# ISMS Policy Document

## 1) Introduction

This document is ISMS Policy Document of SG Systems Global. The document is controlled by and is the property of SG Systems Global. This version Is Issue 1.

The purpose of the ISMS Policy Document is to provide an overview of the Company, the activities it carries out and the quality standards of operation it conforms to. It is not designed to act as a procedure manual, although it does carry information about where procedures information is located and the detailed information on Documentation Requirements for essential procedures.

## 2) Issue Status

The issue status is indicated by the version number in the footer of this document. It identifies the issue status of this ISMS Policy Document. When any part of this ISMS Policy Document is amended, a record is made in the Amendment Log shown below. The ISMS Policy Document can be fully revised and re-issued at the discretion of the Management Team. The ISMS Policy Document will be reviewed on a Quarterly basis as standard.

| Date | Issue Number | Amendment Details | Changer | Authorized By |
|---|---|---|---|---|
| 28th December 2020 | 1 | 1st Issue Authorized | Michael Burns | Stuart Hunt |
| | | | | |
| | | | | |
| | | | | |

*Information Security Officer (ISO)*

This document refers to the Information Security Officer at multiple points. At the time of writing, this position is taken by the company CFO (Michael Burns).

## 3) Who is SG Systems Global?

*History of SG Systems Global*

The company was founded by Ted Tobolka in 2006, originally focused on manufacturing batch control and traceability solutions. It was in 2015 that SG Systems Global launched its V5 Traceability solution, which is the company's focus. Today the company has by 3 Directors (Stuart Hunt – CEO, Michael Burns – CFO and Simon Hartley CTO).

SG Systems Global is a BDA name for S.G. Systems, LLC and has registered offices in the USA (800749944). The company is privately held (further company information can be found here).

*What is V5 Traceability?*

V5 Traceability is a tradename for a software package typically deployed onsite (see network architecture) although hosted solutions exist in the company's portfolio. Typical solutions consist of

- The hardware (computer terminals, printers, scales, barcode scanners)
- The V5 Traceability software
- Comprehensive reporting suite
- Gateway connectivity app.
- Installation & support

*What does V5 Traceability achieve for businesses?*

V5 Traceability aims to significantly improve manufacturing efficiency while simultaneously offering the company an immediate return on investment though digital traceability and the elimination of scrap batches and wasted ingredients.

*SG Systems Global – Our core values*

The company's values are reflected in all employees and fall into 3 categories (Equality, Improvement & Family)

