3.1 General

3.2 Document Management Policy Document

3.2.1 Contents

OutProsys has implemented a policy in order to comply with relevant customer, regulatory and SANS15801:2013 Edition 2 requirements.

It is the policy of OutProsys that all customer documentation whether electronic or hard copy be protected from accidental or intentional unauthorised modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store and transmit that information.

3.2.2 Information Covered:

The policy relates to electronic and hard copy documents received from our customers. Types of customer documents will vary e.g. Membership Loyalty Programme forms, market research questionnaires, surveys and exam papers.

3.2.3 Storage media:

Electronic images of scanned documentation are stored on our server’s hard drives (scanservers, process servers, backup servers and offsite backup server). The backup servers have ZFS file systems.

Customer data is clearly identified on the server i.e. a source image folder within the specific customer folder and accessible to those who have authorised access.

3.2.4 Data file formats and compression:

PNG, JPG and TIF are the approved file formats.

We use a unique file naming system to ensure that all image names remain unique. We do not allow multiple versions of the same image.

3.2.5 Standards related to document management:

Data Protection Policy is incorporated into our ISO 9001 quality management system.

3.2.6 Retention and disposal schedules:

A retention schedule (Process Control Sheet) is maintained for each job. Retention periods are defined by the customer.

3.2.7 Document management responsibilities:

The various procedures and work instructions identify persons/job function responsible for each process.

3.2.8 Compliance with policy:

Head of Finance is responsible for maintaining/monitoring compliance with the policy.

4.1 General

4.1.1 Trusted system

OutProsys has implemented a document management system and is ISO 9001:2015 certified by the BSI Group.

4.1.2 Controls

- Chain of accountability: responsible job function will be indicated on the procedure and work instruction.
- Legislative & regulatory bodies: the various labour, industry and company legislation will be adhered to.
- Technical, procedural, regulatory developments: reviewed on a regular basis
- Information security and confidentiality policy

4.1.3 Segregation of roles

Separation of roles provide a check on any possible errors. It ensures that physical and managerial separations that exist around a system are mirrored by logical access controls. Separation of roles between initial operations and checking has been implemented and is monitored on an ongoing basis.

From receipt to storage of processed documents, a separation of roles exists, this is indicated by the responsible job function on the relevant procedures and work instructions.

4.2 Information Security Management

4.2.1 Information Security Policy

Refer to PRB-ITD-09-OutProsys Data Protection and Information Security Policy.

Ownership of Software:
All computer software developed by OutProsys's employees or contract personnel on behalf of OutProsys or licensed for OutProsys's use is the property of OutProsys and must not be copied for use at home or any other location, unless otherwise specified by the license agreement.

Installed Software:
All software packages that reside on computers and networks within OutProsys must comply with applicable licencing agreements and restrictions and must comply with OutProsys's acquisition of software policies.

Identification/Authentication:
Unique user identification (user id) and authentication is required for all systems that maintain or access Customer Data. Users will be held accountable for all actions performed on the system with their user id.

a. The following authentication method has been implemented: **strictly** controlled passwords
b. The user must secure his/her authentication password such that it is known only to that user
c. The user must log off or secure the system when leaving it

Data Integrity:
OutProsys adheres to the following methods:
Transaction audit
Encryption of data

Security Breaches:
Assess type of breach and determine the conditions that lead to the breach. Investigate and determine what information was compromised. Take the necessary corrective action and always inform any affected clients.

4.2.2 Risk Assessment

We have undertaken a risk analysis. Our Disaster Recovery Plan identifies any potential risks. Of particular importance are the security measures implemented to control the information storage media, which are our servers. Risk analysis includes vulnerability risk factors.

Refer to Disaster Recovery Plan Summary: PRB-ITD-12 -Summary_Disaster_Recovery_Plan.doc
Refer to Disaster Recovery Plan: PRB-ITD_10_Ops_Disaster_Recovery_Plan.xls
Refer to FMD-ITD-130-Security_Implementation_Checklist.

4.2.3 Information Security Framework

Management framework has been established to initiate and control the implementation of information security. The framework has the following objectives:

- Approval & review of information security policy
- Monitoring of threats to information security
- Monitoring and review of security breaches
- Approval of major initiatives to enhance information security

Approval, review and monitoring takes place at IT meetings and annual ISO 9001 management review meetings.

