# Jayex Technology Limited
# ISO27001:2017
# Information Security Management System (ISMS) Policy

## DOCUMENT CONTROL

| Title | |
|---|---|
| Date Issued | 12/02/2018 |
| Originator | Jayex Technology Limited<br>13 Sovereign Business Park<br>Coronation Road<br>London<br>NW10 7QP |

**Table of Contents**

**Control Document**

## 1. INTRODUCTION

This document is the Business Management Manual (the Manual) of **Jayex Technology Limited** and for the purpose of this manual will be referred to as '**ISO 27001 BMS'**.

The Manual is the property of **Jayex Technology Limited** and is a controlled document.

The purpose of the Manual is to provide an overview of **Jayex Technology Limited**, the activities it carries out and the ISMS standards of operation it conforms to.

It is not designed to act as a procedures manual, although it does carry information about where procedures information is located and the detailed information on documentation requirements for the procedures required by the respective standards.

This Manual is designed to meet the requirements of ISO 27001 and any standard which adopts the Annex SL structure.

### 1.1 THE ISSUE STATUS

The issue status is indicated by the version number in the footer of this document. It identifies the issue status of this Manual.

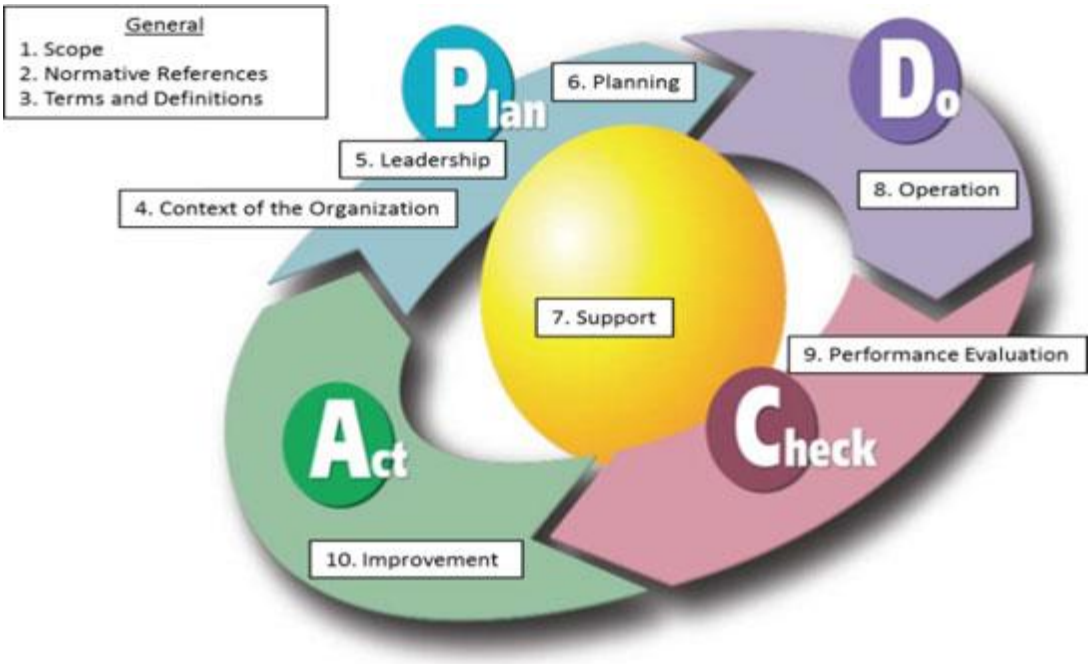
When any part of this Manual is amended, a record is made in the Amendment Log shown below.

The Manual can be fully revised and re-issued at the discretion of the Management Team.