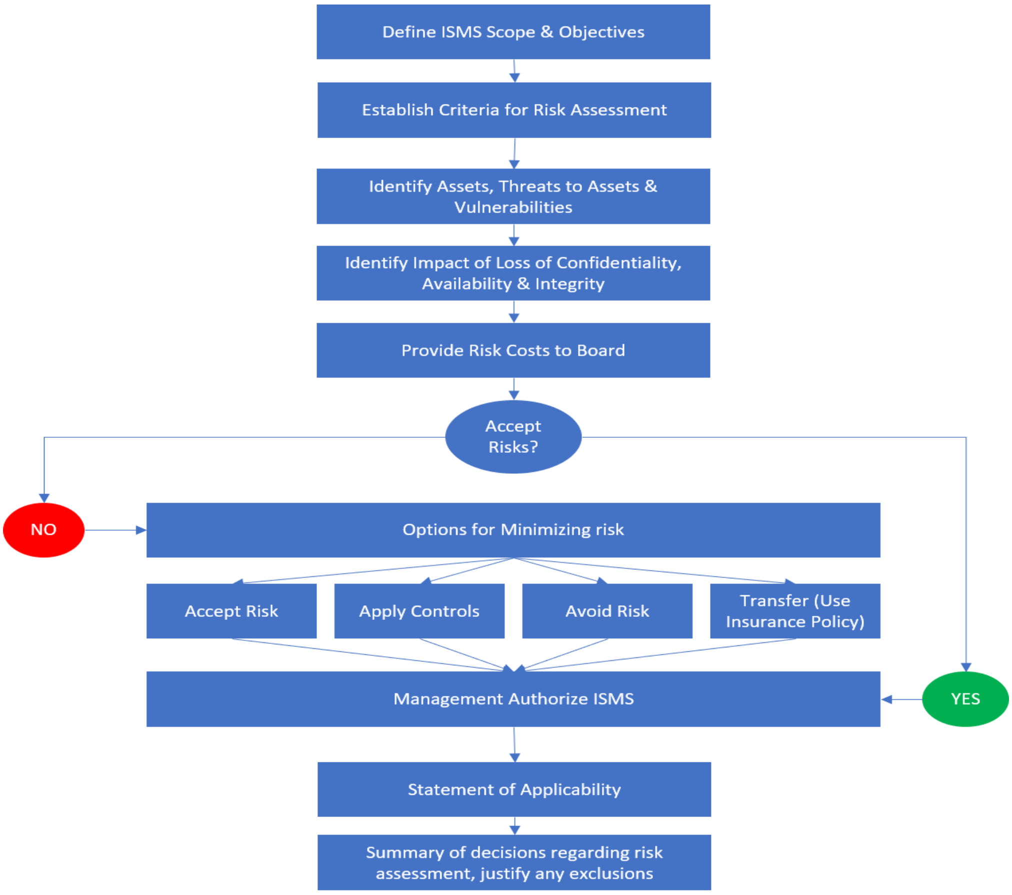
Equality – We value customers and suppliers who treat us as equals. We will give our best efforts to these organisations.
Improvement – We embrace technology and change. We seek to always grow our knowledge for the benefit of ourselves and our partners, and to provide a world-class service.
Family – We seek a happy, motivated team who enjoy being part of the SG Systems Global family – a team that serves our customers with integrity and skill, always.

### 3.1) Registration

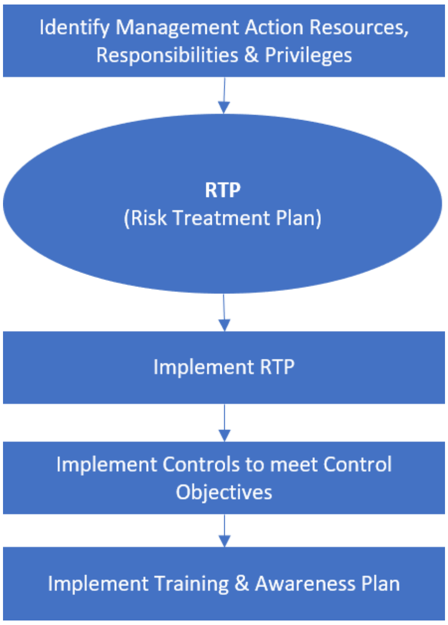
SG Systems Global provides V5 Traceability on a subscription basis to customers in the manufacturing sectors. Typically, Food & Beverage, Plastic & Chemical and large produce sorting and packaging facilities.

## 4) Information Security Management System

This flow chart which details the steps taken and decisions required when establishing an ISMS.


Define ISMS Scope & Objectives
Establish Criteria for Risk Assessment
Identify Assets, Threats to Assets & Vulnerabilities
Identify Impact of Loss of Confidentiality, Availability & Integrity
Provide Risk Costs to Board
Accept Risks?
NO
Options for Minimizing risk
Accept Risk
Apply Controls
Avoid Risk
Transfer (Use Insurance Policy)
Management Authorize ISMS
YES
Statement of Applicability
Summary of decisions regarding risk assessment, justify any exclusions

This flow chart details the steps taken and decisions required when Implementing and operating a RTP (Risk Treatment Plan).


