Agilisys Sefton MBC Partnership

Information Security Management System Policy

August 2018

Version: 1.0 Issue

Table of Contents

1 Context of the organisation (Clause 4)

1.1 Understanding the organisation and its context (Clause 4.1)

Agilisys was awarded contract to provide ICT services to Sefton MBC in July 2018. As part of the contract, Agilisys is responsible to deliver following services :

- Agilisys support the local and cloud-based infrastructure and systems including the provision of a service desk.
- Agilisys support the defined applications used by Sefton detailed within contract schedule 2.1 “Services Description”
- While Agilisys do not support Council third party contracts, Agilisys will engage with third party providers, authorised by the Council, in order to resolve incidents and/ or manage change with the third party

With regards to the Agilisys business itself, there are a number of internal and external factors that create uncertainty that gives rise to risk. These include:

Internal Factors:

Uncertainties in employee relations

Significant organisational changes

Business strategy and goals

Location moves

Company financial performance

Awareness and education in relation to cyber security

External Factors:

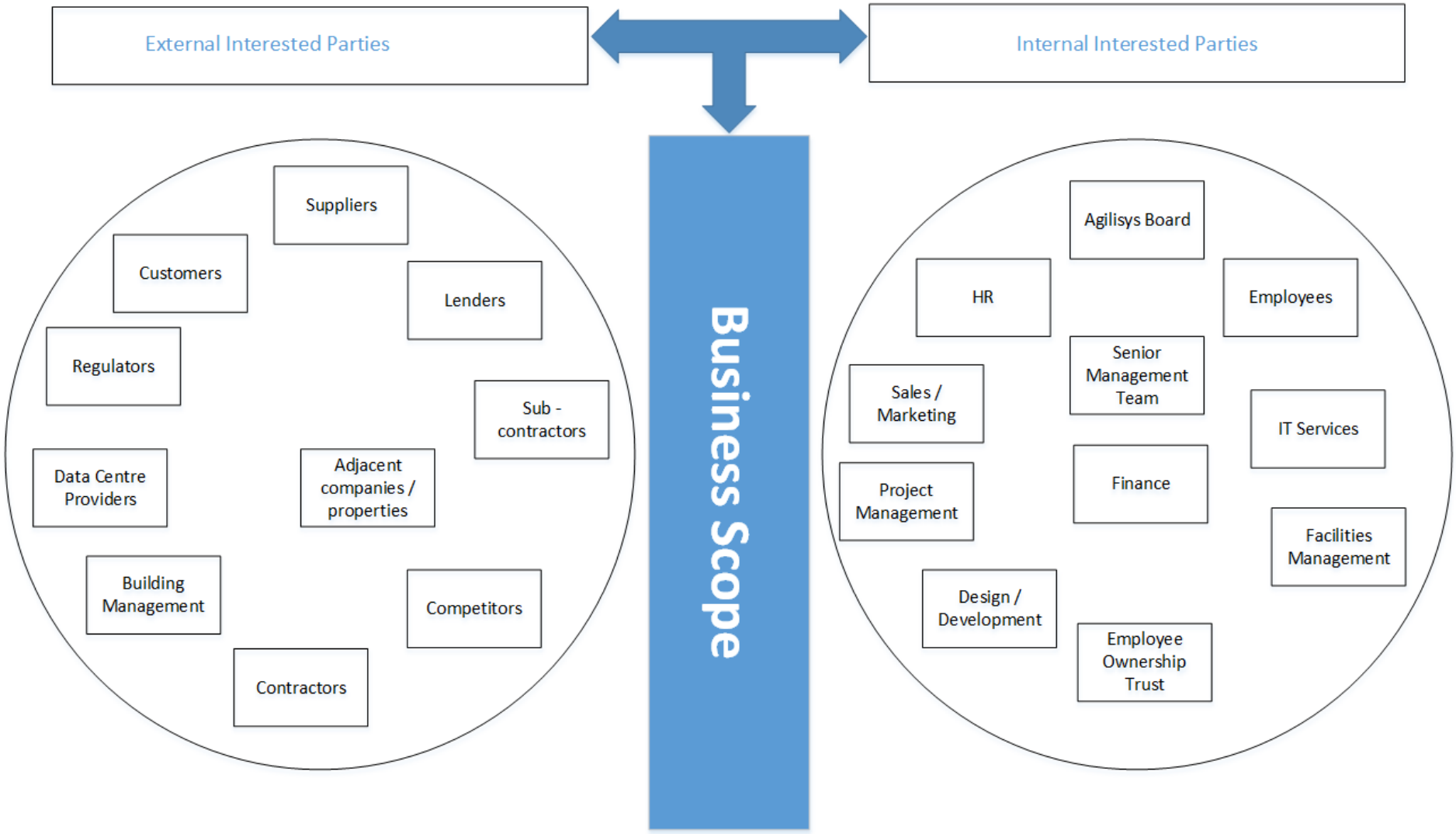
Potential legislative or regulatory changes

