OASIS
Integrated Management System
Procedures Manual

Conforming to the requirements of

Issue: 4
Copy No. 1(Master Copy)
Authorised By: Claire Gallagher
Holder: Claire Gallagher
Date: 10th October 2012
## CONTENTS TABLE

Document Control.................................................................................................................. 3  
Circulation List.......................................................................................................................... 3  
Amendment History................................................................................................................. 3  

| IP01  | DOCUMENTATION AND RECORD CONTROL | 4 |
| IP02  | MANAGEMENT REVIEW MEETING | 8 |
| IP03  | TRAINING, SELECTION AND VETTING | 10 |
| IP04  | CORRECTIVE AND PREVENTIVE ACTIONS | 15 |
| IP05  | INTERNAL AUDITS | 17 |
| IP06  | IDENTIFICATION OF INFORMATION SECURITY RISKS | 19 |
| IP07  | RISK TREATMENT PLANS | 21 |
| IP08  | PROCUREMENT AND SUPPLIER MANAGEMENT | 23 |
| IP09  | IDENTIFICATION OF CUSTOMER REQUIREMENTS | 26 |
| IP10  | SECURITY ARRANGEMENTS | 27 |
| IP11  | STORAGE AND RETRIEVAL OF DOCUMENTS | 32 |
| IP12  | EQUIPMENT MAINTENANCE AND CALIBRATION | 35 |
| IP13  | EMERGENCY AND CONTINGENCY PLAN | 37 |
| IP14  | VISITOR CONTROL | 42 |
| IP15  | MONITORING AND MEASUREMENT | 43 |
| IP 16 | Cleaning Procedure | 44 |
Document Control

Circulation List

This IMS Manual is a controlled document. The Management Representative must ensure that all amendments are circulated and obsolete copies removed and filed. The IMS Manual is distributed as follows by the Management Representative:

<table>
<thead>
<tr>
<th>Copy No.</th>
<th>Holder</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Master)</td>
<td>Executive Vice President of Administration</td>
</tr>
<tr>
<td>2</td>
<td>General Manager (ROI)</td>
</tr>
<tr>
<td>3</td>
<td>General Manager (NI)</td>
</tr>
<tr>
<td>4</td>
<td>General Manager (UK)</td>
</tr>
</tbody>
</table>

All staff shall have access to the Integrated Management System Policy Manual as a Read only document on the network. This shall be password protected under the control of the Management Representative.

Amendment History

This document is amended by the distribution of new revisions of all or part of the IMS Manual to the named holders. The history of amendments is recorded below.

Copies of this document other than those listed above will not be revised, such copies are marked as UNCONTROLLED.

Amendment Record

<table>
<thead>
<tr>
<th>Date</th>
<th>Amendment Number.</th>
<th>Section and Page Number</th>
<th>New Issue Number.</th>
<th>Details of Amendment</th>
<th>Authorisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/03/2007</td>
<td>N/A</td>
<td>All</td>
<td>0</td>
<td>First Issue</td>
<td>Claire Gallagher</td>
</tr>
<tr>
<td>16/09/2009</td>
<td>1</td>
<td>All</td>
<td>1</td>
<td>Revision of manual to incorporate changes in Company name and responsibilities.</td>
<td>Claire Gallagher</td>
</tr>
<tr>
<td>20/05/2011</td>
<td>2</td>
<td>All</td>
<td>2</td>
<td>As Above</td>
<td>Claire Gallagher</td>
</tr>
<tr>
<td>10/19/12</td>
<td>3</td>
<td>All</td>
<td>3</td>
<td>As Above</td>
<td>Claire Gallagher</td>
</tr>
</tbody>
</table>
IP01 DOCUMENTATION AND RECORD CONTROL

1 Scope

This procedure covers:

- The issue, modification and control of all Integrated Management System documentation, together with any external standards held by the Company;
- The control of all records related to the operation of the Integrated Management System.

2 Purpose

This procedure is to ensure that:

- All IMS documentation is authorised prior to issue, and that only current versions of documents are in use;
- Sufficient records are maintained to demonstrate the effective operation of the IMS.

3 Responsibilities

The Management Representative is responsible for the initial authorisation of Integrated Management System documentation.

The Management Representative is responsible for ensuring that documentation is controlled as outlined in this procedure, and that adequate records are maintained to demonstrate the effective operation of the IMS.

Individual members of staff are responsible for generating and maintaining records as required by the various procedures within the IMS.

4 Related Documentation

- Document List

5 Procedure

Control and Issue of Copies

Prior to issue the Executive Vice President of Administration must authorise all Integrated Management System documents. The Executive Vice President of Administration (overall Management Representative) is responsible for maintaining a master copy of each document relating to the Integrated Management System, including sample copies of forms etc.
The Executive Vice President of Administration is responsible for ensuring that all copies of manuals/procedures are marked with an individual issue number, and that copies are issued to all holders listed on the circulation list contained within each individual document.

The Management Representative on each site (General Manager / Branch Manager) shall ensure that:

- Documentation is legible, dated, (with dates of revision), and readily identifiable, maintained in an orderly manner.
- Current versions of relevant documents are available where operations essential to the effective functioning of the Integrated Management System are performed.
- Obsolete documents are promptly removed from all points of issue and points of use, or otherwise assured against unintended use.
- Any archived data and documents retained for legal and/or knowledge preservation purposes are suitably identified.

**Amendments**

Amendments to IMS documentation may be suggested by any member of staff, however, all amendments must be authorised by the Executive Vice President of Administration or appropriate Management Representative, and the relevant Amendment History updated. The revision status of the Amendment History is indicated by the last amendment reference number shown on the sheet.

Amendments may also be made due to the results of audits, management review or to increase the effectiveness of the management system. The revision number of newly amended documentation shall be increased by 1.

Following an amendment, the Management Representative is responsible for circulating the amendment to all copyholders.

Upon receipt of any amendments, each document holder is responsible for the insertion of the amendments and for destroying obsolete documentation.

**Management System Records**

The responsibility for generating and storing records shall be with the relevant members of staff under the overall control of the Management Representative.
All records associated with the IMS are retained in the appropriate files for the duration specified on the Document List. The Document List also includes any data stored electronically.

The purpose of the listing is to identify all items associated with the operation of the Quality system that are retained in the record system, and indicate the minimum time for which each record should be retained.