Identify Management Action Resources, Responsibilities & Privileges
RTP
(Risk Treatment Plan)
Implement RTP
Implement Controls to meet Control Objectives
Implement Training & Awareness Plan

SG Systems Global has a commitment to quality and a formal information security management system (ISMS) that addresses the following areas:

- Quality & Performance Monitoring / Reviews
- Policies & Procedures (See Policies)
- Managing external relationships with CRM
- Financial Management (Cash Flow, Balance Sheet, P&L)
- Strategic and business planning
- Human resource development
- Service innovation

## 4.1) DOCUMENTED INFORMATION

### 4.1.1) Documents

All documents (statement of Intent) are maintained and controlled by the Information Security Officer. Policy and procedure documents are reviewed annually. Any documents requiring amendment are updated, authorised, and completed. All updates to documents are signed and dated by the Information Security Officer. Documents are re-issued as an electronic PDF document and a limited number of hard copies are produced. Obsolete documents will be archived in the Dropbox library and restricted by the Information Security Officer; electronic copies of all past versions are kept. All managers hold responsibility for cascading information to staff.

### 4.1.2) Records

All project records (evidence of past performance) are stored in appropriate electronic folders on Dropbox, Salesforce CRM, and managed by respective departments. Hard copies of documents are restricted to a minimum and should not be produced unnecessarily. Electronic records are encouraged over hard copies due to environmental concerns, available storage space and to prevent unnecessary expenditure.

## 5) MANAGEMENT COMMITMENT

### 5.1) Role of Senior Management

SG Systems Global's Senior Management Team are committed to the development and implementation of an Information Security Policy, an Information Security Management System, and to frequently review this system. Responsibility has been assigned to ensure that the ISMS conforms to the requirement of the standard and the provision to report on performance to the senior management team has been defined.

The Information Security Officer will ensure that SG Systems Global staff are aware of the importance of meeting customer as well as statutory and regulatory requirements, and overall, to contribute to achieving SG Systems Global's Information Security Objectives which are aligned with the current business plan. A separate Information Security Policy document is sent to staff annually.

The Senior Management Team is responsible for implementing the ISMS and ensuring the system is understood and complied with at all levels of the organisation. They are responsible for ensuring that;

- The information security policy and objectives are established and in line with the strategic direction of the organisation
- Integration of the ISMS into the organisations processes.
- That resources needed for the ISMS are available
- Communication covering the importance of effective information security management and conformance to the ISMS requirements is in place.
- The ISMS achieves its intended outcome(s)
- The contribution of persons involved in the effectiveness of the ISMS by direction and support.
- Continual V5 Traceability investment is promoted
- Other management roles within their area of responsibility are supported.

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

## 6) ISMS POLICY

### 6.1) Introduction

This document is the Information Security Policy for SG Systems Global. It describes the company's corporate approach to Information Security and details how we address our responsibilities in relation to this vital area of our business. As a company we are committed to satisfy applicable requirements related to information security and the continual V5 Traceability movement of the ISMS.

Information Security is the responsibility of all members of staff, not just the senior management team, and as such all staff should retain an awareness of this policy and its contents and demonstrate a practical application of the key objectives where appropriate in their daily duties.

We also 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 information security management system. These include but not limited to customers and clients and their requirements are documented in contracts, purchase orders and specifications etc.

Verification of compliance with the policy will be verified by a continuous programme of internal audits.

### 6.2) Scope of the Policy

The scope of this policy relates to use of the database and computer systems operated by the company at its office in Dallas, TX, in pursuit of the company's business of providing software as a service across all markets. It also relates where appropriate to external risk sources including functions which are outsourced.

**Integration** – we maintain a number of flow charts which illustrate key business activities and their correspondence to ISMS requirements. See details

### 6.3) Legal and Regulatory Obligations

The scope of this policy relates to legislation outlined in the ISO27001 manual.

### 6.4) Roles and Responsibilities

Our Information Security Manager (This role is carried out by our designated Chief Executive Officer) is responsible for randomly sampling records to ensure that all required data has been captured, and that data is accurate and complete.