Please note that this Manual is only valid on day of printing.

| Issue | Amendment | Date | Initials | Authorised |
|---|---|---|---|---|
| 1.0 | Initial document | 04/4/2014 | RA | |
| 1.1 | Revised for additional processes | 22/05/2014 | RA | |
| 1.2 | Revised after Audit | 02/09/2014 | RA | |
| 1.3 | Revised after External Audit | 06/06/2015 | RA | |
| 1.4 | Revised after External Audit –<br>1. Number of Staff removed<br>2. Smart Goals added to objectives<br>3. Pagination changes | 9/3/2016 | RA | |
| 1.5 | Added reference to Asset register | 17/08/2016 | MM | |
| 1.6 | Updated after Audit 31 -remove ref to VPN | 23/1/2917 | RA | |
| 1.7 | Updated after Audit 0037 | 1/6/2017 | RA | |
| 2.0 | Revised for ISO27001 - 2017 | 12/2/2018 | RA | 25/10/2108 |
| | | | | |
| | | | | |

### 1.2 PLAN-DO-CHECK-ACT Model



### 1.3 ISMS POLICY

It is the policy of **Jayex Technology Limited** to maintain an information management system designed to meet the requirements of ISO 27001 in pursuit of its primary objectives, the purpose and the context of the organisation.

It is the policy of **Jayex Technology Limited** to:

- make the details of our policy known to all other interested parties including external where appropriate and determine the need for communication and by what methods relevant to the business management system.
- comply with all legal requirements, codes of practice and all other requirements applicable to our activities;therefore, as a company, we are committed to satisfy applicable requirements related to information security and the continual improvement of the ISMS.
- provide all the resources of equipment, trained and competent staff and any other requirements to enable these objectives to be met;
- ensure that all employees are made aware of their individual obligations in respect of this information security policy;
- maintain a management system that will achieve these objectives and seek continual improvement in the effectiveness and performance of our management system based on "risk".

This information security policy provides a framework for setting, monitoring, reviewing and achieving our objectives, programmes and targets.

To ensure the company maintains its awareness for continuous improvement, the business management system is regularly reviewed by "Top Management" to ensure it remains appropriate and suitable to our business. The Business Management System is subject to both internal and external annual audits.

**Scope of the Policy**

The Jayex Information Security Policy is applicable to:

All Jayex information, information owned by its customers, and information about its customers.

All Jayex permanent, contract and temporary personnel, and all third parties, who have access to Jayex premises, systems, networks and information.

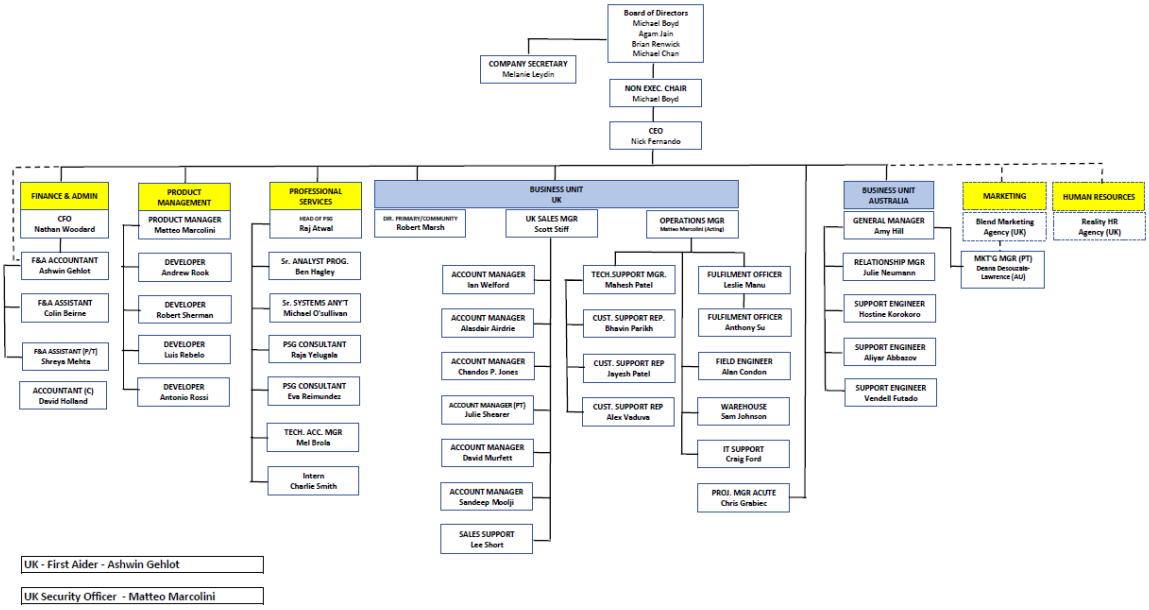
All Jayex computer systems, networks, software, and information created, held or used on those systems. Printed output from Jayex or client systems is also in the scope of this policy.