The Management Representative is responsible for the disposition of the records after the stated retention period.

All data held electronically, including emails, are backed up on a daily basis and stored at Head Office. The IT Department are responsible for ensuring the Security and retrieval of documents held electronically. IT procedures and policies are in place and are available from the IT Company. The Company have compiled an email policy which is attached in Appendix E of the IMS Policy Manual.

Control of Documentation – Document List.xls

The Management Representative manages an Excel Sheet, Document List detailing each individual document created for the Oasis Group. The Document List gives details the document type, title and revision number.

Manual Change & Modification

All requests for changes are reviewed to ensure that the amendment is required and that it is correct. The master copy is amended and approved and the Document List is updated, dated, and to indicate a revision the Issue number is incremented by 1 in both the Document List and in the hard copy. The manual is re-issued to staff and a copy of the old section is kept in the obsolete section of the manual.

Control of Forms & Records

A copy of the current issue level of each form is kept in the ISO 9000 Folder. When forms are revised the issue number is updated incrementally. All forms and records associated with this management system are listed in the Document List, Excel Sheet (hard copy in the ISO9000 Folder).

The Operational Procedures define the controls needed for the identification, storage, protection and retrieval of Clients records. The Client's records are stored in a manner that ensures their protection and ease of retrieval.
Control of External Standards and Documents

The Management Representative on each site is responsible for maintaining any external standards required by the Company, and for monitoring the issue status of these standards through a recognised updating service.

Department Managers are responsible for ensuring that any reference documents are up to date and available.

Classification of Information

The Company have classified types of information into varying levels of sensitivity and have implemented associated protective controls for confidential information taking account of business needs for sharing / restricting information, and the business impacts associated with such needs.

Data Protection

All employee and customer records containing confidential information such as bank details, etc are stored in a locked cabinet under the control of the Finance Department.

Confidential waste is placed in segregated bins for collection and shredding by an outside waste management company.

Currently virus control software has been installed on all computers in the Company. The software automatically requests updates electronically daily via Internet.

Computerised data is backed up in accordance with Back-up Tapes procedure OP04.
IP02 Management Review Meeting

1 Scope

This procedure outlines the conducting of the 6-monthly management review of the operation of the Integrated Management System.

2 Purpose

The purpose of the procedure is to ensure that the Company’s Integrated Management System is suitable and effective and meets the requirements of ISO 9001: 2008 and ISO27001: 2005.

3 Responsibility

The Director of Account Management has overall responsibility for the Management Review process.

4 Related Documentation

- Management review minutes
- Management Meeting minutes

5 Procedure

The Director of Account Management is responsible for ensuring that all elements of the Integrated Management System are reviewed annually. The review shall take the form of a meeting chaired by the CEO, and attended by the following personnel:

- General Manager
- EVP Ops & Sales
- EVP Administration
- CFO Chief Financial Officer

Other Company personnel, for example Operations staff may be required to attend the meeting from time to time to discuss specific issues.

The agenda for the meeting should be all elements of the Integrated Management System, which gives an indication of its continuing effectiveness. The inputs to this meeting shall include the following:
Minutes of the previous meeting
• Review of the Integrated Management System documentation including procedures
• Review of risk assessment and risk acceptance – Information Security (Statement of Applicability, Security threats and controls)
• A measure of the effectiveness of controls
• Review of Contingency Plans
• Applicable legislation and other requirements to which the Company subscribes, including compliance
• Improvement objectives and risk treatment plans
• Customer complaints, communications and feedback, including feedback from all interested parties
• Review of Accidents / Incidents / Security breaches
• Identification of non-conformances to the Integrated Management System
• House keeping procedures
• Results of internal audits including Security audits
• Review of corrective and preventive action(s) taken
• Training needs analysis and review of effectiveness of training
• Supplier re-evaluation & Subcontractor performance /analysis
• Addressing the need to change the policies
• Overview of effectiveness of systems and processes in meeting customer requirements & any recommendations for improvement
• Future progress for the integrated management system including changes which could effect the Integrated Management System e.g. changes to or addition of new information storage facilities.

The results of the review meeting must be available in the form of minutes maintained by the Management Representative. The output of the meeting are any actions to be taken, a time scale for implementation and a date for a follow-up action.

Minutes of Management Review Meetings shall be kept for a period of 5 years.
IP03 TRAINING, SELECTION AND VETTING

1 Scope

This procedure covers the training policy operated by the Company for all staff. It also addresses the vetting controls operated by the Company.

2 Purpose

This procedure is to ensure that new and existing personnel are adequately trained to perform the tasks assigned to them and that all personnel have been satisfactorily vetted to handle secure and confidential information.

3 Responsibility

The General Manager and Branch Manager have overall responsibility for the identification of the training requirements and the provision of training needs, and is assisted in this activity by the Management Team.

4.0 Related Documentation

- Selection and Vetting forms
- Purviews
- Personal Profile Form
- Appraisal Sheet
- Interview Form
- Confidentiality Agreement

5 Procedure

All employees and persons working for and on behalf of Oasis Group shall be competent in their tasks based on their skills, experience and training. Roles and responsibilities are defined within Purviews including Information Security and Quality responsibilities.

An induction presentation is given to all new starts to provide a forum for addressing Quality and Security related responsibilities.

On receipt of induction, the employee shall sign the training record sheet as evidence of training received. A contract of employment shall also be signed outlining Security related responsibilities and associated disciplinary procedures.

All existing staff within the organisation shall receive training on the Information Security and Quality Policies, and the requirements of the Integrated Management System in general. This shall include the importance of meeting objectives, conforming to policies, legal responsibilities and the
requirement for continual improvement. New employees will be covered as a part of the Induction Program of the Company.

The identification of individual training requirements is carried out as part of the monthly Management Meetings and through employee periodic assessments.

It is the responsibility of the department manager to ensure that the people that are assigned to particular tasks are competent on the basis of relevant education, training, skills and experience.

The department manager must also ensure that all employees are aware of the need to follow specified procedures and the consequences of not following them.

The skills required for a particular position are detailed in the relevant Purview. On assignment to a particular position, staff members are trained in the skills required to perform the job. A Personal Profile Form is raised for each employee detailing training, education and experience. Extra training requirements are identified through the appraisals and will be recorded on the Appraisal Sheet.

Purviews - Purviews are available for all positions, which include Security responsibilities. These are signed both by the employee and appropriate manager. Employees are provided with a copy of the Purview.

