DOC 11.1.2.

11.1.6 Delivery and loading areas

Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises are controlled and isolated from information processing facilities to avoid unauthorised access.

11.1.6.1 Time to Reply Ltd's controls for delivery and loading areas are detailed in ISMS-C DOC 11.1.6.

11.2 Equipment

Control objective: to prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations

11.2.1 Equipment siting and protection

Equipment is sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

11.2.1.1 The Site Manager is responsible for implementing the requirements of ISMS-C DOC 11.2.1, which include this control.

11.2.2 Supporting utilities

Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.

11.2.2.1 The Site Manager is responsible for implementing the requirements of ISMS-C DOC 11.2.1, which include this control.

11.2.3 Cabling security

Power and telecommunications cabling carrying data or supporting information services is protected from interception, interference or damage.

11.2.3.1 The Site Manager is responsible for implementing the requirements of ISMS-C DOC 11.2.1, which include this control.

11.2.4 Equipment maintenance

Equipment is correctly maintained to ensure its continued availability and integrity.

11.2.4.1 The Site Manager is responsible for implementing the requirements of ISMS-C DOC 11.2.1, which include this control.

11.2.5 Removal of assets

Equipment, information or software may not be taken off-site without prior authorisation as required by ISMS-C DOC 11.2.5.

11.2.6 Security of equipment and assets off-premises

Security is applied to off-site equipment and assets taking into account the different risks of working outside Time to Reply Ltd's premises.

11.2.6.1 Users of mobile equipment are required, as part of their User Agreements (see Control A.9 above), to provide appropriate physical security for equipment when off-site and to ensure that manufacturer's instructions for protecting equipment are followed.

11.2.6.2 Home working is subject to specific controls, in line with control clause 6.2.2 above.

11.2.6.3 The Managing Director is responsible for ensuring that the Organisation's insurance specifically provides cover against loss of or damage to mobile devices off-site.

11.2.7 Secure disposal or re-use of equipment

All items of equipment containing storage media are checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

11.2.8 Unattended user equipment

Users are required to ensure that any unattended equipment is appropriately protected.

11.2.9 Clear desk and clear screen policy

Time to Reply Ltd has adopted a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities, and the requirement for compliance with this policy is set out in ISMS-C DOC 9.2.1a.

1.8

- **Control A.12 Operations Security**

12.1 Operational procedures and responsibilities

Control objective: to ensure correct and secure operation of information processing facilities

12.1.1 Documented operating procedures
Operating procedures have been documented, are maintained and are made available to all users who need them.

12.1.1.1 The IT Manager is responsible for documenting all the IT working procedures for system activities related to information processing and communications facilities. The procedures required by Time to Reply Ltd are listed in ISMS-C DOC 12.1.1.

12.1.2 Change management
Changes to Time to Reply Ltd, business processes, information processing facilities and systems that affect information security are controlled.

12.1.2.1 The Director (CISO) is responsible for ensuring that all requests for significant non-routine changes to organisational information processing facilities are managed in line with ISMS-C DOC 12.1.2 and control clause 14.2 below is also relevant.

12.1.3 Capacity management
ISMS-C DOC 12.1.3 sets out Time to Reply Ltd's approach to ensuring that the use of resources is monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

12.1.4 Separation of development, test and operational environments
Development, testing and operational environments are separated to reduce the risks of unauthorised access or changes to the operational environment.

12.1.4.1 Time to Reply Ltd's requirements for separate development, test and operational facilities, and its rules for their use and for the transfer of software to the operational environment are documented in ISMS-C DOC 12.1.4.

12.2 Protection from malware

Control objective: to ensure that information and information processing facilities are protected against malware.

12.2.1 Controls against malware

Detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures have been implemented, and user awareness programmes incorporate this.

12.3 Backup

Control Objective: to protect against loss of data

12.3.1 Information backup

Back-up copies of information, software and system images are taken and tested regularly in accordance with the agreed back-up policy below.

12.3.1.1 Time to Reply Ltd's policy is that it acts to maintain the integrity and availability of information and information processing facilities by establishing criteria and routine procedures (in ISMS-C DOC 12.1.3) to ensure that all Time to Reply Ltd's information assets are backed up and that there are tested procedures (see Control A.17 below) for restoring them within an adequate time frame.

12.4 Logging and monitoring

Control objective: to record events and generate evidence.