Reputational damage

Economic factors i.e.Major supplier failure

Customer/end-user drivers

Malicious code introduced through untrusted sources


External Interested Parties
Internal Interested Parties
Business Scope
Suppliers
Customers
Lenders
Regulators
Sub - contractors
Data Centre Providers
Adjacent companies / properties
Building Management
Competitors
Contractors
Agilisys Board
HR
Employees
Senior Management Team
Sales / Marketing
IT Services
Project Management
Finance
Facilities Management
Design / Development
Employee Ownership Trust

1.2 Understanding the needs and expectations of interested parties (Clause 4.2)

An interested party is defined as “a person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity “

The following are defined as interested parties that are relevant to the ISMS :

- Customer - Sefton MBC
- Sefton MBC Estates and Facilities Management
- Suppliers – Agilisys managed suppliers for Sefton MBC including contractors
- Authorised Council Suppliers – Third party providers supporting Council systems or services where approval for Agilisys to engage said providers has been confirmed by the Council
- Agilisys Senior Management team
- Employees – Agilisys employees working on the Sefton MBC partnership
- Agilisys cloud operations teams
- Agilisys Service Centre (including Service Desk and Service Management)
- Regulatory bodies

Interested Party	Requirement Summary	Source
Customer – Sefton MBC	Meet all contractual and SLA requirements Meet all security requirements	Contract terms and conditions
Sefton MBC Estates and Facilities Management	Meet all environmental and physical requirements	Contract terms and conditions
Suppliers- Agilisys managed suppliers for Sefton MBC including contractors	Meet all payment requirements on time Provide adequate support to commission their services Maintain services to SLA	Contract terms and conditions
Authorised Council Suppliers	Engage with suppliers to resolve incidents and action changes Provide adequate support to work with suppliers in order to reduce impact on the operational services	Contract terms and conditions
Agilisys Senior Management Team	Organisation reputation must be protected Maintain ISO 27001 for Sefton MBC	Business plan Future business growth opportunities
Employees - Agilisys employees working on Sefton MBC partnership	Provide suitable tools to run Infrastructure and services Provide education and awareness of Agilisys operational policies & procedures	Performance reviews and team meetings Employee satisfaction survey

	Provide management and guidance with regard to role requirements and expectations	
Agilisys cloud operations team	Assist the local Sefton team in the management of cloud hosted systems and services	OLA document
Agilisys Service Centre	1st and 2nd line support for Sefton systems and services during Limited Support Hours Provide "overflow" support for the local service desk during periods of high demand Provide centralised guidance and support for all Agilisys standard processes & procedures Provide centralised monitoring and operation of Agilisys standard service management tools	SLA agreement
Regulatory bodies	Applicable legal and regulatory requirements arise from legislation listed in Appendix A – Compliance with Legislation (Corporate ISMS Policy)	Legislation GOV.UK portal Legislation reviews with Agilisys General Counsel As advised by client

1.3 Determining the scope of the information security management system (Clause 4.3)

Purpose

The purpose of the ISMS is to:

- Ensure that Agilisys understands and manages security-related risks to assets and services it manages on behalf of Sefton MBC
- Provide leadership, direction and visible management support for information security
- Provide a framework for the reporting and review of information security incidents
- Provide a central resource of all security related information for all local Agilisys employees and contractors
- Demonstrate compliance with the principles and practices of ISO 27001:2013 to auditors and clients to fulfill our contractual commitments to Sefton MBC.