All means of communicating information, both within Jayex and externally. These include Data and voice transmissions, e-mails, fax, telex and voice and video conferencing

Top Management (To be signed and dated annually) See Version control for Signature

## 2. OVERVIEW OF THE ORGANISATION

Jayex Technology Limited is a subsidiary of Jayex Healthcare Limited, operating in London since 1978. Headquarters in London. Jayex specialise in healthcare self-service solutions and patient flow management. The company's software engineers are continuously developing ground breaking technical solutions to improve efficiency in clinics and hospitals. The organization offers a personal service to all their customers with designated Account Managers that provide consultation and advice.




*Last Updated Aug 2018*

### 2.1 SCOPE OF REGISTRATION

The design, supply and maintenance of advanced Healthcare service solutions.

## 3. OBJECTIVES

We aim to provide a professional and ethical service to our clients. In order to demonstrate our intentions, Our Management Team will Analyse:-

- Customer feedback/ complaints
- Security breaches
- Support cases
- Reduce Hardware/Laptop venerability by using Encryption

to ensure that our Objectives are being met.

**Information Security**

Our objectives are set out in our business plan and are then disseminated to each department/project for incorporation into their management roles.

Each department is responsible for delivering its objectives and this is monitored via individual, appraisals & team meetings. Jayex's ISMS Objectives are as follows:

- Objective 1: Existing services - Jayex will continue to deliver its services within a secure environment

- Objective 2: Development - Jayex will conduct annual risk assessments to ensure that risk to information in the care of Jayex is minimised or eliminated.

Whilst the above company objectives are "high-level", we have further analysed and categorised these into our Risk & Opportunities Matrix. In some cases, this may allow for specific objectives being set across different functions. This shows how we measure and set targets in meeting the "high level" objectives.

## 4. CONTEXT OF THE ORGANISATION

### 4.1 Understanding the organisation and its context

The context of the organisation is demonstrated within this Business Management System and all associated processes connected with the services / products offered.

The legal legislation / regulatory compliance to the service / products offered are listed below.

| Legal and Regulatory Legislation connected with the business | Hyperlink to Legislation etc |
|---|---|
| Code on Employers Monitoring Practices | https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf |
| EU Directive on Privacy and Electronic Communications | https://ico.org.uk/for-organisations/guide-to-pecr/ |
| Human Rights Act 1998 | https://www.legislation.gov.uk/ukpga/1998/42/contents |
| Working time directive | http://www.acas.org.uk/index.aspx?articleid=1373 |
| UK Data Protection Act 1998 | https://www.legislation.gov.uk/ukpga/1998/29/contents |
| UK Electronic Communications Act 2000 | https://www.legislation.gov.uk/ukpga/2000/7/contents |
| The Consumer Protection Regulations 2000 | http://www.legislation.gov.uk/uksi/2000/2334/contents/made |
| Freedom Of Information Act 2000 | https://www.legislation.gov.uk/ukpga/2000/36/contents |
| The Telecommunications (lawful Business Practice and Interception of Communications) Regulations 2000 | http://www.legislation.gov.uk/uksi/2000/2699/contents/made |
| Computer Misuse Act 1990 | http://www.legislation.gov.uk/ukpga/1990/18/contents |
| The Electronics Signatures Regulations 2002 | http://www.legislation.gov.uk/uksi/2002/318/made |
| The Telecommunications (Data Protection & Privacy, Direct Marketing) Regulations 1999 | http://www.legislation.gov.uk/uksi/1999/2093/made |
| The Consumer Protection (Distance Selling) Regulations 2003 | http://www.legislation.gov.uk/uksi/2000/2334/contents/made |
| Regulation of Investigatory Powers Act 2000 (RIPA) | https://www.legislation.gov.uk/ukpga/2000/23/contents |
| Civil Contingencies Act (2004 & 2005) (UK Government) | https://www.legislation.gov.uk/ukpga/2004/36/contents |
| Business Continuity Practice Guide: 2006 (UK Tripartite Authorities: Financial Services Authority (FSA), HM Treasury, Bank of England) | http://www.fsa.gov.uk/pubs/other/bcm_guide.pdf |
| Copyright, Designs and Patents Act 1988 (CDPA) | https://www.legislation.gov.uk/ukpga/1988/48/contents |