12.4.1 Event Logging

Event logs recording user activities, exceptions, faults and information security events are produced and kept, in line with ISMS-C DOC 12.4.1, for a period specified in ISMS-C DOC 18.1.3a, and regularly reviewed to assist in future investigations and access control monitoring.

12.4.2 Protection of log information

Logging facilities and log information are protected against tampering and unauthorised access, as required by ISMS-C DOC 12.4.1.

12.4.3 Administrator and operator logs

System administrator and system operator activities are logged and the logs are protected, as required by ISMS-C DOC 12.4.1.

12.4.4 Clock synchronisation

The clocks of all relevant information processing systems within Time to Reply Ltd are synchronised to a single reference time source, as specified in ISMS-C DOC 12.4.1.

12.5 Control of operational software

Control objective: to ensure the integrity of operational systems.

12.5.1 Installation of software on operational systems

The installation of software on operational systems is controlled by ISMS-C DOC 12.1.1a.

12.6 Technical vulnerability management

Control objective: to prevent exploitation of technical vulnerabilities

12.6.1 Management of technical vulnerabilities

Timely information about technical vulnerabilities of information systems used by Time to Reply Ltd is obtained, Time to Reply Ltd's exposure to those vulnerabilities evaluated, and ISMS-C DOC 12.6.1 sets out the measures taken to address the associated risks.

12.6.2 Restrictions on software installation

Rules have been established governing the installation of software by users, as described below.

12.6.2.1 Time to Reply Ltd only uses externally evaluated and certificated products apart from those developed for customer use.

12.6.2.2 Installation and updating third party commercial software is described in ISMS-C DOC 12.5.1.

12.6.2.3 Malware, that might cause covert channels, is controlled through the anti-malware software (see control clause 12.2 above) and User Agreements (see control clauses 9.2 and 9.3 above).

12.7 Information systems audit considerations

Control objective: to minimise the impact of audit activities on operational systems.

12.7.1 Information systems audit controls

Audit requirements and activities involving checks on operational systems are carefully planned as set out in ISMS-C DOC 12.7.1 and agreed with appropriate management to minimize the risk of disruptions to business processes.

- **Control A.13 Communications Security**

13.1 Network security management

Control objective: to ensure the protection of information in networks and its supporting information processing facilities

13.1.1 Network controls

Networks are managed and controlled as set out in ISMS-C DOC 13.1.1, in order to protect information in systems and applications.

13.1.2 Security of network services

Security mechanisms, service levels and management requirements of all network services have been identified and included in *[any/the]* network services agreements, whether those services are provided in-house or outsourced and are managed in line with ISMS-C DOC 13.1.1

13.1.3 Segregation in networks

Groups of information services, users and information systems are segregated on the network(s) in line with the requirements of ISMS-C DOC 13.1.3 and ISMS-C DOC 13.1.3a.

13.2 Information transfer

Control objective: to maintain the security of information transferred within the organisation and with any external entities.

13.2.1 Information transfer policies and procedures

Formal transfer policies, procedures and controls are in place to protect the transfer of information through the use of all types of communication facilities.

13.2.1.1 Time to Reply Ltd's Internet Acceptable Use Policy (ISMS-C DOC 8.1.3), its e-mail usage rules (ISMS-C DOC 8.1.3a), its information classification procedures (ISMS-C DOC 8.2), its anti-malware policy (ISMS-C DOC 12.2.1) and related procedures, and the technological controls implemented as required in all those procedures, protect exchanges of information from interception, unauthorised copying, modification, destruction or misrouting.

13.2.1.2 The wireless user's addendum to the standard User Agreement (see Control A.9, 9.1) sets out how wireless communication is protected.

13.2.1.3 The mobile phone user's addendum to the standard User Agreement (see Control A9, 9.1) sets out how mobile voice communication is protected.

13.2.1.4 Time to Reply Ltd has a procedure (ISMS-C DOC 13.2.1) for secure voice communication at all its sites.

13.2.1.5 Time to Reply Ltd's use of cryptographic techniques is controlled under Control A.10, 10.1 above.

13.2.1.6 Time to Reply Ltd has procedures for handling (ISMS-C DOC 8.3), retention (ISMS-C DOC 18.1.3a) and disposal (ISMS-C DOC 11.2.7) of information and related media.

13.2.2 Agreements on information transfer

Agreements are established in line with ISMS-C DOC 8.2 for the transfer of information, and address the secure transfer of business information between Time to Reply Ltd and external parties.

13.2.3 Electronic messaging

Information involved in electronic messaging is appropriately protected.