Scope of the ISMS

The provision of contracted information technology and telecommunications managed services to the public sector. In accordance with the Statement of Applicability (to be drafted on or before 1st December, 2018).

Inclusions:

• All Physical and Information Assets owned or managed by Agilisys.
• Services and Support provided to Sefton MBC including:
    - Networks
    - Servers & Systems
    - Service Desk & Service Management
    - Desktop Services
    - Application Support & Development
    - Database Administration
• Data provided by Sefton MBC
• All Agilisys Staff supporting Sefton MBC.

Exclusions:

- Services provided by Agilisys Cloud Operations (within scope of separate ISO27001:2013 certification)

- Services provided by Agilisys Service Centre (within scope of separate ISO27001:2013 certification)

- Services provided by Council third party providers

- SOA Annex A 'Not Applicable' controls

A14.2.7 – Outsourced development.
A14.3.1 – Protection of test data.

Locations:

Agilisys Offices:

Agilisys – Sefton Office

4th Floor St Peters House
Balliol Road
Bootle
L20 3AB

1.4 Information Security Management System (Clause 4.4)

In accordance with the requirements of ISO27001:2013, Agilisys has established and implemented this ISMS, and established procedures to maintain and continually improve the system. The master document for this ISMS is the Agilisys Information Security Management System Policy, which follows the ISO27001:2013 standard.

Agilisys has also established supporting policies and procedures to express detailed response to standard requirements.

2 Leadership (Clause 5)

2.1 Leadership and commitment (Clause 5.1)

The Agilisys management team plays a key role in information security. They have specific responsibilties for commitment, resourcing, training and awareness which are detailed in s.2.3 Organisational roles,

responsibilities and authorities of this document. Furthermore a security culture is supported through line management down to every employee.

Agilisys Senior Management will enforce the enactment of all Information Security Management activities, and insist upon the complete co-operation of Agilisys employees engaged in the provision of this process. Failure to do so will be met with such disciplinary action as is deemed appropriate under the exact circumstances of non-compliance with the relevant area of the ISMS and the level of impact experienced as a result of non-compliance, to be determined by the Agilisys Senior Management Team.

In the case of an external third party failing to engage appropriately with the ISMS, resulting in non-compliance with governance standards, then this will be escalated to Agilisys Senior Management and whatever action deemed appropriate may be taken, including potentially termination of contracts, based upon the impact experienced as a result of this non-compliance and individual contractual obligations.

2.2 Information Security Policy (Clause 5.2)

This document forms part of the Agilisys Sefton MBC Partnership *Information Security Management System* (ISMS). Its purpose is to define the overall Agilisys Information Security Policy. Supporting policies containing detailed information security requirements will be developed in support of this policy.

It is based upon the International Standard *ISO:IEC 27002:2013 Code of Practice for Information Security Management*,.

Agilisys is committed to ensuring the confidentiality, integrity, availability and security of its business information. Through information security Agilisys are able to operate a secure environment protecting our staff and clients and their information assets.

This *ISMS Policy* addresses a range of issues including management support, commitment, and direction in accomplishing information security goals. The policies and procedures outlined in this document are based on Agilisys' requirements for a secure operating environment, an assessment of the risks that the services provided face, and relevant legislative requirements.