It is the responsibility of all staff to ensure that all data is treated with the utmost confidentiality, and that no data is given out without the prior authority of any person affected.

### 6.5) Strategic Approach and Principles

#### 6.5.1) Information Classification

All staff have access to the data stored on the SG Systems Global Office environment and this is structured to have different access and permission levels. Data retrieved from the preformatted forms completed on the web site are automatically attached to the correct fields.

#### 6.5.2) Access Control / Company Passwords

User Accounts are partitioned by access level. With senior management having wider permissions than other employees. There are specifically privileged accounts and therefore there is potential reason for anyone to desire access to another persons account.

Passwords MUST NOT be written down either on paper or retained electronically. Passwords will be changed on a 45 day basis and the last twenty passwords may not be reused according to the password policy of Microsoft's Office 365 platform.

Passwords should be no less than 8 characters in length and consist of both numbers, letters and a special character.

#### 6.5.3) Incident Management

Any and all incidents must be reported immediately in the first instance to the Chief Executive Officer who also fulfils the role of Information Security Manager. (Incident Management Policy)

#### 6.5.4) Physical Security

Access to the office via magnetic swipe card entry via two possible doors. The office building is also manned 24/7 by security personnel or reception staff accordingly.

### 6.5.5) Third-party Access

Access to records is available to only those authorised to view the individual records.

### 6.6) Business Continuity Management

Our telephone system is a hosted IP based one. We use different broadband service providers, so in the event of a failure, we can easily switch to the other provider.

We have an automated backup process as part of our Salesforce and Dropbox subscription, which backs up customer data to multiple data centres across the globe.

### 6.7) Approach to Risk Management

We have carried out a full risk assessment of the potential for a breach of security as documented within our separate Risk Assessment Document.

We aim to reduce all opportunities for data to be compromised. This includes the possibility of theft of data.

### 6.7.1) Action in the event of a policy breach.

Access to internal and customer systems is centrally controlled and removal of access to the system is a simple procedure, which is controlled by the Information Security Manager or by the Head of Customer Services at the request of the Information Security Manager.

Similarly access to the premises is also controlled by the Information Security Manager. Magnetic swipe cards are revoked on cessation of employment and issued on employment commencing.

Immediately a policy breach has been detected any relevant user is either removed or reset depending upon the most appropriate action in the circumstances.

### 6.8) Information Security Objectives

Our objectives are set out in our business plan 2018-2020 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. SG Systems Global's Quality Objectives are as follows:

Objective 1: Existing services - SG Systems Global will continue to deliver its services within a secure environment.

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

### 6.9) Responsibility, authority and communication

The management structure of SG Systems Global is shown as an organisation chart (see **Appendix**) the chart shows functional relationships and responsibilities.

### 6.9.1) Management Representative

The Information Security Officer is responsible for the maintenance, measurement and review of our Information Security Management System. The Information Security Officer will ensure that the processes needed for the Information Security Management System are established, implemented and maintained within SG Systems Global. In addition he/she will report to Senior Management about system performance.

### 6.9.2) Internal Communications

Senior Management utilise SG Systems Global's internal communications framework in order to distribute information about the effectiveness of the Information Security Management System.

Regular security meetings are held internally to discuss appropriate items. SG Systems Global also makes use of google mail and calendar to ensure staff can be notified instantly when in the office or on the move.

### 6.9.3) Implementation

Following the annual audit, results will be collated and disseminated through SG Systems Global's internal communications framework:

## 6.10) Management Review

### 6.10.1) General

Senior Management ensures:

- That the ongoing activities of SG Systems Global are reviewed regularly and that any required corrective action is adequately implemented and reviewed to establish an effective preventative process
- Measurement of SG Systems Global's performance against our declared Information Security Objectives
- That internal audits are conducted regularly to review progress and assist in the investment of processes & procedures. The reviews will be discussed as part of SG Systems Global's SMT meetings.