| | |
|---|---|
| Companies Act 2006 contains a number of provisions concerning records and communications | http://www.legislation.gov.uk/ukpga/2006/46/pdfs/ukpga_20060046_en.pdf |
| The Human Rights Act 1998 (HRA) | https://www.legislation.gov.uk/ukpga/1998/42/contents |
| The Privacy and Electronic Communications Regulations 2003 | http://www.legislation.gov.uk/uksi/2003/2426/contents/made |

Jayex HR department Manager will consult with Company Lawyers to establish compliance and is responsible for keeping the legal compliance register up to date and this is reviewed every time the ISMS is reviewed. l

### 4.2 Understanding the needs and expectation of interested parties

| Description | Location | Needs and expectations |
|---|---|---|
| Employees | Netsuite | Employees want to work in an environment that creates products and services that will meet the needs of the customers. This can be observed by review of the customer complaints. |
| Shareholders/owners of the business | Locked cabinet in Office | Shareholders want the security of investment and a good return. Continual improvement in security can be accessed by review of the management reports and SMART objectives set. |
| Accountants | Netsuite | Accounts want access to Accounts for the company to ensure proper compliance and Auditing |
| Company Solicitors / Lawyers | Netsuite | Company Lawyers/Solicitors want access to legal commitments made by company and advise company officers accordingly |
| Government agencies/regulators | Netsuite | Government agencies want the company to comply with information security/business continuity laws and regulations. These can be reviewed in the ISMS and Business continuity policies |
| Emergency services (e.g., firefighters, police, ambulance, etc.) | Assumed 999 | Access to buildings may be required by emergency services |
| Clients | Netsuite | Clients want the company to comply with security clauses in the contracts signed. Which can be seen and are monitored by the ISMS procedures and policies |
| Media | Netsuite | Media want quick and accurate news related to incidents. This can be obtained from the Incidence logs |
| Suppliers and partners | Netsuite | Clients want to comply with security clauses in the contracts signed. Clients can audit the ISMS policies and procedures to ensure compliance and see ISMS external Audit certificated |
| Directors | Netsuite | Ensure that the business continues to function in a profitable manner without hindrance and bureaucracy. |