Agilisys proactively encourages our people and our clients to operate in a secure environment. Advice on information security and implementation of the policy can be obtained by contacting the Agilisys Security Team via informationsecurity@agilisys.co.uk

Any Agilisys employees, contractors or temporary staff who have access to Agilisys's information technology (IT) facilities, information systems (IS) and data, are responsible for complying with this or any supporting policy.

The policies for information security will be reviewed annually at minimum.

2.3 Organisational roles, responsibilities and authorities (Clause 5.3)

The Sefton MBC Service Director supported by the Head of Information Security has been given the responsibility and authority to ensure that the ISMS conforms to the requirements of ISO27001:2013. The Information Security team has been given the responsibility for reporting performance of the ISMS within the organisation (Corporate ISMS Policy – Section 2.2). These responsibilities will be governed via the joint ISMS Board which will have appropriate Council SIRO/Accountable Officer representation

In addition to the Corporate security roles and responsibilities there are additional local roles and responsibilities as defined below:

Role	Responsibilities
Local ISMS Board	▪ Establish local information security risk management roles and responsibilities ▪ Advising, monitoring and overseeing the local Information Security Risk Management Process ▪ Ensure that a local information security risk management program is effective. ▪ Provide oversight for the information security risk management activities carried out locally to ensure consistent and effective risk-based decisions ▪ Provide direction on information security risks and issues that cannot be resolved between risk owners and stakeholders ▪ Escalation to Security Steering Committee and where applicable to the Council Information Management Working Group ▪ Set the overall security objectives for this ISMS ▪ Provide visible senior management commitment to and support of information security ▪ Provide sufficient resources to develop, implement, operate and maintain the ISMS ▪ Conduct management reviews of the ISMS ▪ Provide clear priority of security tasks based on risk and cost to the business ▪ Support intiatives to enhance information security
Stakeholders (Agilisys Division Heads, Service Leads & Tower Heads Council Information Asset Owners, SIRO)	▪ Engage in regular risk assessments and other information security risk management activities ▪ Ensuring the achievement of information security risk management activities in their areas of responsibility ▪ Planning, budgeting and performance in information security risk management for their areas of the business (e.g. IT, Customer Services) ▪ The day-to-day security of their business line and related assets ▪ Monitoring significant changes in the exposure of their business line and assets to major threats ▪ The reporting of process non-compliances using the *Security Incident Process*

3 Planning (Clause 6)

3.1 Actions to address risks and opportunities (Clause 6.1)

3.1.1 General (Clause 6.1.1)

While planning for the ISMS , Agilisys will consider the issues referred to in *clause 4.1* and requirements refered in to in *clause 4.2* and determine the risks and opportunities that need to be addressed to:

a) ensure the information security management system can achieve its intended outcome(s);
b) prevent, or reduce, undesired effects; and
c) achieve continual improvement,

and **plans**:

1) actions to address these risks and opportunities; and

2) how to:

i) integrate and implement the actions into its information security management system processes; and
ii) evaluate the effectiveness of these actions.

Identification and analysis of risks and application of appropriate controls to manage identified risks are accomplished and recorded in the Statement of Applicability and the Risk register and Treatment Plan.

3.1.2 Information security risk assessment (Clause 6.1.2)

Agilisys has designed and implemented an information security risk assessment process that provides a consistent,repetable risk assessment methodology conforming to the requirements of the ISO/IEC 27001:2013 standard. This process is accomplished through the risk register and treatment plan.

The ISMS Board has initial oversight of recommendations arising from risk assessments.

The *Information Security Risk Management Process* is published on the Agilisy intranet.

3.1.3 Information security risk treatment (Clause 6.1.3)

The Statement of Applicability and the Risk register (incl. risk treatment plan) provide details concerning controls applied to manage ISMS risks.

Both documents are reviewed at least annually by the designated risk owners to ensure that identified risks are still applicable to the organisation, to ensure that applied controls continue to be adequate and effective, and to recommend actions to improve currently applied controls.