## 6.11) Review Input

The weekly Security Group meetings review the following information:

- Risk management and the status of risk assessments and treatment plan
- Monitoring and measuring of results including internal audits
- Fulfilment of information security objectives
- Serious untoward incidents
- Status of preventive, non conformances and corrective actions
- Follow up actions from previous management reviews
- Changes in external and internal issues that are relevant to the ISMS
- Recommendations / opportunities for continual investments.
- Feedback from interested parties

### 6.11.1) Implementation

- Meetings are scheduled
- A suggested agenda is prepared by the chair
- Members invited to add items to the agenda
- Agenda is circulated to members
- Meeting take place and actions defined
- Meetings are minuted by a designated staff member
- Minutes are approved by Chair
- Minutes are circulated amongst members
- Completion of actions is reviewed at the next meeting.

## 6.12 Review Output

The Security Group reviews produce the following outputs:

- Policies and procedures are updated to make operations more efficient
- Operations and services are improved through measurement against targets and actions to improve or rectify specific areas.

- Where resources are lacking actions are put in place to rectify this.

### 6.12.1) Implementation

- Corrective actions are identified
- Targets created
- Improvements actioned
- Situation re-evaluated at a specified later date.

## 7) PROVISION OF RESOURCES

SG Systems Global will provide all the resources needed to implement and maintain the Information Security Management System and improve effectiveness of the system. SG Systems Global will also ensure that the resources needed to enhance the satisfaction and requirements of service users, service commissioners and staff are identified and in place through audit and continual review.

### 7.1 Human Resources General

### 7.1.1 Competence, Awareness & Training

We maintain a detailed Training Matrix demonstrating who has received what training and when.

### 7.2 Infrastructure

SG Systems Global's buildings, workspace, and associated utilities are managed by an FM company. The procurement and management of hardware, software and supporting services such as communication and information systems are coordinated by various members of the technical team.

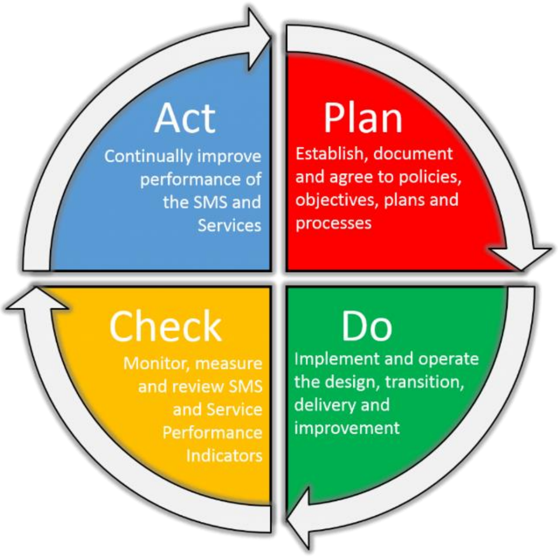
We maintain a detailed asset register, including serial numbers, description and location or person to whom assigned.

### 7.2.1 Implementation

Buildings, workspace and associated utilities requirements are regularly reviewed to ensure we make efficient use of office space. Both hardware and software is reviewed on an ongoing bases to ensure that head office staff are equipped with fit for purpose IT equipment and software.

IT systems are maintained and serviced internally an external IT company in conjunction with the office manager.

Head office prepares and distributes a wide range of information including Management Accounts, Management & Performance information & Training updates.


Act
Continually improve performance of the SMS and Services
Plan
Establish, document and agree to policies, objectives, plans and processes
Check
Monitor, measure and review SMS and Service Performance Indicators
Do
Implement and operate the design, transition, delivery and improvement

## 8) RISK ASSESSMENT METHODOLOGY

We have identified the following process as a means of conducting regular risk assessments relating to Information Security Issues.

Within each of these areas the risks (if any) are identified together with a rating as to the importance of the risk. The associated consequence or severity of the risk is also rated together with the probable likelihood of the risk occurring.