Standard operating procedures and manuals are distributed throughout the premises as required.

The effectiveness of training provided and the competency of staff is determined through employee periodic assessments / appraisals.

Integrated Management System awareness training shall include the following:

- Introduction to the policy statement, and the Integrated Management System
- Specific Quality training
- Specific training on Security arrangements
- Potential consequences of departure from specified operating procedures
- Responsibility of the employee to achieve conformance with the IMS

Particular attention is paid to the training of personnel whose daily job functions can or may cause:

- Affect product or service Quality
- Significant risk to Security
In these cases the Company ensures that personnel shall be competent on the basis of appropriate education, training and/or experience.

Training for emergency situations shall be provided by the Company, e.g. fire evacuation, Security breaches etc.

Where a sub-contractor is called upon to provide services, the appropriate Manager shall ensure the sub-contractor has the appropriate training and qualifications. Relevant issues relating to the IMS will also be communicated to such staff e.g. Security arrangements, etc.

Training records are maintained by the Accounts Manager for all staff members. Training Records shall detail all training, including both internal and external training, completed by the employees.

All potential employees are made aware at the application stage that it is a requirement for all site personnel to be vetted and any position in the Company requires the completion of a vetting form on commencement of employment.

The Management Representative is responsible for ensuring the successful vetting of all site personnel.

Recruitment Screening - Potential recruits are adequately screened by the Recruitment Agency. References are verified by telephone and comments are recorded on the Interview Form. All Employees and third party users of IT facilities are required to sign a Confidentiality Agreement.

In the event of a foreigner being employed, the Accounts Manager shall ensure that a Home Office check is carried out on the individual.

No member of staff / potential employee may gain access to the information storage facility prior to completion of the vetting or in the event of unsuccessful vetting.

On completion of successful vetting, a Security pass is issued to the employee. This pass is coded to enable access to only those areas appropriate to the nature of the individuals work.

**User Training - Security Awareness**

Staff members are inducted in accordance with the Human Resources Process. This includes an induction into operational and Security procedures. This is recorded on the Employee Interview Form, signed procedures and Confidentiality agreement form.
Technical Training Requirements

- Network Management
- Database Administration
- Back-up
- Access Control Technology
- CCTV Security

Training is received in Access Security and Network Management. Certificates are received for this training. Technical Training is identified according to job description and requirements and is recorded in the individual’s training records.

Records of Security vetting are maintained in the individuals’ personnel files. A record is maintained on the issue of Security passes and the Management Representative shall ensure that these are returned on the individual leaving the Company.
Vacancy

PURVIEW

Competency Model

Gap analysis

Security Vetting

Training Plan

Verify effectiveness and competency

Training Matrix / Training Records

Personnel Audit / Appraisals
IP04 CORRECTIVE AND PREVENTIVE ACTIONS

1 Scope

This procedure covers the identification, reporting and resolution of non-conformances or problems / issues relating to the Quality and Information Security aspects of the Integrated Management System.

2 Purpose

This procedure is to ensure that all instances of non-conformance (incidents) or opportunities for improvement are identified promptly, and that appropriate action is taken to prevent recurrence of the incident or problem.

3 Responsibility

It shall be the responsibility of all employees to ensure that all problems, incidents and opportunities for improvement are identified and resolved.

The Management Representative has overall responsibility for the operation of the reporting systems, and for reporting to management where necessary.

4 Related Documentation

- Incident Report Form
- Management meetings minutes

5 Procedure

Problems, incidents and opportunities for improvement may include but are not limited to the following circumstances:

- Incorrect classification / labelling of information
- Complaints from customers
- Security breaches, theft of information,
- Other aspects of the Company’s services which do not conform to expected standards.

Incident Management Procedures

Incidents are recorded on an Incident Form, detailing the nature and details of any incident, concern, non-conformance or Security breach. The reason or root cause of the incident or concern is investigated and corrective action is agreed to prevent reoccurrence. These are reviewed to ensure corrective/preventative actions have been or are being taken at the weekly Operations Meeting and again briefly at the monthly Management Meeting.
Responding to Incidents

Security incidents shall be reported using the current Incident Form. This includes suspected Security weaknesses, software malfunctions, etc.

The Disciplinary Procedure is communicated to staff through the Employee Contract.

Security Breaches are a disciplinary offence, action detailed in the Disciplinary Procedures.

The Management Representative on each site, via the appropriate supervisor/manager, is responsible for the investigation of the incident, and for reporting the actions taken to the Management Meeting and for recording actions on the Incident Form as applicable. The action taken should consider not only the immediate action to be taken to correct the problem, but also action necessary to prevent a recurrence.

The Management Representative is responsible for reviewing all issues and opportunities for improvement, to ensure the effectiveness of corrective actions.

In addition to the above, all issues and opportunities for improvement are reviewed as part of the management review process.

Preventive Action

The Company adopts a proactive approach to identifying problems before they occur and will where possible introduce preventive actions before problems occur.

Monthly management meetings shall be held to discuss and deal with any problems, Quality issues, resource issues and potential problems arising in order that proactive preventive actions may be determined and implemented. All issues and resulting actions are recorded and monitored through the minutes of the meetings.

In addition to the ongoing review, problems, incidents and opportunities for improvement and associated corrective actions will be reviewed as part of the management review. The management review meeting held will also be used to identify potential problems and preventive actions to be taken to avoid any disruption to Quality of service.
IP05  INTERNAL AUDITS

1  Scope

This procedure covers the conduct of internal audits of the Integrated Management System in all areas of the Company’s activities.

2  Purpose

The purpose of the Internal Audit is to ensure that the Integrated Management System is systematically reviewed on a regular basis to check its continuing suitability and effectiveness.

3  Responsibility

The Director of Account Management has responsibility for the organisation and operation of the internal audit program. The appropriate member of staff as applicable will carry out audits.

4  Related Documentation

- Internal Audit Schedule
- Internal Audit Report Form

5  Procedure

The Director of Account Management is responsible for the establishment of an Internal Audit Schedule, covering all elements of the Integrated Management System, and for selecting personnel as internal auditors with relevant experience and who are capable of conducting independent internal Information Security and Quality related audits.

The audit schedule shall be adjusted on a continual basis as a consequence of previous audit results. The time scale shall be such that all elements are audited at least once in a year; although those activities which are deemed more sensitive, (whether from a Quality or Security viewpoint), shall be audited more frequently.