The reviews will:

- Take into account the ongoing changes to business requirements and priorities
- Consider new threats and vulnerabilties
- Confirm that existing controls remain effective and appropriate

The *Information Security Risk Management Process* defines the roles and responsibilities of information risk management.

3.2 Information Security Objectives and planning to achieve them (Clause 6.2)

The Agilisys Sefton MBC ISMS is built and designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to the business and its clients.

Business objectives are set by the Agilisys Sefton MBC Senior Management Team. Information Security objectives are then based on the business objectives. These objectives are reviewed periodically (based on business requirements) by the Management Team or sooner in the case of major impacting changes.

While setting up objectives, Agilisys will also determine :

- Resource requirements
- Identify objective delivery owners
- Timeline of achieving those objectives.
- Result evaluation

Information security objectives for the Agilisys Sefton ISMS are to be defined, however initial objectives are defined in draft for agreement below:

1. Defining the timetable and plan to achieve ISO 27001:2013 certification for the Sefton MBC ISMS.

2. Review and improve the effectiveness and coverage of security updates and upgrades for the estate.
3. Support implementation and testing of BC/DR for Sefton.
4. Regular scanning of the Sefton network to support vulnerability management.
5. Increase security awareness across all staff working in Sefton (including working with the Council regarding security awareness for Council staff).

Plan to achieve objectives.

Objective Number	Objective description	Owner	Resource required	Verification Method	Est.Completion date
1	Defining the timetable and plan to achieve ISO 27001:2013 certification for the Sefton MBC ISMS (Source: contract)	Agilisys Service Director	Members of Information Security Management System Board	Stage 1 & stage 2 audits	July 2020
2	Review and improve the effectiveness and coverage of patching and upgrade for estate (Source: contract)	Agilisys Information Security	Ad-Hoc representation at the Security Steering Committee - Networks - Server & Systems - Desktop - Application Support	Initial review submitted to the Operational Board with Monthly progress report to ISMS Board and quarterly report to Operational Board	Monthly reporting
3	Support implementation and testing of BC/DR for Sefton MBC (Source: contract)	Agilisys Service Director	- Application Support - Business Analysis - Networks - Server & Systems	Initial criticality review of the Sefton application/ systems Review of current Sefton BC plan Convene BC/DR board to define objectiives, plan and governance including gap analysis of current plans Documented BC/DR test plan Test schedules 6 monthly review	Jul-Sep 2019
4	Regular scanning to support vulnerability management. (Source: contract)	Agilisys Information Security	- Networks - Server & Systems - End User Computing	Scanning reports	December 2018
5	Increase security awareness across all staff working in Sefton (including working with the Council regarding security awareness for Council staff). (Source: contract)	Agilisys Information Security	- HR - Council HR, SIRO, IMG - Corporate Comms - L & D - Service Desk	Initial review and deployment of the Agilisys security awareness training modules. Review with Council to determine requirements	December 2018 Quarterly reporting

4 Support (Clause 7)

The Information security management system is owned by the ISMS Board. All activites related to this ISMS is the responsibility of the ISMS Board (A.6.1.1 Information security roles and responsibilities)

4.1 Resources (Clause 7.1)

The ISMS Board is committed to providing the resources needed for the establishment, implementation maintenance and continual improvement of the Information Security Management System.

4.2 Competence (Clause 7.2)

The Agilisys Information Security team has the necessary competence within its members to undertake activities related to the ISMS. Where applicable additional training will be provided to acquire the necessary competence.

4.3 Awareness (Clause 7.3)

The Agilisys Information Security Team is aware of the information security policy and implications of not conforming with ISMS requirements.