13.2.3.1 ISMS-C DOC 8.1.3a sets out Time to Reply Ltd's rules on e-mail usage, and ISMS-C DOC 8.2 sets out security requirements related to information

classification, encryption and digital signatures and users are trained on correct use of e-mail, including the requirement to verify that e-mail addresses are correct prior to despatch.

13.2.3.2 The IT Manager is responsible for ensuring that Time to Reply Ltd's e-mail system is set up and configured in line with *Operations Work Instruction ISMS-C-DOC 8.1.3b,* which was drawn up to document the controls identified in the e-mail risk assessment.

13.2.3.3 The IT Manager is responsible for Time to Reply Ltd's web mail service and for its protection by a firewall configured according to Operations Work Instruction ISMS-C-DOC 8.1.3b and for ensuring that it is only accessible to authorised and authenticated users by means of a secure connection, the configuration of which is in line with Operations Work Instruction DOC [ ].

13.2.3.4 The Operations Director is responsible for business continuity plans in respect of the e-mail systems, (see Control A.17 below).

13.2.3.5 Instant messaging systems are part of the secure deployment of Google G-Suite and are used by all staff.

13.2.4 Confidentiality or non-disclosure agreements

A confidentiality and non-disclosure agreement (ISMS-C DOC 13.2.4) reflecting Time to Reply Ltd's requirements for the handling of information is in place (also see control clause 7.1.2 above) and is reviewed regularly

- **Control A.14 System Acquisition, Development and Maintenance**

14.1 Security requirements of information systems

Control objective: to ensure that information security is an integral part of information systems across the entire lifecycle. This includes the requirements for information systems which provide services over public networks.

14.1.1 Security requirements analysis and specification
Statements of information security requirements are included in the requirements for new information systems, or enhancements to existing information systems.

14.1.1.1 Time to Reply Ltd carries out a risk assessment (in line with RM-ISMS DOC 6.1.2, and see section 6 above) at the requirements stage of specifying any new information systems, or enhancements to existing systems (irrespective of whether they will be bespoke systems or commercial off the shelf systems). Required controls are identified and the IT Manager is responsible for ensuring that these controls are integrated into the purchase decision, specification and purchase contract. The Information Security Manager is responsible for ensuring that required manual controls are designed and implemented.

14.1.1.2 Application controls that ensure correct processing are also (where appropriate) considered at the design stage.

14.1.1.3 Software is subject to testing and formal approval in line with ISMS-C DOC 12.1.3; non-compliant products are not accepted.

14.1.1.4 Time to Reply Ltd accepts products tested and evaluated in line with international standards without requiring further testing.

14.1.2 Securing application services on public networks
Information involved in application services passing over public networks is protected from fraudulent activity, contract dispute and unauthorised disclosure and modification, as set out in ISMS-C DOC 14.1.2.

14.1.3 Protecting application services transactions
Information involved in application service transactions is protected in line with ISMS-C DOC 14.1.2 to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

14.2 Security in development and support processes

Control objective: to ensure that information security is designed and implemented within the development lifecycle of information systems.

14.2.1 Secure development policy
Rules for the development of software and systems have been established and documented in ISMS-C DOC 14.2.1, and must be applied to developments within the organisation and contracted development by third parties.

14.2.2 System change control procedures
Changes to systems within the development lifecycle are controlled by the use of the formal change control procedures set out in ISMS-C DOC 12.1.2

14.2.3 Technical review of applications after operating platform changes

When operating platforms are changed, business critical applications are reviewed and tested in line with ISMS-C DOC 12.1.3 to ensure there is no adverse impact on organisational operations or security.

14.2.4 Restrictions on changes to software packages
Time to Reply Ltd does not seek bespoke modifications to commercial software packages

14.2.5 Secure system engineering principles
Principles for engineering secure systems have been established in ISMS-C DOC 14.2.1a, and are to be applied to any information system implementations

14.2.6 Secure development environment
Time to Reply Ltd's has established a procedure for appropriately protected secure development environments for system development and integration efforts that cover the entire system development lifecycle, and this is recorded in ISMS-C DOC 14.2.1a.

14.2.7 Outsourced software development
Time to Reply Ltd does not outsource software development

14.2.8 System security testing
Security functionality is tested during development, as described in ISMS-C DOC 14.2.1a

14.2.9 System acceptance
Acceptance criteria for new information systems, upgrades and new versions have been established and suitable tests of the system(s) are carried out during development and prior to acceptance, all as specified in ISMS-C DOC 12.1.3.