We use an Excel spreadsheet to collect and analyse the risks identified in the following assets / asset groups :

- Buildings, offices, secure rooms security
- Hardware – desktops. Laptops, removable media
- Software applications
- Infrastructure / servers
- Client information and data
- Paper records
- People and reputation
- Key contacts
- Critical third party suppliers
- Utilities

All typical / likely threats have been assessed based on their potential effects on Confidentiality, Integrity and Availability (CIA attributes) using a ratings scale of;

Very Low - 1, Low – 2, Medium – 3, High 4 and Very high – 5 and expressed across key areas of Vulnerability, Probability and Impact

Following this analysis evaluations are drawn as to what the most appropriate action is together with the estimated cost of implementing action to address the identified issue and an estimate of the cost of ignoring the risk. Key evaluation criteria use is 1 – Accept risk, 2 - Apply controls, 3 - Avoid risk, 4 – Transfer the risk.

### 8 .1) Risk Treatment Plan – Statement of Applicability

The approach to our risk treatment plan has been designed and implemented using the main headings within the standard 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.

This document is kept digitally on Dropbox.

## 9) MEASUREMENT, ANALYSIS & IMPROVEMENT

### 9.1) Information Security Standards

In all SG Systems Global's services there are a specific set of quality measurements developed to be used to audit each service to enable a purchaser to be assured of the quality of delivery.

Service Level Agreements (Download Policy) are used to identify the areas of a contract that will be measured and monitored.

### 9.1.1) Implementation

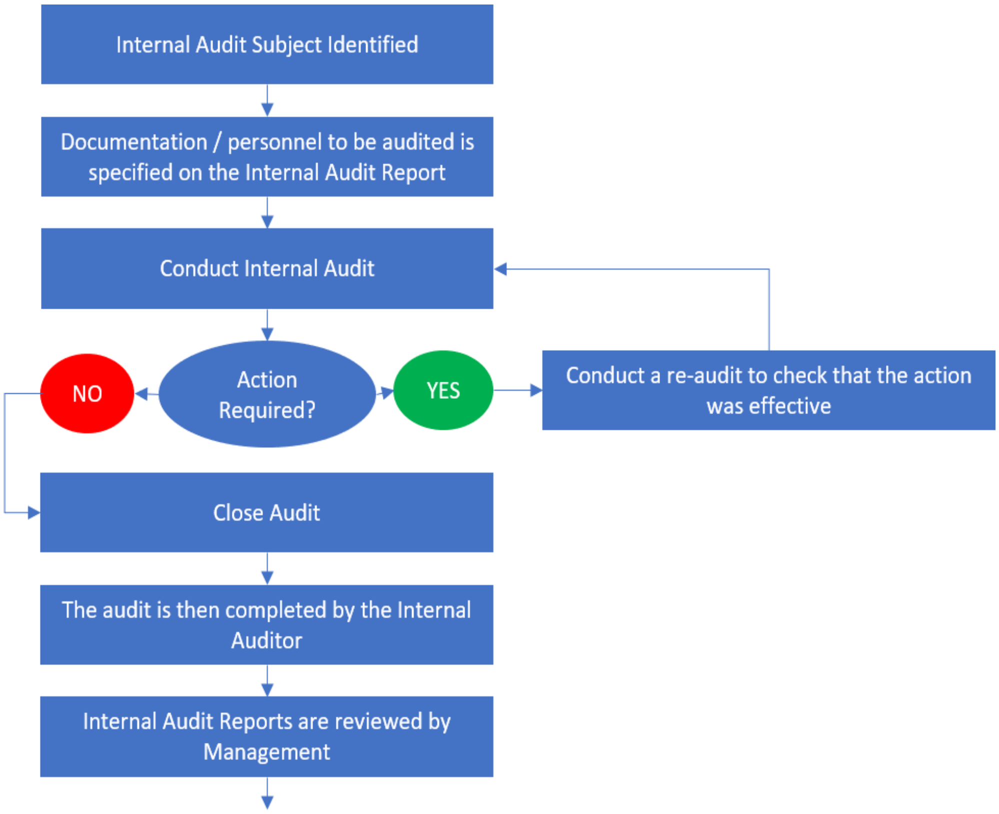
We review our performance as part of a continuous review of Management Information. These reports help us to assess whether we are meeting our performance targets and provide us with month on month business performance benchmarking information. SG Systems Global conducts annual audits, and provides quarterly reports to the Board of Trustees.