Prior to each audit the auditor reads the section of the relevant procedure or work instruction in order to prepare audit checks.

The auditor will satisfy his/herself whether or not the procedure is being complied with. This is achieved by asking questions, checking a sample of records, observing what is happening and listening to auditees.

The Audit Report is used to record areas checked, records checked, persons
spoken to, equipment looked at and any problems found.

Any non-conformances or observations will be recorded on the Audit Report Form.

The auditor discusses the audit findings with the person responsible for the area being audited to obtain a commitment on corrective action and whenever possible, decide upon a date for completion of same. This is recorded on the Audit Report.

The Audits are reviewed within a month of audit to record the implementation and effectiveness of the corrective action taken. This is recorded on the Audit Report.

All audit reports are analysed and the findings summarised prior to the Management Review for the purpose of identifying areas for improvement

Any changes to existing procedures, work instructions, etc. resulting from the preventive action(s) must be made and recorded.
IP06 IDENTIFICATION OF INFORMATION SECURITY RISKS

1 Scope

This procedure covers the process of risk identification and the subsequent risk assessment process in the following areas:

- Routine and non-routine activities
- Activities of all personnel having access to the workplace
- Facilities at the workplace where provided by the Company or others

2 Purpose

To ensure that all Security risks are assessed on a regular basis and in a consistent manner.

3 Responsibilities

The Management Representative and Management Team have overall responsibility for the identification of Security risks and the introduction of subsequent control measures. This process may be delegated to relevant supervisors/operations manager as required.

4 Related Documentation

- Statement of Applicability
- Visitors Book
- Security Risk Assessment

5 Procedure

The Register of Information Security Risks is reviewed every year and/or when operations at the Company are changed, and/or with the introduction of new or modified equipment or processes, and/or as a result of Security breaches / incidents, and/or as a result of changes in legislation.

Information Security risks are identified through the identification of Security threats and a Statement of Applicability. The risk assessment, residual risks and identified acceptable levels of risk shall be reviewed as above and shall take account of changes in operations, technology, business objectives, identified threats, the effectiveness of controls and legal and contractual requirements.

The Company will endeavour to reduce risks/aspects to an acceptable level through the introduction of suitable control measures and risk treatment plans.
On commencement of a new contract, the Sales Manager shall carry out a specific risk assessment on the site at the enquiry stage to identify any special requirements or secure systems of work required.

The results of the inspections will be reviewed at the management Meeting and suitable corrective and preventive actions will be agreed.

Based on the risk assessment the Company will develop safe methods of work, emergency preparedness plans and contingency plans which reflect the potential emergency situations e.g. Security breaches, loss of information through fire etc.

All personnel will be trained in the operation of the safe methods of work, emergency preparedness and contingency plans.

The plans will also be reviewed after Security breaches and incidents and also at the Management Review Meeting.

Where work is being carried out on the Company’s premises it will be the responsibility of the Management Representative to ensure that the risks associated with such work are assessed. Visiting contractors will be required to sign a copy of the Company’s Confidentiality Agreement and details of Visitors and Contractors will be recorded in the visitor’s book.
IP07  RISK TREATMENT PLANS

1  Scope

This procedure covers the following principal activities:

• Setting of Security related objectives and targets / risk treatment plans
• Development of management programmes to meet objectives & targets
• Reviewing of progress of objectives and targets set
• Actions to take when the Company fails to achieve an objective and target set

2  Purpose

To ensure that realistic objectives and targets are established in relation to Security issues, and to the operation of the IMS, and that progress in achieving the objectives and targets is reviewed.

3  Responsibilities

The Director of Account Management, in conjunction with other members of management, is responsible for devising, maintaining and updating risk treatment plans at relevant levels within the organisation.

All staff are responsible for assisting in the achievement of the various objectives and targets.

4  Related Documentation

Risk Treatment Plans (Objectives and Targets / Management Programmes)

5  Procedure

Setting of Objectives and Targets

Objectives and targets are identified with consideration to the following:

• Significant Security threats / risks
• Financial considerations
• Legal requirements
• Views of interested parties
• Operational and business requirements / targets
All details regarding IMS objectives and targets are recorded on the Objectives and Targets Record Form. For each significant Security risk, at least one objective is devised. All objectives with clearly defined targets will include:

- Start date
- Completion date
- Responsibility
- Measurable targets

A Management Programme will be drawn up for each objective and target. Each Management Programme must be given a title, a reference number and the objectives and targets to be achieved must be identified.

The Management Representative shall select relevant personnel to be responsible for the completion of the management programmes.

At the end of each calendar year, the objectives and targets are updated and revised. The Management Team must set new objectives and targets for the coming year. The new objectives and targets devised must be recorded on the Objectives and Target Record Form.

The Management Representative must ensure that objectives and targets are communicated to all employees through the publication of the objectives and targets on the notice board in the Company.

**Reviewing Progress of Objectives and Targets**

Progress of achievement of Objectives and Targets must be reviewed at least every three months, (progress meeting depends upon the timescale for the objective and target). The progress against each target must be recorded on the Objective & Targets Record Form.

Any action(s) to be completed as a result of the review must be recorded, with timescales for implementation.

**Failure of Objectives and Targets**

In the event where the Company fails to achieve Objective(s) and Target(s) in the stated timescale, an investigation shall be conducted by the Management Representative to determine the cause of the failure. As a result of the investigation, corrective action(s) and/or preventive action(s) must be outlined and a new target date for completion of the corrective action(s) must be set.
IP08  PROCUREMENT AND SUPPLIER MANAGEMENT

1  Scope

This procedure covers:

• The selection and evaluation of all suppliers of goods and services, and of subcontractors used by the Company,
• The purchase of all goods and materials which directly affect Quality, and
• The inspection of all goods and materials received by the Company.
• The control of assets in accordance with ISO27001:2005

2  Purpose

The purpose of the procedure is to ensure that only suppliers and subcontractors meeting the Company’s Quality requirements are used by the Company, that the purchasing of materials is controlled in a manner which maximises the use of materials, and minimises the Company’s purchasing costs, and that all materials are checked for compliance with the specified requirements prior to use. This procedure also ensures adequate control over assets and the secure handling of assets.