### 4.3 Determining the scope of the business management system(ISO 27001)

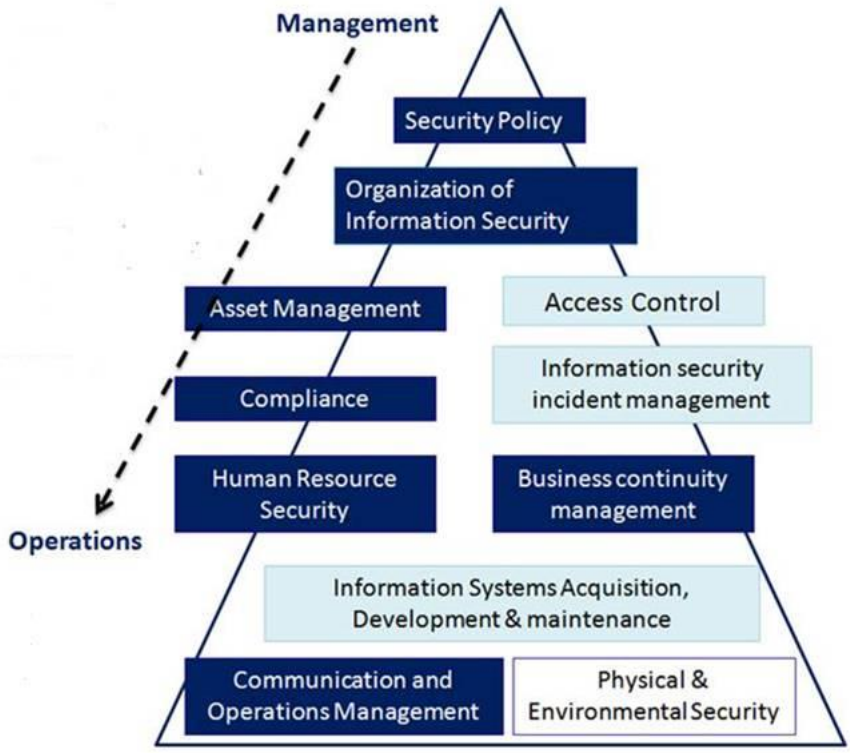
Information Security

The scope of the system covers all the core and supporting activities of the company. The activities and arrangements of all personnel including any sub-contractors also fall within the scope of the system.

### 4.4 Information Security Management system

The organisation has established, implemented, maintained and will continually improve an information security management system in accordance with ISO27001. This Business Manual provides information as to how we meet these requirements, with reference to key processes and policies, as appropriate.

**Enter below a flowchart of all processes involved within organisation**



# 5 LEADERSHIP

## 5.1 Leadership & Commitment

**Jayex Technology Limited's** Top Management Team are committed to the development and implementation of an ISMS Policy and the Information SecurityManagement System which are both compatible with the strategic direction and the context of the organisation, the whole system is frequently reviewed to ensure conformance to ISO 27001. Responsibility has been assigned to ensure that the business Management System conforms to the requirements of the respective standard and the provision to report on performance to the top management team has been defined.

The designated Senior Management Representative(s) will ensure that **Jayex Technology Limited** staff are aware of the importance of meeting customer as well as statutory and regulatory requirements, and overall, to contribute to achieving **Jayex Technology Limited's** Information Security Policy and Objectives which are aligned with the organisations strategic direction

The Senior Management Team is responsible for implementing this system and ensuring the system is understood and complied with at all levels of the organisation.

In summary, the Senior Management Team will ensure that:

### 5.1.1 Leadership and commitment for the Business Management System

- The company has a designated Senior Management Representative who is responsible for the maintenance and review of the Management System.
- The ongoing activities of **Jayex Technology Limited's** are reviewed regularly and that any required corrective action is adequately implemented and reviewed to establish an effective preventative process.
- Measurement of our performance against our declared Information Security Objectives is undertaken.
- Resources needed for the system are available and employees have the necessary training, skills and equipment to effectively carry out their work.
- Internal audits are conducted regularly to review progress and assist in the improvement of processes and procedures.
- Objectives are reviewed and, if necessary amended, at regular Management Review meetings and the performance communicated to all staff.
- The information security policy and objectives are established in line with the strategic direction of the organisation and that intended outcome(s) are achieved.
- The management system is integrated into the organisations business processes.
- Communication covering the importance of the effective management system and conformance to the management system requirements is in place.
- Continual improvement is promoted.
- The contribution of persons involved in the effectiveness of the management system is achieved by engaging, directing and supporting persons and other management roles within their area of responsibility.

An internal audit of procedures and policies is conducted annually. A review of the Information Security Objectives takes place once a year. In addition achievement of the quality objectives are measured against annual targets set in relation to the business plan. Staff contribution towards the Information Security Objectives is measured in supervision and documented annual appraisals in March

### 5.2 ISMS Policy

The ISMS Policy of **Jayex Technology Limited** is located within section 1.3 of this Manual.

### 5.3 Organisational roles, responsibilities and authorities

**Jayex Technology Limited** has an organisation chart in place, employee contracts together with job descriptions to ensure that the appropriate personnel are in place to cover the whole context of the organisation and strategy of the business.

Our Information Security Manager (this role is carried out by- see Org chart) is responsible for randomly sampling records to ensure that all required data has been captured, and that data is accurate and complete.

*See Organisation Chart Section 2*

## 6 Planning for the Business Management System

### 6.1 Actions to address operational risk and opportunities

We have identified the risks and opportunities that are relevant to our Business Management system from an operational perspective. This also links to section 4.1 and 4.2 of this manual and also provides information on low-level objectives. This 'Context, Risk, Opportunities and Objectives' (CROO) document is separate to this manual. Within each of the areas the risks are identified together with a rating as to the importance of the risk. The associated consequence & mitigation of the risk is also noted together with any new opportunities that we have identified. Where applicable, we have identified measurable objectives and these can be found within a separate tab in the 'CROO' document.