14.3 Test Data
Control objective: to ensure the protection of data used for testing.

14.3.1 Protection of test data
Test data is selected carefully, protected and controlled in line with ISMS-C DOC 12.1.3.

- **Control A.15 Supplier Relationships**

15.1 Information security in supplier relationships

Control objective: to ensure protection of the organisation's assets that are accessible by suppliers.

15.1.1 Information security policy for supplier relationships

Time to Reply Ltd agrees information security requirements with suppliers for mitigating the risks associated with access to Time to Reply Ltd's information assets.

15.1.1.1 Time to Reply Ltd has a defined policy (ISMS-C DOC 15.1.1) governing information security in supplier relationships.

15.1.1.2 Time to Reply Ltd has a defined process (ISMS-C DOC 15.1.2) for managing third party service contracts.

15.1.2 Addressing security in third party agreements

Agreements with suppliers account for information security involving suppliers accessing, processing, storing, communicating or providing IT infrastructure components, as required in ISMS-C DOC 15.2.2, and suppliers are not allowed to access Time to Reply Ltd's information assets until such an agreement has been signed.

15.1.2.1 Where a supplier has a standard agreement and no provision to vary it to meet a client's requirement, the supplier's standard clauses are assessed against Time to Reply Ltd's requirements and the risk associated with the gap is assessed before deciding whether or not to proceed with the offered terms. Where there is a significant variation between the requirements and what is offered, the Managing Director's approval to proceed with the provider is required.

15.1.3 Information and communication technology supply chain

Agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain.

15.2 Supplier service delivery management

Control objective: to maintain an agreed level of information security and service delivery in line with supplier agreements.

15.2.1 Monitoring and review of supplier services

Time to Reply Ltd regularly monitors, reviews and audits supplier service delivery, in line with ISMS-C DOC 15.1.2

15.2.2 Managing changes to supplier services

Time to Reply Ltd manages changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, taking account of the criticality of business information systems and processes involved and re-assessment of risks, and the procedures for doing this are contained in ISMS-C DOC 15.2.2

- **Control A.16 Information Security Incident Management**

16.1 Management of information security incidents and improvements

Control objective: to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.2 Responsibilities and procedures

Management responsibilities and procedures have been established in ISMS-C DOC 16.1.5 to ensure a quick, effective and orderly response to information security incidents that ensures appropriate corrective or preventative actions, restores normal operations as quickly as possible, and ensures that improvement opportunities are identified and acted upon.

16.2.1 Reporting information security events

Information security events must be reported to the Information Security Manager as quickly as possible, as set out in ISMS-C DOC 16.1.2-3

16.2.2 Reporting information security weaknesses

All employees and contractors using information systems and services are required by ISMS-C DOC 16.1.2-3 to note and report to the Information Security Manager any observed or suspected weaknesses in systems or services

16.2.3 Assessment of and decision on information security events

Information security events are assessed in order to determine whether they are classified as information security incidents, in line with the procedure described in ISMS-C DOC 16.1.5

16.2.4 Response to information security incidents

16.2.5 Information security incidents are responded to in accordance with ISMS-C DOC 16.1.5

16.2.6 Learning from information security incidents

Knowledge gained from analysing and resolving information security incidents is to be used to reduce the likelihood or impact of future incidents, as described in ISMS-C DOC 16.1.5

16.2.7 Collection of evidence

In all information security incidents, irrespective of whether or not a follow-up action against a person or organisation involves legal action (either civil or criminal), evidence is collected, retained and presented as set out in ISMS-C REC 16.1.2-3a to conform to the rules for evidence laid down in the data Protection Act 2018

- **Control A.17 Information Security Aspects of Business Continuity Management**

17.1 Information security continuity

Control objective: information security continuity is embedded in the organisation's business continuity management systems.

17.1.1 Planning information security continuity
Time to Reply Ltd has determined its requirements for information security and the continuity of information security management in adverse situations, a described in the single framework (as described in ISMS-C DOC 17.1.1).

17.1.2 Implementing information security continuity
Time to Reply Ltd has established and implemented processes, procedures and controls to ensure the required level of continuity for information security during adverse situations, as described in ISMS-C DOC 17.1.2.

17.1.3 Verify, review and evaluate information security continuity
Time to Reply Ltd verifies the established and implemented information security controls at regular intervals (as described in ISMS-C DOC 17.1.3) in order to ensure that they are effective during adverse situations.

17.2 Redundancies

Control objective: to ensure availability of information processing facilities

17.2.1 Availability of information processing facilities
Information processing facilities are implemented with redundancy sufficient to meet availability requirements, as described in ISMS-C DOC 17.1.1a.

- **Control A.18 Compliance**

18.1 Compliance with legal and contractual requirements

Control objective: to avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1 Identification of applicable legislation and contractual requirements

All relevant legislative, statutory, regulatory and contractual requirements and Time to Reply Ltd's approach to meet these requirements have been explicitly defined, documented and are kept up to date for each information system and Time to Reply Ltd.

18.1.1.1 All legislative, contractual, statutory and regulatory requirements that apply to Time to Reply Ltd and to its information assets are identified by the Chief Information Security Officer in a compliance database.

18.1.1.2 The Managing Director is responsible for creating and maintaining the database (ISMS-C DOC 18.1.2a) of Time to Reply Ltd's statutory and regulatory information/data and computer-related compliance requirements. The controls and responsibilities necessary to meet these compliance requirements are also identified in this schedule.

18.1.2 Intellectual property rights

Appropriate procedures have been implemented to ensure compliance with legislative, regulatory and contractual requirements relating to intellectual property rights and on the use of proprietary software products.

18.1.2.1 Time to Reply Ltd has adopted a policy on intellectual property rights compliance which is set out in ISMS-C DOC 18.1.2A. This policy is prominently displayed near all digital copying equipment and elsewhere, as appropriate.

18.1.2.2 Time to Reply Ltd's procedures to implement this policy are contained in ISMS-C DOC 18.1.2b.

18.1.3 Protection of records

The organisation operates record control for all records generated within the scope of the ISMS, as described in ISMS-C DOC 18.1.3.

Time to Reply Ltd's procedure, set out in ISMS-C DOC 18.1.3a, protects records from loss, destruction, falsification and unauthorised access, in accordance with legislatory, regulatory, contractual and business requirements.

18.1.4 Privacy and protection of personally identifiable information

Time to Reply Ltd ensures the privacy and protection of personally identifiable information as required in relevant legislation and regulation.

18.1.4.1 Time to Reply Ltd's Data Protection and Privacy policy is set out in ISMS-C DOC 18.1.4.

18.1.4.2 Time to Reply Ltd has appointed a Data Protection Officer who is responsible for ensuring that the procedures set out in ISMS-C DOC 18.X are implemented.

18.1.4.3 Time to Reply Ltd has implemented specific technical measures to protect personal information.

18.1.5 Regulation of cryptographic controls

Cryptographic controls are used in compliance with all relevant agreements, legislation and regulations, as set out in ISMS-C DOC 10.1.2.

18.2 Information security reviews

Control objective: to ensure that information security is implemented and operated in accordance with the organisational policies and procedures.

18.2.1 Independent review of information security
Time to Reply Ltd's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) is independently reviewed at planned intervals, and when significant changes to the security implementation occur.

18.2.1.1 The Director (CISO) is responsible for organizing independent audits of the ISMS. Where necessary, the Director (CISO), in conjunction with the Information Security Manager engages expert (technical) external assistance. The audit procedures are contained in ISMS-C DOC 8.1.3c and Control A.12, 12.7 of this Manual is also applicable.

18.2.1.2 The ISMS is also subject to periodic reviews by external compliance auditors.

18.2.1.3 Risk assessments are reviewed annually to ensure that they are still complete and up to date.

18.2.2 Compliance with security policies and standards
Department Managers regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

18.2.2.1 Department Managers are required, under their job descriptions, to carry out monthly checks to ensure that all security procedures and work instructions within their area of responsibility are being carried out, to identify shortfalls and to take action to ensure that shortfalls are immediately corrected. This action should involve identification of the causes of the non-compliance, an evaluation of the need for action to ensure non-recurrence of the shortfall, a determination of the appropriate action, followed by a review of the action to ensure that it has achieved its objectives. This follows Time to Reply Ltd's continual improvement approach.

18.2.2.2 Managers are required to document these reviews in accordance with ISMS-C DOC 18.2.2 as well as the actions required, and responsibilities and timeframes, in the case of shortfalls.

18.2.2.3 These management reviews and any actions arising must be reported in accordance with ISMS-C DOC 18.2.2 to the independent reviewers (see ISMS-C DOC 18.2.1)

18.2.3 Technical compliance review
Information systems are regularly reviewed and tested for compliance with Time to Reply Ltd's information security policies and standards, as set out in ISMS-C DOC 18.2.2.

•