3  Responsibility

The Accounts Department has overall responsibility for the approval of suppliers and subcontractors to the Company. All members of staff have a responsibility for monitoring the performance of suppliers and subcontractors on an ongoing basis, and for notifying the Accounts Department of poor performance.

The Accounts Department are responsible for the authorisation of all Purchase Orders.

All office staff are responsible for the checking of goods delivered direct to site.

The Management Representative at each site is responsible over the preparation and updating of the Register of Assets and the asset owners are responsible for the handling of information, hardware and software in a secure manner.

4  Related Documentation

• Purchase Order
• Approved Supplier/Subcontractor List
• Delivery Notes
• Supplier / Sub-contractor Performance Assessment
• Asset Register

5 Procedure

Supplier Control

A list of approved suppliers is maintained. Our basis requirements of our suppliers are that they supply their goods on time and at the right price. Any specific requirements will be provided in writing to our suppliers. The criteria for approval can be one or all of the following:

• Price
• Availability
• Reputation
• Previous experience
• Quality

The basis for approval will be recorded on the Approved Suppliers List. An account is set up on the computer system.

Supplier performance is reviewed on an ongoing basis and if any supplier is no longer meeting the Company’s requirements appropriate action will be taken. This may result in the supplier being removed from the Approved suppliers List.

Every 12 months a formal review of suppliers is carried out. This review is recorded on the Approved Suppliers List. Problem suppliers are discussed at the Management Review Meeting and appropriate action will be decided upon. This may result in removal of suppliers from the Approved Suppliers List.

Purchasing Data

A Purchase order is raised in accordance with the Accounts Payable procedure 4/12.

Goods Inwards

On receipt, goods are identified against the supplier delivery docket. Goods are inspected against the supplier Delivery Docket for

• Quantity,
• Description;
• Condition of packaging.

Discrepancies are noted on the Supplier Delivery Docket and the Supplier Delivery Docket is signed. The supplier invoices are checked against the supplier delivery docket/ P.O.

Control of Assets

The General Manager and Branch Manager, in conjunction with the COO where applicable, is responsible for the compilation of an Asset register for Oasis (Belfast) and Oasis (Dublin). The Register shall identify assets in the following categories,

- Information
- Hardware
- Software

The Register shall classify all assets and assign ownership of these (as defined within ISO27001).

The General Manager and Branch Manager is responsible for the monitoring of asset management and for the addition of assets and secure disposal of assets as required.

Asset owners shall ensure the secure handling of assets and in particular the transport, handling and storage of the confidential documents in a secure manner.

The Asset Register shall be reviewed and updated on at least an annual basis by the Management Team.
IP09 IDENTIFICATION OF CUSTOMER REQUIREMENTS

1 Scope

This procedure covers the preparation and submission of all estimates and tenders within the Company, and the review and acceptance of all orders.

2 Purpose

The purpose of the procedure is to ensure that all estimates and tenders are prepared in a consistent format, and that all orders are reviewed prior to acceptance.

3 Responsibility

It is the responsibility of the Account Manager to ensure all enquiries are dealt with and all orders reviewed upon receipt to ensure customer requirements have been adequately identified and that orders can be met to the customers’ satisfaction.

4 Related Documentation

• Sales Procedures

5 Procedures

Sales & Marketing
Sales and marketing is managed in accordance with the Sales & Marketing Process Document No. 4/2.

Identification of Customer Requirements
Customer requirements are identified in accordance with the Sales & Marketing Procedure Document No. 4/2.

Customer accounts are set up in accordance with Account Creation/ Box storage Procedure & Vault Storage Document No’s. 4/3 and 4/3 V.

Orders
Orders/ requisitions are received in accordance with the Maintaining Service Level Agreements Procedure Document No. 4/4.

Customer Complaints
Customer complaints/Non-conformances are dealt with in accordance with the Non-Conformance Issues Procedure Document No. 4/5.
IP10 SECURITY ARRANGEMENTS

1 Scope

This procedure covers the Security arrangements maintained by the Company.

2 Purpose

The purpose of the procedure is to ensure that adequate arrangements are in place so that customer requirements are achieved to the customers’ satisfaction.

3 Responsibility

It is the responsibility of the operations staff to ensure that this procedure is adhered to.

Information Security Infrastructure

Management Information Security Forum

There is an Information Security forum consisting of the Operations Manager, the Sales and Marketing Manager, Accounts Manager and the COO. The COO chairs the forum. This forum meets monthly as part of the monthly Management Meeting. Minutes detailing items discussed and decisions made are kept.

Security measures are co-ordinated through the management forum. The responsibilities for the protection of individual assets are defined in the Assets Register.

New installations and major changes to the IT facilitates are approved and authorized by the Security Manager and the IT Consultant. Independent advice is sought from an independent IT Consultant. The Independent Consultant advises on Security threats.

The implementation and organization of Security is independently reviewed.

Information Security Co-ordination

Security Manager (General Manager (Dublin) and Branch Manager (Belfast))

The Security Manager is responsible to oversee all Information Security activities and provide the co-ordination of all facets of the Information Security under managerial control.
The Security Managers principle activities, will include:

- Establishing a management Security forum.
- Undertaking risk assessments
- Establishing controls.
- Recording Security incidents.
- Reporting to the management forum on progress, incidents, Security status and current threats.
- Carrying out Security reviews.
- Monitoring compliance with the IMS system.
- Setting up and removing users on the system, monitoring the system, preparing Security procedures, managing change control and data back-up, implementing applicable internal controls, implementing and testing application fallback with the assistance with IT Providers.

General Manager of Operations
The Security Manager is responsible for issuing passwords to the O’Neills system and for the issue and control Access Control swipes cards. He is responsible for the control of the Access control system. He is responsible for the system back up rotation.

The General Manager of Each Branch and Director of Account Management of Finance
The General Manager of Each Branch is responsible for maintaining and ensuring the confidentiality of employee information. The Director of Account Management of Finance is responsible for maintaining the Security of accounting information. This involves password control, physical access control of the filing cabinets, and restricted access to offices.

4 Related Documentation

- Purviews
- Confidentiality Agreements
- Back-up logs
- Access Control records

5 Procedure

Physical and Environmental Security

Security of Data Centres and Computer Rooms
The server containing all databases is located in the Hub room, which has a cooling fan. This room is locked and is secured by four access control doors. All of the PCs are within access-controlled areas. There is a clear desk policy.
Physical Security Perimeter and Physical Entry Controls
All areas are access controlled. To access the vault and operations room, a PIN and a swipe card is required. There are a number of physical domains which area access controlled by either PIN or Swipe cards. Entry and exit is recorded through the swipe control system.