The controls identified in this document feed into our risk treatment plan (Statement of Applicability), which has been designed and implemented using the main headings within the standard (Annex A, Table A.1 – control objectives and controls) as a guide to establish that all controls required have been considered and that there are no omissions. The document identifies controls to mitigate risks following the process of identification, analysis and evaluation. The SOA document is separate to this Manual.

### 6.1.2 Information Security Risk Assessment

In accordance with our 'CROO' matrix referenced in 6.1, above, we have assessed any typical / likely Information Security threats based on their potential effects on Confidentiality, Integrity and Availability (CIA) attributes.

Following this analysis, appropriate controls have been identified, which feed into our Statement of Applicability, as described in section 6.1.3, below.

### 6.1.3 Information Security Risk Treatment

The approach to our risk treatment plan has been designed and implemented using the main headings within the standard (Statement of Applicability - Control objectives and controls) as a guide to establish that all controls required have been considered and that there are no omissions.

The document identifies controls to mitigate risks following the process of identification, analysis and evaluation described in section 7 and is directly linked to the aspects of the organisation.

The SOA document is separate to this Manual and conforms to the requirements as defined within clause 8.3 of the ISO 27001standard.

**Please see below document as demonstration:-**

a) CROO Document (Context, Risk, Opportunities & Objectives)
b) Statement of Applicability

### 6.2 ISMS Objectives and planning to achieve them

The ISMS Objectives and methods of achieving the objectives is located within section 3 of this Manual.

## 7 Support

### 7.1 Resources

**Jayex Technology Limited** determines and provides the resources needed for the establishment, implementation, maintenance and continual improvement of the management system.

We ensure that the below elements are taken into account when completing an evaluation:

- The capabilities of, and constraints on, existing internal resources;
- What needs to be obtained from external providers

NOTE: If you operate as a "multi-site" client (i.e. have various locations covered under certification), please also include details of how you monitor the above and how this is carried out in practice

### 7.2 Competence

All employees have the training and skills needed to meet their job requirements. All employees are monitored on an ongoing basis to identify any training and development needs. Competences and training needs are identified / satisfied by using:

**Please see below documentation as demonstration of compliance:**

| | |
|---|---|
| Job descriptions which set out the competences required | |
| Contracts of employment which set out contractual and legal requirements | **Employee handbook** |
| Induction checklists to ensure / check understanding | **Induction check list** |
| Appraisal reviews to monitor performance | **JAYEX TECHNOLOGY LIMITED Annual Review** |
| Development plans to set objectives | **JAYEX TECHNOLOGY LIMITED Annual Review** |
| On the job reviews to ensure / check levels of competence | **Jayex_Training_Matrix** |
| Tests of understanding | |
| A Training / competency matrix | **Jayex_Training_Matrix** |
| | |

### 7.3 Awareness

We ensure that all employees are aware of all policies and their contribution to the effectiveness of the Management System through:

- *Notice Boards*
- *Employee Handbook*
- *Awareness Training*
- *Induction*

### 7.4 Communication

Senior management utilise JAYEX TECHNOLOGY LIMITED's internal communications framework in order to disseminate information about the effectiveness of the Information Security Management System

### 7.5 Documented Information

#### 7.5.1 General

**Jayex Technology Limited** demonstrates documented compliance to ISO 27001 through this Business Management System Manual (which includes processes& procedures) on an electronic system which is available on the google drive which is accessible to all employees. All information is read only and only accessible via the document owner for amendment.

#### 7.5.2 Creating and updating

The creation of documentation to support the Business Management System is primarily the responsibility of the designated "Top Management Representative".

Identification will be sought by a document number, date and author. To aid the approval and suitability of documents, the Managing Director of **Jayex Technology Limited** authorises the release and delegates any training required to the "Top Management Team".

#### 7.5.3 Control of documented information

All documentation is controlled by version and date and is listed on a "ISO Dashboard on google drive"

**Jayex Technology Limited** has Netsuite and Google Drive software in place to avoid the loss of confidentiality, improper use or loss of integrity.

Control of documents can be seen on the Dashboard and encompasses the following elements:-

- Distribution, Access, Retrieval and use
- Storage and preservation, including preservation of legibility
- Control of changes (e.g. version control)
- Retention and disposition

Documents can be retrieved by authorised personnel from the storage locations specified *and / or from folders on the network*. Customer records are identified by *customer name on Netsuite.*

On or after the retention period stated, the relevant records will be reviewed by Top Management and will either remain in-situ, be archived or destroyed.

If records are to be destroyed, they will be disposed of in a controlled manner; *sensitive hard copies will be shredded and soft copies will be deleted from the system*. If records are to be archived, they will be identified and stored appropriately

**Please see below document as demonstration of compliance:**

**Hardware_Software_Disposal_Procedure.docx**

## 8 Operation

### 8.1 Operational planning and control

**Jayex Technology Limited** has determined the requirements and controls implemented for all processes needed to meet Information Security requirements and has implemented the actions described in section 6.1 of this manual. We will also implement plans to achieve ISMS objectives, as highlighted in sections 3 and 6.2 of this manual. We retain documented information to the extent necessary to have confidence that the processes have been carried out as planned. We shall control any planned changes and will review the consequences of unintended changes, taking action to mitigate any adverse effects.

### 8.2 Information Security risk treatment

In line with the criteria established in section 6.1.2 of this manual, we perform ISMS risk assessments at planned intervals or when significant changes are proposed or occur. Documented information of the results of risk assessments is retained.

### 8.3 Information Security risk treatment

The risk treatment is incorporated within Risks & Opportunities – See Clause 6.1

## 9 Performance Evaluation

### 9.1 Monitoring, measurement, analysis and evaluation

Monitoring is based on risk and is linked to the risk & opportunities register together with the risk assessments which are carried out. This is also monitored through internal audits (section 9.2) and management review (section 9.3) to ensure the effectiveness of the management system.

### 9.2 Internal Audit

An internal audit schedule is prepared on an annual basis year and covers the requirements of the ISO27001 standard. Internal audits are carried out through “risk or claused based” auditing.

Appropriate personnel are allocated to complete the internal audits and must record appropriate evidence for completeness. All audits completed must be authorised by Top Management as complete once any non-conforming areas have been dealt with (without any undue delay). Internal audit documentation must be kept and filed appropriately.

**Please see below document as demonstration of compliance:**

***INTERNAL AUDITS CHEDULE-COMBINED***
***Corrective Action Log***
***INTERNAL AUDIT REPORT(Internal Audit Plan)***

### 9.3 Management Review

Management reviews take place on annual basis. The attendees present are “Top Management” and any other appropriate persons of the business.

All inputs / outputs are full documented and minuted in line with the requirements of the specific ISO standard in which **Jayex Technology Limited** wish to be certified. Any actions arising from the meeting must be completed without any undue delay and appropriate evidence filed with the Management review documentation.

**Please see below document as demonstration of compliance:**
***Management_review_Procedure.doc***

## 10 Improvement

### 10.1 Nonconformity and corrective action

Should a nonconformity occur, including those arising from complaints, internal audits & external 3rd part assessment **Jayex Technology Limited** designate the appropriate "Top Management" representative to ensure that corrective action including root cause analysis is completed and implemented to avoid any further occurrences. This is then analysed and should the risk to the business pose to be "high" then this is then entered onto the "CROO document" (See Clause 6.1) to assist in mitigating the risk to the business.

Should any non-conformances occur or be identified then an internal audit report / non-conformance report must be completed to ensure that a full analysis of the problem is resolved. A summary of all actions will be maintained within the Management Action Log.

The corrective action plan summary must be completed, as this then forms part of the Management Review meeting.

**Please see below document(s) as demonstration of compliance:**

**Audit Schedule**

### 10.3 Continual Improvement

Continual Improvement will be ongoing through various elements of the Business Management System which is encompassed within this document. The list below is not exhaustive: -

- CROO Document – Evaluated at several stages (clause 5.1, 6.1)
- ISMS Policy / Objectives
- Planning of Changes
- Competency Matrix
- Customer Satisfaction
- Internal Audits
- 3rd Party External Audits
- Management Review