4.4 Communication (Clause 7.4)

Internal communication regarding this ISMS will be conducted as described in this table below:

Who shall communicate	Whom to communicate	What to communicate	When to communicate	How to communicate
Corporate communication	Employees Contractors Agilisys Senior Leadership Team	Changes information security policy Changes in corporate policies and procedures Information regarding Security awareness Security incident warnings to employees Legislative changes	Ad-hoc	Via Agilisys corporate intranet and Agilisys Service Centre incident warnings
Member of Senior Leadership Team	CEO & Board members	Changes in contractual requirements Risk above local tolerance	Ad-hoc	Report provided by SSC members
Service Delivery Manager or Procurement team	Suppliers	Changes in Terms and conditions of contract Licencing information	Ad-hoc	By letter or Contract Change Notice

Council retained IT function	Council staff and Council SLB	Changes information security policy Changes in corporate policies and procedures Information regarding Security awareness Security incident warnings to employees Legislative changes	Ad-hoc	Via Intranet, Yammer, Email and eLearning platform
Service Director	Customer	Changes in contractual requirements SLA reports on service being provided	Ad-hoc As agreed by customer	Contract Change Notice
Service Director	Contractors	Changes in contractual requirements SLA reports on service being provided	Ad-hoc	By letter or Contract Change Notice
Service Director	Employees	Changes in contractual requirements	Ad-hoc	By email
Service Director	Employees	Changes in client policy	Ad-hoc	By email
Service Director	Agilisys SSC	Report risk above local acceptance level	Ad-hoc	By email
Service Director	Employees	Findings from client audit	Ad-hoc	By email
Information Security Manager or Service Director	Agilisys staff / ISMS Board	Sefton MBC Internal audit reports	Ad-hoc	Audit report
Service Director	Customer	Responses to FOI requests, subject access requests	Ad-hoc	According to the agreed procedure

General communication will be established via Corporate Intranet, emails, posters and formal meetings.

4.5 Documented Information (Clause 7.5)

4.5.1 General

The Agilisys Sefton Information Security Sanagement System includes:

a) documented information required by the ISO/IEC 27001:2013 International Standard; and

b) documented information determined by the organisation as being necessary for the effectiveness of the information security management system.

4.5.2 Creating and updating

Process owners are responsible for the creation,review and updating documented information supporting Agilisys ISMS. This process is controlled via the Control of Documents procedure.

4.5.3 Control of documented information

Agilisys will document all mandatory information determined as being necessary for the effectiveness of the ISMS.

All documentation is controlled in accordance with the Control of documents procedure which defines the requirements for:

- Producing, reviewing, changing and distributing a Controlled Document.

To maintain the efficiency and effectiveness of the ISMS all information security documentation will be reviewed at least annually.

5 Operation (Clause 8)

5.1 Operational Planning and Control (Clause 8.1)

The ISMS Board will plan, implement and control the processes needed to meet information security requirements to implement actions determined by information risk assessments and necessary to achieve the information security objectives.

Any planned changes will be controlled through the local *Change Control Process.*

5.2 Information security risk assessment (Clauses 8.2)

ISMS risk assessments are performed annually and ad-hoc basis. When significant changes are being considered, risks associated with the proposed change are identified and assessed as part of change management and, if appropriate, added to the ISMS Risk register. Risk reviews are performed as per risk score.

5.3 Information security risk treatment (Clause 8.3)

The risk treatment plan, analysis, controls applied and reviews are documented and recorded via the ISMS risk register and the Statement of Applicability.

6 Performance evaluation (Clause 9)

6.1 Monitoring, measurement, analysis and evaluation (Clause 9.1)

Agilisys will monitor following activities as part of effectiveness of information security management system.

What will be monitored & measured	Methods for monitoring & measurement	When shall monitoring & measurement be performed , analysed & evaluated	Who shall monitor & measure

Security Incidents	Service desk incidents	Monthly	Information Security Team ISMS Board
ISMS Risks	Risk assessment and reviews	Annually or if new risk is identified (local or corporate)	Risk owners ISMS Board Information Security Team Council IMG where applicable
Corrective Action log	Actions included in CAPA log	Every 4 months	Local ISMS Board, Risk owners
Security Objectives	Discussion with objective owner	Every 3 months	ISMS Board, Objective owner
Service continuity/DR test findings	Service continuity/DR test report	As per BC/DR test schedule	Team manager Information Security Team

6.2 Internal audit (Clause 9.2)

Agilisys will establish an audit schedule to conduct internal audit on all services in scope of ISMS to measure the effectiveness of selected controls.

Audit criteria and scope will be defined; audit results will be reported to the ISMS Board to discuss findings.

6.3 Management review (Clause 9.3)

There will be an annual management review of the Agilisys ISMS to ensure its continuing suitability and effectiveness. Business and security objectives will be reviewed and assessed to help identify improvements and the need for changes or updates to the ISMS.

The purpose of management review is to ensure that top management review Agilisys' information security management system (ISMS), at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives.

Minutes and actions from this review are documented and a record of the review is maintained on Agilisys electronic document management system (MS SharePoint).

The input to the management review includes:

- results of ISMS audits and reviews;
- feedback from interested parties;
- changes in external and internal issues that are relevant to ISMS
- fulfilment of information security objectives
- results of risk assessment and status of risk treatment plan
- status of preventive and corrective actions;
- results from effectiveness measurements;

- Recommendations for continual improvement.
- follow-up actions from previous management reviews;

The output from the management review includes decisions and actions related to:

- improvement of the effectiveness of the ISMS;
- update of the risk assessment and risk treatment plan;
- modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:
- business requirements;
- security requirements;
- business processes effecting the existing business requirements;
- regulatory or legal requirements;
- contractual obligations; and
- Levels of risk and/or criteria for accepting risks.
- resource needs; and
- Improvement to how the effectiveness of controls is being measured.

7 Improvements (Clause 10)

7.1 Nonconformity and corrective action (Clause 10.1)

Findings of exernal and internal audits including observation and nonconformity will be included in ISMS Corrective action log to implement action needed.The results of any corrective action will be verified prior to signoff. The results and actions will be communicated and agreed with all interested parties.

7.2 Continual improvement (Clause 10.2)

The security requirements and objectives of an organisation are likely to change over time, Agilisys uses audit results, corrective and preventative actions, risk assessments, analysis on incidents and monitored events and management reviews to continually looks for ways to improve the ISMS.

8 Controls

Controls will follow the Corporate ISMS Policy and are documented within the Statement of Applicability (SOA)

9 Appendix A – Compliance with legislation

Legislative requirements notified by Sefton Council:

PSN Code of Connection (CoCo) v1.31 (7th April,2017)

Document Control

Revision History

Version	Date	Amended By	Summary of changes
0.1	31/08/2018	Steve Morgan	Initial Draft
0.2	10/09/2018	Steve Morgan	Updates after initial review
1.0	14/09/2018	Steve Morgan	Included Appendix A as per approval comments

Document Approval

This document requires the following approvals. ('Approved' assumes review undertaken prior to approval).

Version	Date	Name	Title / Role	Approval Status (Pending/Approved)
0.1	04/09/2018	Rob Alcock	Service Director	Pending
0.1	04/09/2018	Simon Pilgrim	Head of Information Security	Pending
0.1	04/09/2018	Mark Wishart	Arvato Security Officer	Pending
0.1	04/09/2018	Helen Spreadbury	Sefton Council	Pending
0.2	10/09/2018	Helen Spreadbury	Sefton Council	Approved
0.2	10/09/2018	Rob Alcock	Agilisys Service Director	Approved

Document Reviews

This document has been reviewed by the following people, in addition to those listed above.

Version	Date	Name	Title / Role
0.1	04/09/2018	Rob Alcock	Service Director
0.1	04/09/2018	Simon Pilgrim	Head of Information Security
0.1	04/09/2018	Mark Wishart	Arvato Security Officer
0.1	04/09/2018	Helen Spreadbury	Sefton Council
0.2	10/09/2018	Helen Spreadbury	Sefton Council
0.2	10/09/2018	Rob Alcock	Agilisys Service Director