Isolated Delivery and Loading Areas
Deliveries and Collections of client’s data is undertaken by the Company personnel. These items are held in Incoming/Outgoing holding areas within the secure car-parking area. These are validated before acceptance into secure Warehouse or Vault areas. Vehicles are never opened while the main roller shutter is open.

Collection of client data is controlled through the generation of a works order. Collections are limited to client-authorised personnel who are required to sign the works order.

Third party collections: Items for collection by third parties are left in the lobby.

Third party deliveries: All deliveries held in the lobby until they are checked against the Purchase Order.

Clear Desk Policy
There is a clear desk policy – defined in Purviews and breach of it is a disciplinary offence.

Removal of Property
Removal of property such as equipment, data, software and documentation belonging to the organisation requires authorisation.

Removal of laptops and organisation documentation is limited to management.

Equipment Security

Equipment Location and Protection
The Network Server is sited in a clean, sealed Hub Room. Telephone equipment and alarms controls are also located in the Hub Room. Four swipe card locks, two requiring pin codes, restrict access. This room is sealed and the environmental conditions are suitable i.e. dry and clean. There are no major sources of electromagnetic interference.
The Security PC’s and equipment are stored in a cabinet, secured behind two locked doors. There is an air-cooling system and access is limited authorised personnel only.

**Power Supplies**
There is a UPS system in place to protect against power surges and power loss, allowing for a safe shutdown. A generator is contracted to be available through the Company’s electricians.

**Cabling Security**
Power and telecommunications cabling is protected from interception or damage. All cables are trunked. No sensitive information is transmitted by cable.

**Equipment Maintenance**
There are service maintenance agreements with service providers in place for all critical pieces of equipment. There are preventive maintenance programmes in place. These maintenance service providers keep records of maintenance.

**Security of Equipment – Off-site**
Mobile phones are used for after hours emergency call outs would affect business continuity – the on-call mobile is a backed up through a pager. Phones should never be left unattended. Our telecommunications agent can cancel the SIM number and re-issue a replacement with the same number, within 2 hours.

Driver PDT and MC50 Scanners are never left unattended.

The roller shutter zappers pose a risk of unauthorised access. In the event of a lost zapper, the electrician can recode system.

Shutter Keys are issued to all personnel with the authority to lock-up and are never left unattended.

Unattended vehicles pose a risk of loss of client information. All vehicles automatically alarm and disable.

Laptops pose a risk of access to sensitive information such as leads. Laptops and software are password protected. Data is synchronised with main system.

**External, physical Security:** The perimeter and roof are have both CCTV and infrared beams integrated into the alarm systems and are centrally monitored 24 hrs, 365 days.

**Secure Disposal of Equipment**
In the event of disposal all memory of PCs are wiped and PC’s are professionally destroyed. Similarly, any media containing sensitive data is professionally destroyed.

Computer and Network Management

Documented Operating Procedures

There are Operating Manuals available for all computer applications.

An approved subcontractor carries out the network management and maintenance.

O'Neils Software undertake maintenance and support and regular upgrades of the Operations Software.

The daily management of the O'Neils Software is detailed in the Operations, Customer Service and Accounts Procedures together with the Operations and Administration Operating Manuals.

Daily management and use of the Operations Software is restricted by password access control.

The Customer Services Manager is responsible for making any administrative changes, including account creation, invoicing scheduling. The Operations Manager is responsible for making any operational changes including adding new users, access control and work scheduling.

Compliance with the requirements of ISO 27001 is specified in the contract. This includes documented procedures for the management and maintenance of the network.

No development or testing is carried out
IP11  STORAGE AND RETRIEVAL OF DOCUMENTS

1  Scope

This procedure covers all activities carried out by the Company in relation to the collection, storage and retrieval of confidential documentation.

2  Purpose

The purpose of the procedure is to ensure that document storage and retrieval activities are carried out with the utmost Security and to the customers’ requirements.

3  Responsibility

It is the responsibility of the Operations Manager to ensure adherence to this procedure.

4  Related Documentation

- Operational Procedures

5  Procedure

Operations Control

Work Environment

Records are stored in accordance with PRISM (Professional Records & Information Systems Management) recommendations:

Magnetic Media Vault:

<table>
<thead>
<tr>
<th></th>
<th>PRISM</th>
<th>Bow Lane Vault</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature</td>
<td>62-68°F (16.6-20°C)</td>
<td>19.6°C</td>
</tr>
<tr>
<td>Relative Humidity</td>
<td>40-50%</td>
<td>45%</td>
</tr>
</tbody>
</table>

These conditions are monitored 24 hrs, 365 days, by the thermo-hydrograph. Printouts of data are retained only as required.

Identification and Trace-ability

Bar Codes are allocated to clients in accordance with Bar Code Allocation Procedure Document No. OP05
Boxes/files for storage are bar coded by the client in accordance with the Bar coding Guidelines and box/ file transmittal sheet (Dublin). Media is bar coded by Oasis Group in accordance with the Media Creation Procedure Document No. OP16

Media is scanned into a location in accordance with the Box Movement Procedure. OP06

The contents of boxes are entered into the computer system in accordance with Data Entry Procedure Document No. OP09 & OP14

The status of material for storage during transit is monitored through the PDT / MC50 Scanners in accordance with the Driver Scanner. The status of material for storage while in the Depository is indicated by the database in accordance with the Box Movement Procedure Document No. OP06 & OP13

**Customer Property**

On receipt, customer property is checked for condition/ suitability of boxes. If deemed unsuitably boxed, the customer is informed and given an option to re-box or instruct Oasis to re-box. The material is identified in accordance with the Box Movement Procedure.

Material is safeguarded whilst in storage in accordance with the Structure and Infrastructure Procedure. In the event that customer property is lost or damaged the customer is informed. This would be recorded with in accordance with the Non Conformance Procedure.

**Preservation of Product**

The preservation of product during transit and internal processing is detailed in the Box movement In/ Box Procedure.

**Compliance with Legal Requirements**

Relevant legislation is identified and reviewed to identify the Company’s obligations:

- Freedom of Information Act
- Software Act
- Data Protection Act

The controls required to comply with these obligations are relative to information maintained relative to personnel and Company accounts.

Client data under the jurisdiction of the FoI Act or Software Act would be the sole responsibility of the Client.
**Compliance with Security Policy**

Security reviews are carried out on an ongoing basis against the controls outlined in the Risk assessment and Asset Register and the controls detailed in this Information Security Manual. This covers IT facilities and all other areas covered by the scope of this system.

**Technical Conformity Checking**

An independent IT Support Company reviews the Company’s IT facilities.
IP12  **EQUIPMENT MAINTENANCE AND CALIBRATION**

1  **Scope**

This procedure covers the controls exercised over the calibration system operated by the Company and also outlines how Company vehicles are maintained in a manner to ensure that they are able to carry out their required function.

2  **Purpose**

This procedure will apply to all inspection, measuring and test equipment required to verify service Quality. This procedure is also to ensure all vehicles are maintained in a roadworthy condition and safe from damage, deterioration or theft.

3  **Responsibilities**

The General Manager and Branch Manager has overall responsibility for ensuring that adequate monitoring and measurement is carried out and for ensuring adequate control is maintained over the equipment. The General Manager and Branch Manager may designate suitable staff for this purpose.

4  **Related Documentation**

- Calibration records
- Service reports

5  **Procedure**

**Calibration & Statutory Inspections**

The Operations Manager is responsible for the operation of the calibration system within the Company. They will maintain a list of all equipment, which is subject to calibration and the frequency of calibration required.

Equipment will be calibrated by recognised external test houses.

Each piece of calibrated equipment will be identified with a label indicating its calibration status, certificates will also be held.

Items failing calibration shall be reported to the General Manager or Branch Manager as appropriate, and any corrective actions taken to ensure the reliability of past measurements.
Liebert Air Conditioning & Humidifier

This piece of equipment is serviced quarterly by the authorised service agent and adjusted if necessary. This system has a tamper control password.

Equipment maintenance is defined in the Facility Structure and Infrastructure Document No. 3/8. (Asset Register)

Control of Vehicles

Vehicle maintenance is carried out on a scheduled basis. In Belfast, records of vehicle servicing are held by the leasing company, although in Dublin, service records are maintained by the Transport Manager.

The Transport Manager retains a file for each vehicle operated by from the Oasis (Dublin). This file contains details of all servicing and repair carried out on each vehicle.

Vehicles are required to be kept in a clean and tidy manner at all times. All vehicles are regularly washed by the technicians as required. There should be no unsecured tools or equipment in the cab of the vehicle.

Each vehicle undergoes an annual service prior to its PSV and a major service approximately every 35,000 kilometres. The driver of the vehicle can also request maintenance at any time.

It is the responsibility of the driver to check the vehicle before use and ensure that it is in safe working order. The flower method should be used (Fuel, Lights, Oil, Water, Electrics & Rubber).

Any vehicle defects should be reported immediately to the relevant Manager, he will log the defect and take the necessary action. At no time should a defective vehicle be driven.
IP13  EMERGENCY AND CONTINGENCY PLAN

1  Scope

This procedure covers the following principal activities:

- Fire emergency situations
- Security breaches
- Bomb threats
- Explosions

2  Purpose

To ensure that in the event of an emergency evacuation, a fire or Security breach the Company has an effective emergency plan and contingency plan in place.

3  Responsibilities

All employees are expected to be familiar with and adhere to the requirements of this procedure.

4  Related Documentation

- Fire Drill Record Form
- Fire Safety Compliance Check sheet
- Fire Fighting Equipment Record
- GPS Vehicle tracking system
- Emergency Response booklets
- Business Continuity Plan
- Contingency Plan Drill Record

5  Procedure

All employees are made aware of the fire evacuation procedure. Fire drills are performed twice a year. An induction presentation also given to all new starts.

Evacuation Procedure

In the event of an evacuation from the site the alarm shall be raised and all employees and persons on site are to follow the instructions given by Senior Management.

When a situation arises requiring evacuation of the Company, the following actions must be adhered to:
• Ensure all employees are aware of the evacuation.
• Commence the Evacuation Procedure. Evacuation points displayed on premises
• Inform all relevant authorities where it is safe to do so.

All employees contractors and site visitors must evacuate the building through the nearest safe escape routes. Ensure all personnel leave in an orderly fashion. When outside, all employees must congregated at the assembly area.

A plan showing the location of fire extinguishers and fire exit points is displayed at various points in the building

The Management Representative or in her absence the Operations Manager shall retain a print off of the clock in system from each morning and shall also retrieve the visitors book for roll-call purposes.

No persons are allowed to re-enter the building unless it has been made safe by the appropriate authority.

Fire Prevention Guidelines

The following are recommendations in the prevention of fires:

• Keep all fire exits clear at all times.
• Keep rooms locked when not in immediate use.
• Keep rubbish in bins in an orderly fashion.
• Always check that fire doors are closed.
• Always check that doors on fire escape routes are unlocked.
• Always report any defective equipment and damage immediately.
• Always report any spillages of flammable material immediately.

Finding A Fire

When a fire is discovered at the Company, the following actions must be adhered to:

• Ensure all employees are aware of the fire.
• Attack the fire with the appropriate appliances only if safe to do so.
• Commence the Evacuation Procedure. Evacuation points displayed on premises
Tackling a Fire

The fire can be tackled, by trained personnel only, if there is no immediate personal danger. The procedure to attack the fire is listed below:

- Switch off power supply in electrical fires (where possible).
- When fighting the fire, the trained employee should position himself between the fire and an escape route.
- Ensure the fire is completely extinguished and not ready to ignite.

Extinguishing appliances are only used for SMALL FIRES, if the fire is getting “out of control”, withdraw, close door and call the fire brigade.

Calling the Fire Brigade

The appropriate employee, (usually the management representative), should call the Fire Brigade. Telephone the Fire Brigade at 999, (where safe to do so). When the Exchange Operator answers, ask for the “FIRE SERVICE”; give the phone number of the Company.

Do not replace the receiver until the information has correctly been received by the operator.

Fire Instruction and Drills

All personnel should be instructed and trained to ensure they understand the fire precautions and the action to be taken in the event of a fire. Fire drills are carried out every 6 months and recorded on the Fire Drill Record Form. All new personnel should receive the training as part of their induction to the Company.

The training should cover the following areas:

- Action to be taken on discovering a fire.
- Action to be taken on hearing the smoke alarm.
- Raising of the fire alarm.
- Calling the Fire Brigade.
- Location, types and use of fire fighting equipment.
- Fire escape routes.
- Closing of fire doors.
- Fire meeting point for employees.

Records should be kept and maintained of the Fire Training.

Fire Fighting Equipment

Fire extinguishers are serviced by a competent authority on an annual basis. Records of these services are held by the Management Representative.
Contingency Planning in the event of a Security Breach

Control of Vehicles

All vehicles are GPS tracked. A tracking unit in each vehicle is linked to a computer map. In the event of a vehicle seizure the vehicle movements may be traced to aid capture. Any confidential material in the vehicle at the time of seizure may be regained within a short period of time. All documents are scanned in on loading the vehicle, which will identify any missing items.

Reports can be generated identifying each vehicle movements', detailing times, locations, stoppages and mileage etc.

For any queries on vehicle movements, reports may be generated, or the vehicle movements replayed on the map for visual presentation.

Control of Site Activities

The storage facility is covered by CCTV which will monitor and record all activities over a 24-hour period.

The estate where the facility is located has a Security barrier with 24 hour guarding.

Bomb Threats/Suspect Packages

In the event of a bomb threat or suspect package leaving discovered all personnel are instructed to notify management immediately and not to examine any suspect packages

The Management Representative or most senior person on the day is to evacuate the facility as in the evacuation procedure listed above

On notifying the relevant authorities all personnel are to remain outside the premises until instructed to return by the most senior member of the emergency services in attendance.

Business Continuity Plan

The COO and Management Team have prepared a Business Continuity Plan in order to ensure the continued operation of services in the event of an emergency.

The nominated Managers shall implement the Business Continuity Plan as agreed by the COO to ensure continued operation of services in the event of prolonged site evacuation.
Measuring the effectiveness of controls

To ensure that the Security requirements of the business are achieved, the Business Continuity Plan shall be tested at planned intervals.

The COO shall, on an annual basis carry out a drill to ensure the successful operation of the contingency plans.

The Management Representative shall maintain a record of the operation of the drill. He shall also record any lessons learned and opportunities for improvement. The achievement of undisrupted operations shall be rated and used as a measure of the effectiveness of the plans.

The results of drills shall be reviewed at the Management review meeting and any corrective or preventive actions agreed as necessary. Such actions may include the amendment to contingency plans or procedures and all personnel shall be instructed on relevant changes.
IP14 VISITOR CONTROL

1 Scope

This procedure covers the control operated over visitors and contractors working on the site.

2 Purpose

The purpose of the procedure is to ensure that all Security risks are minimised and that all visitors and contractors are identified on site.

3 Responsibility

It is the responsibility of the Office staff to ensure all visitors sign in and out of the premises and are accompanied by a member of staff while on site.

It is the responsibility of the Operations Office to ensure that all contractors on site complete and sign a confidentiality agreement defining responsibilities in relation to Security arrangements.

4 Related Documentation

- Visitors Book
- Confidentiality Agreement

5 Procedure

All visitors or contractors on site must report to the office and sign the visitors book on entering and leaving the site.

Where an external party has requested to visit the site the names of the visitors are to be made known to the Company prior to the visit.

The Operations staff maintains all records.

A member of staff accompanies all visitors on site. Under no circumstances may a visitor gain entry to the facility storage area without prior Security checks being carried out.
IP15 Monitoring and Measurement

1 Scope

This procedure details the Integrated Management System monitoring carried out at Oasis Group.

2 Purpose

To ensure that environmental conditions are controlled for the storage of documents and that action is taken when levels exceed acceptable/legislative limits.

To ensure that service delivery not only meets but exceeds the requirements of the Customer.

3 Responsibilities

The Operations Manager is responsible for all environmental monitoring within the Company.

4 Related Documentation

- Prism Guidelines
- Event Log
- Exceptions Report
- Service Level Report

5 Procedure

Environment

The temperature and humidity of storage locations is required to be measured and monitored continuously against the limits specified in the Prism Guidelines. This is achieved through the Liebert Air Conditioning & Humidifier. This is preset with required limits and will sound an alarm if the limits are exceeded and will maintain an Event Log.

Processes

Collection and delivery of boxes is monitored through the scanning of boxes against the Work Order. This will highlight any outstanding collections and deliveries. The O’Neils Software will generate an Exceptions Report for any incomplete transactions.

Compliance with service levels are monitored through the Service Level Report available from O’Neils Software.
Service

The measurement and monitoring of services is detailed in the relevant procedures. The close daily contact with Clients and alertness of all direct contact personnel ensures a constant awareness of a Client’s satisfaction with services provided by Oasis Group.

Analysis of Data

The Management Representative will review the following records as part of the Operations Meeting in order to identify areas for improvement.

- Non-Conformance issues
- Customer Feedback Surveys
- Operational issues
- Projects
- Staff Issues

Review for Improvement – Corrective/Preventative Action

The results of the above analysis are discussed at the Management Meeting. The reason for the non-conformity, potential non-conformity or opportunity for improvement will be investigated and recorded in the minutes. Corrective and/or preventive action will be decided upon and recorded in the minutes. The effectiveness of the corrective and preventive action taken will be assessed at the subsequent management meeting.

Measurement of Customer Satisfaction

Customers are surveyed using the Quality Control Survey form (annually to assess their satisfaction with our product and services. Clients’ activity levels are monitored on an ongoing basis through the O’Neills System.

Customer Services undertake regular Contact Calls, both telephone and site-visit to ensure customer satisfaction. These are done on a minimum of an annual basis.

Account Management Policy

Oasis Group strives to create a synergy with its customers so as to become an extension of their office.
Procedures
The following procedures are followed:

- Commencement of contact:
  - Daily contact to ensure smooth transaction of documents/multimedia.
  - Annual call by phone or in person to ensure service levels are meeting customers expectations.

- The following points are raised at this time:
  - Collections and Deliveries are on time
  - Collections and Deliveries are correct
  - Drivers are polite and courteous
  - Billing is correct and understood
  - Informing the customer of how much storage intake they currently have and enquiring what their expected growth maybe so as we can accommodate them.
  - Ensuring the customer is aware of the full range of services offered by Oasis Group.
  - Updating customer authorisation list
  - Asking customers for any suggestions they might have for improvements.