4.3 Business Continuity Planning

Refer to PRB-ITD-10_Ops_Disaster_Recovery_&_Business_Continuity_Plan
Refer to PRB-ITD-12 -Summary_Disaster_Recovery_&_Business_Continuity_Plan.

4.4 Consultations

If required, OutProsys consults with relevant regulatory, government, external audit bodies, legal advisors and experts in the field of information technology.

OutProsys has implemented a document management system and is ISO 9001:2015 certified by the BSI Group.

5.1 General

5.2 Procedures Manual

5.2.1 Documentation

OutProsys has an established document management system containing documented procedures and work instructions.

5.2.2 Content

Procedure Manual include:

- Information capture: refer: PRB-HOP-15-Receipt&Prep.docx
- Document image capture refer: PRB-HOP-16-Scanning.doc
- Data capture refer: PRB-HOP-02-SP7 Manual Data Capture.doc
- Indexing refer: PRB-HOP-02-SP7 Manual Data Capture.doc
- Authenticated output procedures (refer to 5.7)
- File transmission (refer to 5.8)
- Document retention (refer to 5.9)
- Information preservation (refer 5.10)
- Information destruction (refer to 5.11)

- Back up & system recovery (refer to 5.12 and PRB-ITD-07 Back up procedure)
- System Maintenance (refer to 5.13 and PRB-HOP-17-Scanner_Maintenance.doc)
- Security & Protection (refer to 5.14 and PRB-ITD-09-OutProsys_Data Protection Policy)
- Use of contracted services (refer to 5.15)
- Workflow (refer to 5.16)
- Date and time stamps (refer to 5.17)
- Version control (refer to 5.18)
- Maintenance of documentation (refer to 5.19)
- Scanner Maintenance refer: PRB-HOP-17-Scanner_Maintenance.doc
- Pre & Post Processing: refer PRB-HOP-01 Pre-process, PRB-ITD-02 Post process, PRB-ITD-04 Programme Customisation, PRB-ITD-03 Defining pre process, PRB-ITD-05 Defining de format specification, PRB-ITD-06 Defining post process specification and relevant work instruction I:\ISO9001\C-Works Instruction Manual\Hopkins
- Project specific work instructions: refer to relevant work instruction I:\ISO9001\C-Works Instruction Manual\Hopkins
- Web Portal refer: PRB-ITD-13-Web_Portal.doc
- Storage & Destruction refer: PRB-HOP-03-Procedure for control of customer property.doc
- Audit Trail refer: 7.2.2

5.2.3 Compliance with Procedures

Staff are made aware of procedures and receive adequate training, by means of the ISO 9001 quality management system or project specific training.

5.2.4 Updating and Reviews

If any changes are made they will be documented, the same procedure used in ISO 9001:2015 for updating and reviewing procedures is followed.

Refer: QMA-PRO-01-Document Control Procedure.doc

5.3 Information Capture

Refer:
PRB-HOP-15-Receipt&Prep
PRB-HOP-16-Scanning
PRB-HOP-02-SP7 Manual Data Capture.doc
Capture rules refer: relevant customer work instruction I:\ISO9001\C-Works Instruction Manual\Hopkins

5.3.2 Information Loss

Refer to PRB-ITD-09-OutProsys Data Protection and Information Security Policy

5.3.3 Creation and importing

All scanned documents have an automated audit trail built into the scan application.

5.3.4 Metadata

All scanned documents have an automated audit trail built into the scan application.

5.4 Document Image Capture

Refer:
PRB-HOP-15-Receipt&Prep

PRB-HOP-16-Scanning
PRB-HOP-02-SP7 Manual Data Capture.doc
Capture rules refer: relevant customer work instruction I:\ISO9001\C-Works Instruction Manual\Hopkins

5.4.2 Preparation of Documents

Refer: PRB-HOP-15-Receipt&Prep

5.4.3 Document Batching

Refer: PRB-HOP-15-Receipt&Prep.docx

5.4.4 Photocopying

Refer: PRB-HOP-15-Receipt&Prep.docx

5.4.5 Scanning Processes

Refer: PRB-HOP-16-Scanning.doc

5.4.6 Quality Control

5.4.6.1 Sample set

Refer: PRB-HOP-16-Scanning.doc (scan operator checks image quality)
Refer: PRB-HOP-02-SP7 Manual Data Capture.doc (double capture process is also used to identify poor quality images)

5.4.6.2 Evaluating Image Quality

Refer: PRB-HOP-16-Scanning.doc (scan operator checks image quality)
Refer: PRB-HOP-02-SP7 Manual Data Capture.doc (double capture process is also used to identify poor quality images)

5.4.6.3 Checking Scanner Performance

Refer: PRB-HOP-17-Scanner_Maintenance.doc

5.4.7 Rescanning

Refer: PRB-HOP-16-Scanning.doc and PRB-HOP-02-SP7 Manual Data Capture.doc procedures.

5.4.8 Image Processing

Refer:
PRB-HOP-15-Receipt&Prep.docx
PRB-HOP-16-Scanning.doc
PRB-HOP-01 – SP6 Pre Process
PRB-HOP-02-SP7 Manual Data Capture.doc

Job specific pre-processing requirements are defined on the job specific work instruction.
Refer: I:\ISO9001\C-Works Instruction Manual\Hopkins

5.5 Data Capture

5.5.1 New Data

Refer: PRB-HOP-02-SP7 Manual Data Capture.doc

Unless specified by the client, all work is double captured to ensure the highest levels of accuracy.

5.5.2 Conversion and Migration

Job specific work instructions will indicate how we receive the documents, whether electronic or hard copy. If images are received electronically they are securely uploaded to our servers where they are recorded and backed up. The customer will indicate the number of images they have sent so that we can reconcile and ensure that we have received all the images.

5.6 Indexing

Refer to PRB-HOP-02-SP7 Manual Data Capture.doc
Unless specified by the client, all work is double captured to ensure the highest levels of accuracy.

5.6.1 General

Refer: PRB-HOP-02-SP7 Manual Data Capture.doc procedures.

5.6.2 Manual Indexing

Refer: PRB-HOP-02-SP7 Manual Data Capture.doc procedures.

5.6.3 Automatic Indexing

When required Barcode recognition software is either performed using approved handheld barcode scanners if we are scanning hard copies.

Electronic barcode recognition is performed using zbar software (http://zbar.sourceforge.net/)

5.6.4 Index Storage

Index data is retained for at least as long as the source images it relates to is retained.

5.6.5 Index Amendments

All data amendments in the original defiles are done by Technical Coordinator or Head of Operations and the work is then recombined and exported. A copy of the file is always made and archived before making any amendments.

5.6.6 Index Accuracy

Refer: PRB-HOP-02-SP7 Manual Data Capture.doc procedures.
Unless specified by the client, all work is double captured to ensure the highest levels of accuracy.

5.7 Authenticated Output Procedures

Post process and export procedures vary according to customer requirements. Export format is defined by the customer.

5.8 File Transmission

5.8.1 Intra-system Data File Transfer

5.8.1.1 General

Intra-system file transfers include:

- Local area network transmissions
- Movement between storage sub-systems under system control
- Transfer between storage sub-systems under operator control

5.8.1.2 Local Area Network Submission

The authorised administrator transfers files (if necessary) via a local area network or between remote locations via a fixed communication line.

5.8.2 External Transmission of Files

We maintain a direct private Ethernet link with our offsite backup server. All data transmissions are encrypted. File transmissions via rsync over SSH (encrypted). Clients access to files are on sFTP.

5.9 Document Retention

Retention periods are defined by the customer.

5.10 Information Preservation

Retention periods are defined by the customer.

5.11 Information Destruction

Refer: PRB-HOP-03-Procedure for control of customer property.doc

5.12 Backup and System Recovery

Backup refer: PRB-ITD-07 Backup procedure
System recovery refer: PRB-ITD-07 Backup procedure

5.13 System Maintenance

Refer: PRB-HOP-17-Scanner_Maintenance.doc

5.13.1 General

Refer: Maintenance log – FMD-HOP-210-Weekly Scanner Cleaning Checklist.xls

5.13.2 Scanning Systems

Refer: PRB-HOP-16-Scanning.doc

In order to ensure the consistency of our scanned image quality, our scan operators perform checks on the image quality throughout the scanning process and all images go through a combination of electronic quality check and a double capture index process where image quality is again verified. Poor quality images are rescanned.

5.14 Security and Protection

5.14.1 Security Procedures

Refer: PRB-ITD-09-OutProsys Data Protection and Information Security Policy

Key Operational Security Controls

- Training of staff in respect of security and confidentiality
- Restricted access via User names, passwords and SSH keys
- Backup, Archiving and Shredding systems tested, maintained and documented
- Restricted access to Customer Data and Documents
- Restricted access to the Building and Storerooms

5.14.2 Encryption Keys

Authorised SSH keys and passwords are used to access the servers with client images and data.

5.15 Use of Contracted Services

5.15.1 General

We do not outsource scanning, if our data capture service is outsourced, the supplier only performs single capture and OutProsys performs the double capture process to verify the quality of all characters.

5.15.2 Procedural Considerations

Images are securely uploaded to the supplier servers (Rsync over SSH). The outsource control sheet located \\eric.outprosys.com\OutSource_Control_Sheet.xls is updated to reflect date sent, quantity of images sent, file name, quantity of de files and quantity of records sent. Once it has been processed by the supplier, it is updated with date received, quantity de files and quantity of records received. Differences in de files and records sent and received are noted and investigated.

5.15.3 Transportation of Paper Documents

Usually the customer will arrange for delivery or collection of documents to and from our premises. When transportation is arranged by OutProsys a reputable courier supplier on our approved supplier list will be used.

5.15.4 Use of Trusted Third Party

N/A

5.16 Workflow

Refer: I:\ISO9001 for various procedures & work instructions
Refer: QMA-PRO-01-Document Control Procedure.doc

5.17 Date and Time Stamps

The scan server check system clocks on a daily basis.

5.18 Version Control

5.18.1 Information

Change control procedures – same as ISO 9001
Refer: QMA-PRO-01-Document Control Procedure.doc

5.18.2 Documentation

Change control procedures – same as ISO 9001
Refer: QMA-PRO-01-Document Control Procedure.doc

5.18.3 Procedures and Processes

Change control procedures – same as ISO 9001
Refer: QMA-PRO-01-Document Control Procedure.doc

5.19 Maintenance of Documentation

Review of documentation (annual review as done with ISO 9001)
Change control procedures – same as ISO 9001
Refer: QMA-PRO-01-Document Control Procedure.doc

6 Enabling Technologies

6.2 System Description Manual

Hardware:
Refer: PRB-ITD-16-OPs_Network.xls
Software:
Refer: FMD-ITD-030-Software Register.xls
Configurations:
Refer: PRB-ITD-16-OPs_Network.xls

6.3 Storage Media and Sub-system Considerations

Only authorised staff have access to enter or amend stored information.

6.4 Access Levels

Physical access controls: server room has a code lock
Electronic access controls: Username, password and SSH Keys

Authorised personnel:

- System Manager = Director: Jason Love
- System Administrator = Aragon
- System Maintenance = System Engineers, Louis & Aragon
- Authors or originators = System Engineers, Louis & Aragon
- Information Storage & Indexing = System Engineers, Louis & Aragon
- Information Retrieval = System Engineers, Louis & Aragon

6.5 System Integrity Checks

6.5.1 General

We have uninterrupted power supply to the operations through a combination of an onsite battery inverter system, UPS (Uninterruptible Power Source) and a 50 KVA standby Generator which can keep us operational in the event of complete power loss to the building for an unlimited period of time.

6.5.2 Digital and Electronic Signatures (including biometric signatures)

N/A

6.6 Image Processing

Image resolution is defined per job, tested and approved. Vectors are used for auto-rotation. Scanning is done in either simplex/duplex depending on the job requirements.

Refer: PRB-HOP-16-Scanning.doc

6.7 Compression Techniques

Images are scanned into one of our approved file formats.

6.8 Form Overlays and Form Removal

Image quality issues are identified either during scanning, our electronic image check or double capture process and then rescanned.

6.9 Environmental Considerations

Equipment user manuals are either stored electronically I:\ISO9001\F-External Docs Manual or hard copy documents are kept on file.

Computer servers are stored in a secure server room with codelock access; the room has an air conditioner with an option to switch to battery power to ensure backup and that a regulated temperature is maintained. There is also a smoke detector linked to our alarm system should there be a fire. If the temperature rises above a predetermined level, an automated email is sent every hour to authorised personnel to alert them so that the necessary action can be taken.

6.10 Migration

Refer: PRB-ITD-15-DRBD Disk Replacement.docx

6.11 Information Deletion and/or Expungement

Appropriate authorisation is obtained if information needs to be deleted. A record deletion approval is maintained.

7. Audit trails

7.1 General

7.1.1 Audit Trail Data

Various control sheets form part of the audit trail.
Manual audit trail: documents are logged on control sheets from prep to scan to store.
Electronic audit trail: when the document is scanned it automatically gets its date, filename, customer, job, count recorded in a database with a backup copy created and maintained.

7.1.2 Creation

All scanned documents have an automated audit trail built into the scan application.

7.1.3 Date and Time

All scanned images have a date & time stamps, this forms part of the audit trail.

7.1.4 Storage

Manual: Refer to form distribution, which will indicate location of records
Automated: Authorised personnel can access audit trails i.e. date and time stamps
Manual: Hard copy forms will be stored in a secure location
Automated: Audit trail data will be stored on our main file server with backups maintained on the offsite backup server.

7.1.5 Access

Only authorised staff have access.

7.1.6 Security and Protection

Security and protection methods will be followed as outlined in the PRB-ITD-09-OutProsys_Data Protection Policy

7.2 System

7.2.1 General

7.2.2 Audit Trail Information

Types
Receipt of hard copy documents: Processing Control Sheet
Prepping of hard copy documents: Prep & Scan Control Sheet
Scanning of hard copy documents: Prep & Scan Control Sheet
Scanning of hard copy documents: Date & time stamp (automatically created)

Storage
Manual: prep & scan control sheets and operator time sheets
Automated: time, date stamps and done files

Security & Protection
Manual: Hard copy forms will be stored in a secure location
Automated: Audit trail data will be stored on our main file server with backups maintained on the offsite backup server.
The same security & protection methods will be followed as outlined in the PRB-ITD-09-OutProsys_Data Protection Policy

Scanned document information

The following audit trail information is stored, where data is scanned on a batch basis:

1. Unique document identifier (filename)
2. Date and time stamp
3. Customer
4. Job
5. Number of pages scanned
6. Scanner used
7. File format
8. Scan operator
9. Batch quantity

10. Size of file

7.2.3 Migration and Conversion

Where information is moved from one storage device to another, details of the move are stored in the audit trail.

7.3 Store Information

7.3.1 General

7.3.2 Information Capture

Key information is kept in the audit trail.

7.3.2.2 File Information

The following audit trail information is stored, where data is scanned on a batch basis:

1. Unique document identifier (filename)
2. Date and time stamp
3. Customer
4. Job
5. Number of pages scanned
6. Scanner used
7. File format
8. Scan operator
9. Batch quantity
10. Size of file

7.3.2.3 Scanned Document Information

The following audit trail information is stored, where data is scanned on a batch basis:

1. Unique document identifier (filename)
2. Date and time stamp
3. Customer
4. Job
5. Number of pages scanned
6. Scanner used
7. File format
8. Scan operator
9. Batch quantity
10. Size of file

7.3.3 Batch Information

The following audit trail information is stored, where data is scanned on a batch basis:

1. Unique document identifier (filename)
2. Date and time stamp
3. Customer
4. Job
5. Number of pages scanned

6. Scanner used
7. File format
8. Scan operator
9. Batch quantity
10. Size of file

7.3.4 Indexing

Audit trail data includes date and time of creation and any modifications. Where amended or deleted audit trail data is generated.

7.3.5 Change Control

Audi trail data is created and stored, where a change is made to stored information.

7.3.6 Digital Signatures

N/A

7.3.7 Destruction of Information

An audit trail is kept of the deduction of source document following scanning, date of shredding is recorded on the Prep & Scan Control Sheet.

7.3.8 Workflow

Refer to 7.2.2