All security and implementation matters are reported by the Security Group to the Board, reviewed accordingly and implementation is planned by the Technical Director.

### 9.2) Internal ISMS Audits

The internal audit process is as follows:

### 9.2.1) Internal Audit Process Flowchart


Internal Audit Subject Identified
Documentation / personnel to be audited is specified on the Internal Audit Report
Conduct Internal Audit
NO
Action Required?
YES
Conduct a re-audit to check that the action was effective
Close Audit
The audit is then completed by the Internal Auditor
Internal Audit Reports are reviewed by Management

### 9.3) Monitoring & Measurement of Processes

#### 9.3.1) Implementation

Where the agreed requirements are not met, an action plan clearly detailing compliance will then be agreed with SG Systems Global's CEO with a timescale for compliance set at 6 months with the service commissioner or client.

### 9.4) Monitoring & Measurement of Service

Our approach determines what needs to be measured inclusive of security processes and controls, the methods by which we ensure valid results, the periods and persons involved in conducting this activity and the reporting frequency and the responsibility for analysing and evaluating the results. We retain all documents and records involved in this process.

SG Systems Global establishes at the outset of a new service contract the reporting demands within the Service Level Agreement. This process will be supported with the data reports compiled and will enable the review to monitor performance, effectiveness of delivery, contract compliance and potential service developments. SG Systems Global provides full information for this purpose on a quarterly and annual basis.

### 9.5) Analysis of Data

Incident logs are used to record any Information Security incidents or breaches giving cause for concern, and these are regularly assessed during the weekly Technical meeting to identify areas for improvement.

#### 9.5.1) Implementation

The data is collected by services and submitted to SG Systems Global's Research Department. Data is monitored by Senior Management.

### 9.6) Continual Improvement

The organisation will continually improve the effectiveness of the Information Security Management System through the use of the quality policy, quality objectives, audit results, analysis of data, corrective and preventive actions and management review.

#### 9.6.1) Implementation

We review our performance as part of a continuous review of Management Information, service-user/customer feedback and comments. In particular we review our progress against our company information security objectives (business plan aims), with a view to seeing what we can improve and where. The chart below illustrates this process:

### 9.7) Corrective Action and Improvement

Both these areas are reviewed within the agenda for the Management Review meetings and typically cover the action taken to control and correct any non-conformances noting any consequences of the action taken and themes which may be evident.

In terms of continual improvement, we also review the suitability, adequacy and effectiveness of our ISMS.

### 9.8) Complaints Policy

SG Systems Global is committed to giving its clients the best possible service, involving them in the development of their V5 Traceability platform, and giving them opportunities to air any complaints that they may have on the service we provide. To this end we operate the procedure outlined in our subscriber terms and conditions whereby an issue can be escalated.

### 9.9) Preventative Action

SG Systems Global has various processes and procedures in place to ensure that preventative action against nonconformities can be introduced, documented and seen through till completion to address the initial problem. The complex nature of the clients we work with, demands that we have flexible but effective processes and procedures in place.

However, SG Systems Global also uses internal and external audits and risk assessments to continuously improve its service delivery, financial, HR and operational functions

## Appendix – List of Controlled Documents

| Ref No | Name | Version | Date | Associated Documents |
|---|---|---|---|---|
| | ISO 27001 Policy Document | 1 | Dec-20 | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |