![mandata logo] Software that delivers.	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	1 of 25

1   Introduction

This manual provides the framework for the policies and procedures for the Mandata Limited. Mandata have implemented an Integrated Information Security and Quality Management System compliant to ISO/IEC 27001:2013 and ISO/IEC 9001:2015 which it requires all staff to comply with.

2   Confidentiality Notice

This document and the information contained therein is the property of Mandata. This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Mandata.

3   Terms and definitions

Terms used are those defined in standards wherever appropriate. The standards used as reference include ISO 27000 and ISO9000.

In particular, the **Integrated Management System** (IMS) is a set of interrelated and interacting elements to establish policies, objectives, and processes to achieve those objectives. This includes structure, roles, and responsibilities, planning and operation. It considers risk to the quality, information and information processing as practised by Mandata and manages such risk in accordance with the board's requirements.

4   Management System
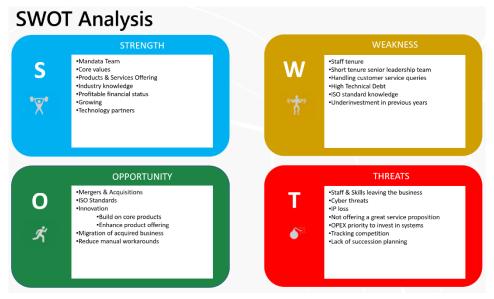
4.1   Context

4.1.1   Overview

The Mandata group of companies develop and produce integrated road transport management software solutions for haulage, transportation, and logistics businesses.

The Mandata group currently incorporates Mandata Ltd but also includes Stirling Solutions, Returnloads.net & Eureka . All entities are under the same management authority and activities are integrated into single business processes. The offices used for the Mandata group are Newcastle (HO), Leicester, Leeds & Wexford Ireland.

![mandata - Software that delivers.]	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	2 of 25

Mandata has an active strategy of acquisition with the intention that any new acquisitions are included in the scope of the management system at the earliest opportunity. The IMS has been designed with this in mind.
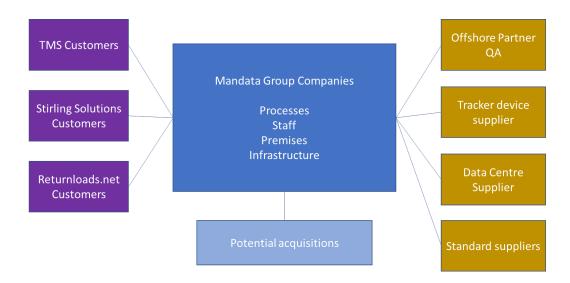
No specific industry based regulations are required to be followed other than legislation and

regulation required to be complied with by all organisations.

![mandata logo] Software that delivers.		Reference:	IMSSOP04001
		Issue Date:	2nd May 2024
		Issue Number:	7.0
Integrated Management System Manual		Author:	Mark Gilston
		Approver:	Alison Young
		Page:	3 of 25

4.2   External and Internal Interested parties

External:

All Customers

Customers require
- products delivered as per original specification;
- Mandata to deliver within the SLA agreed in the master services agreement;
- Support queries to be attended to in a timely manner;
- Software developed using secure system engineering principles
- Security of information stored in the hosted in the SaaS product
- Mandata to demonstrate control over their quality and information security processes

Offshore Partner (QA)

The offshore partner is required to:
- Deliver services within the SLA in the master services agreement
- Use secure methods of testing
- Operate within the parameters of the NDA
- Report on performance to Mandata as required

The offshore partner requires from Mandata
- Clear work instructions for each engagement
- Mandata to operate within the parameters of the NDA
- Feedback on performance against contract
- On time payment for services

Classification : Public

	Reference:	IMSSOP04001
mandata	Issue Date:	2nd May 2024
Software that delivers.	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	4 of 25

Tracker device supplier

The device supplier is required to:
- Required to supply working trackers to order
- Respond to returns in a timely manner

The device supplier requires from Mandata:
- Clear order instructions
- Ontime payments for goods and services
- Clear information regarding any device faults

Data Centre Supplier

The data centre supplier is required to:
- Provide a secure environment for Mandata infrastructure
- Supply all essential services (power, climate control, fire safety)

The data centre supplier requires from Mandata:
- Mandata staff to follow all physical security policies and procedures when visiting site
- Clear agreements in place for services
- On time payment for services received

Internal:

Board of Directors
The board of directors require:
- the IMS to be embedded into business processes ensuring consistent quality of product and service delivery.
- Risks to be managed as agreed
- All staff to follow and comply with the policies and procedures which make up the IMS
- Certification to ISO9001 and ISO27001 to be maintained

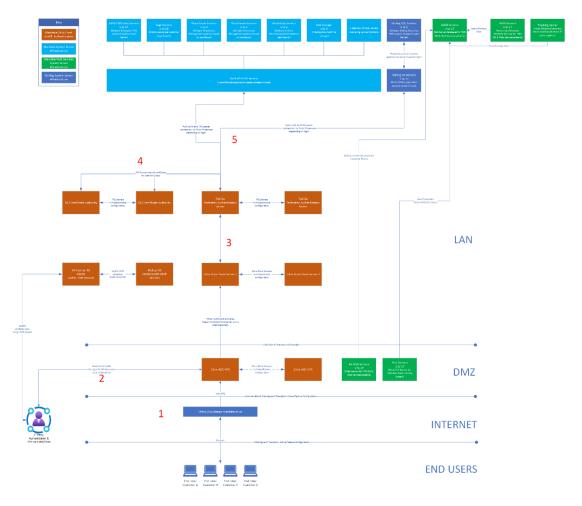**Staff**
All Mandata Staff are required to follow all policies and procedures put in place by the organisation. Staff also need assurance that:

- their own personal information is kept secure
- development plans to enable them to increase their knowledge and ability to do their job are in place
- the organization takes responsibility for their health and wellbeing

Classification : Public

Software that delivers.	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	5 of 25

4.2.1   Internal and external interfaces and dependencies

Newcastle Data Centre

	Reference:	IMSSOP04001
![mandata - Software that delivers.]	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	6 of 25

TMS GO & GO+

GO PLUS Architecture Diagram

	Reference:	IMSSOP04001
mandata Software that delivers.	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	7 of 25

Mandata TMS

Mandata Enterprise TMS CUSTOMER WEB PORTAL

Software that delivers.	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
	Author:	Mark Gilston
Integrated Management System Manual	Approver:	Alison Young
	Page:	8 of 25

Stirling Systems

Bing Maps API

Stirling Geo service – C# service

Transport Lite – c# - quick entry application

Tomtom Webfleet Service

Databases created per Company

StirlingMaster
Abacus_XXX
ADL_XXX
PalletLine_XXX
Rating_XXX
StirlingLink_XXX
StirlingManager_XXX
Transport_XXX
WMS_XXX
Workshop_XXX

Where XXX is the company extension and is named in the StirlingMaster database

Stirling TMS (2 applications) – Utilized by Hauliers to manage their work. *(Visual C++ MFC app and C# app)*

eStirling – Used by Hauliers customers to view Transport, Warehouse and Subcontractor information *(C#, ASP .net and Javascript)*

Webfleet service – C# service

Stirling WMS – Utilized by Hauliers to manage their warehouse *(Visual C++ MFC app)*

License Service – C#

TMS API – Utilized by Hauliers customers to allow integration (C#)

Stirling Workshop – Utilized by Hauliers to manage their workshop *(Visual C++ MFC app)*

Identity Server – for authentication only

Depot Tracks – Hauliers Loaders and unloaders scan freight on and off vehicles
WMS Tracks – Hauliers Warehouse staff use to record Goods in and Goods out *(Xamarin C# - only targeting Android platform)*

Microsoft SQLServer Database – Multiple databases per company – see note for list

IIS hosted web services

Accounts – Utilized by Hauliers to manage their accounts *(Visual C++ MFC app)*

eDriver – Hauliers drivers to capture signatures on collection and delivery *(Android only - Java)*

TomTom webfleet application

ADL scanning – Utilized by Hauliers to scan, categorise and store documents *(C# .net application)*

Stirling Link App – Links to third party accounts systems. *(Visual C++ MFC app)*

Stirling Mandata Service – responsible for allowing Mandata TMS to connect to Stirling WMS and accounts *(C# windows service)*

Stirling Import and Export applications. C# .net. Generally read csv files from a folder and apply stored procedures to contents

Making Tax Digital – C# app

HMRC – API

FTP Service – standalone C# service that moves files using ftp protocol

Classification : Public

		Reference:	IMSSOP04001
mandata **Software that delivers.**		Issue Date:	2nd May 2024
		Issue Number:	7.0
	Integrated Management System Manual	Author:	Mark Gilston
		Approver:	Alison Young
		Page:	9 of 25

Returnloads

Eureka

	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	10 of 25

4.3 Scope

The scope of both systems has been identified:
9001:
The provision of software development to the haulage industry by Mandata (Group), Stirling solutions, Eureka & Returnloads. (7.1.5.2 Measurement and Traceability - Excluded from scope)

27001:
The management of information security in the provision of software development to the haulage industry by Mandata (Group), Stirling solutions, Eureka & Returnloads in accordance with statement of applicability version 1.

4.3.1 In Scope

- All activities carried out across the group
- All information stored either on premise or in the third-party data center
- All paper records
- All software development
- Offices based in Newcastle, Leicester, and Leeds
- All staff at the above locations and remote workers

4.3.2 Interfaces and dependencies

The following are excluded from scope but interfaces and dependencies accounted for:

- Third Party Suppliers (these are managed through the supplier management processes)
- Premises that are considered a home/office for remote workers

Reference:	IMSSOP04001
Issue Date:	2nd May 2024
Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	11 of 25

5   Management responsibility

5.1   Leadership and commitment

Management leadership is demonstrated through:

- Taking accountability for the effectiveness of the IMS
- Establishment of an Information Security Policy;
- Establishment of a Quality Policy
- Establishment of objectives and plans for the IMS;
- Integration of the IMS into the organisation's processes;
- The importance of security management and quality and adherence to policies being communicated to the organization;
- Promoting the use of the process approach and risk based thinking;
- Making resource available to establish, implement, operate, monitor, review, maintain and improve the IMS;
- Ensuring that the IMS achieves its objectives;
- Ensuring internal IMS audits are conducted to maintain compliance with ISO/IEC27001:2013 and ISO/IEC9001:2015 and to support continual improvement.

Commitment to customer focus is demonstrated by ensuring that:

- Customer and applicable statutory and regulatory requirements are determined, understood and consistently met through regular review;
- The risks and opportunities that can affect the conformity of products and services and the ability to enhance customer satisfaction are determined and addressed;
- The focus on enhancing customer satisfaction is maintained

Appropriate records of the above activities are retained.

5.2   Policy

The Quality Policy and the Information Security Policy and their supporting policies have been issued and are available on SharePoint

Classification : Public

	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	12 of 25

5.3 Roles and Responsibilities

The board of directors are ultimately responsible for ensuring information security and quality is maintained at Mandata and have created the Management System Forum with delegated authority for ensuring that the IMS conforms to the requirements of the standards as well as reporting on the performance of the IMS to top management.

The membership of the Management System Forum is made up of:
- Chief Operating Officer (Chair)
- Strategy Planning & Partnerships Director
- Finance Director
- Head Of Business Operations
- Head Of Technology Operations
- Head Of People
- Technical Director
- vCISO

The Management System Forum will meet every quarter to review the standing agenda

The leaders of Mandata are responsible for ensuring that their staff and those working under their control are aware of and follow the tenets of both policies and the supporting management system.

All staff are responsible for complying with the integrated management system including reporting of risks, information security events and incidents in accordance with procedures.

6 Planning

6.1 Actions to address risks and opportunities

Mandata has identified, and has access to, applicable legal and regulatory requirements relevant to the Management System and the interests of relevant interested parties.

These legal, regulatory and other requirements have been taken into account in establishing, implementing and maintaining the Management System.

This information is documented and kept up to date. New or variations to legal, regulatory and other requirements are communicated to affected employees and other interested parties.

The information security risk assessment and treatment process is described in the Risk Management Framework document (ISPOL06001).

![mandata - Software that delivers.]	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	13 of 25

Risk assessment is carried out using a spreadsheet tool using the scales set out in the Risk Management Framework. The spreadsheet tool is also the risk treatment plan.

6.2   Objectives

In addition to the high-level objectives laid out in the Information Security and Quality policies, the following objectives have been established:

- % Staff Awareness training completed annually >90%
- % non-conformances closed within target time >95%
- System uptime as a percentage of available time >99.9%
- % Continual Improvement items reviewed and planned within the target time >80%
- % Business Continuity Tests carried out to plan >90%
- Increase in Customer NPS Scores
- Reporting of all security events and weaknesses
- No of developments with test failures < 5%

Measurements and the plans to achieve these objectives are laid out in the Objectives and Measurements document (IMSREC06003 Integrated Objectives and Measurements.xlsx (sharepoint.com)

7   Support

7.1   Provision of resources

The Management System Forum is responsible for the planning, implementation and control of the IMS and ensuring that any resource issues arising are raised through the COO to the Board.

Management ensures that where controls are implemented, they are implemented correctly and achieve the level of security and business continuity required

Audits are performed to ensure those controls and processes which have been implemented are functioning as expected and actions taken where identified as necessary

Where improvements are identified, management ensures that these are actioned within an agreed time-frame.

Software that delivers.	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
	Author:	Mark Gilston
Integrated Management System Manual	Approver:	Alison Young
	Page:	14 of 25

7.2 Competence

The project team have identified the skills and knowledge required by all staff to ensure an effective IMS and this is reflected in Job Descriptions

Where there is a gap between the skills and knowledge available and the requirements determined, a training and awareness programme is undertaken to close this gap;

7.3 Awareness

All staff will receive security training on entry to the company. Continued awareness is delegated to managers who are provided with periodic updates in accordance with the schedule agreed at the management review meeting.

7.4 Communication

The following information from the management system will be communicated as and when deemed necessary by the Management System Forum.

- IMS performance measures
- Current risk position
- Customer satisfaction measures
- Information on new threats and measures to mitigate
- Staff awareness updates
- Internal audit results
- Security Audits
- Due diligence questionnaires

The appropriate recipients of this information will be selected by Management System Forum.

7.5 Control of Documented Information

7.5.1 Structure

All formal IMS documents are controlled and stored on the SharePoint system, and referenced according to the relevant area of the ISO27001:2013 or ISO9001:2015 standard for ease of retrieval (see section on referencing below). Access to the system is controlled and can be restricted according to individual needs and requirements while making sure that all who need to have a view of certain documents are still able to do so.

Records are controlled and retained in line with the statutory requirements listed in Appendix A of this document.

Classification : Public

	Reference:	IMSSOP04001
mandata Software that delivers.	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	15 of 25

Documents are organised into areas as listed below:

04	Management System and Context
05	Leadership
06	Planning
07	Support
08	Operation **
09	Performance Evaluation
10	Continual Improvement

** Sub folders are created within this folder

7.5.2 Referencing

All formal IMS documents are referenced in accordance with these guidelines.

IMS references should be labelled IMS**XXX***YY***ZZZ** where XXX = the acronym for the document type (see below), YY = the number of the area listed above and ZZZ = a unique number (001, 002,003 etc.).

7.5.3 Document types

POL	Policy
SOP	Standard Operating Procedure
REC	Record
PRO	Process Maps

e.g the Information Security Policy is referenced IMSPOL05001

7.5.4 Publishing

The document owner is responsible for publishing and reviewing the document at planned intervals. Documents must not be published without prior approval for their adequacy and completeness.

The inbuilt SharePoint version control is used for published documents using minor and major versions.

Classification : Public

mandata		Reference:	IMSSOP04001
Software that delivers.		Issue Date:	2nd May 2024
		Issue Number:	7.0
Integrated Management System Manual		Author:	Mark Gilston
		Approver:	Alison Young
		Page:	16 of 25

7.5.5 Headers and Footers

Header detail must contain the following fields:

Document Name
Document Reference
Issue date
Issue no
Author/Owner
Approver
Page no

Footers must contain

Document classification
Version number & revisions

7.5.6 Document Review

Documents are reviewed at planned intervals or if there is any significant change in procedures or the environment. The planned intervals are not less than annually and it is the responsibility of the document owner to ensure that the review is carried out.

If there is no change to a document when it has been reviewed, a new copy should still be published with the next version number with the issue date and next review date updated to reflect that the review has taken place.

8 Operation

Documented information on all operational processes and procedures are stored within the management system in section 08 Operation and, where applicable, in the relevant subsections relating to the Annex A controls.
Risk assessments are carried out annually or in the event of significant change to the organisation, infrastructure or environment. Risk treatment progress is monitored via the spreadsheet tool (See section 6 of this manual).

mandata Software that delivers.	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	17 of 25

9 Performance Evaluation

9.1 Monitoring, measurement, analysis and evaluation

Monitoring and measurement of the IMS takes place in line with the Objectives and Measurements document as described in Section 6 of this manual. Further measurements are taken as required by the Management System Forum. Results are communicated under the direction of the Management System Forum and are an input into the Management Review process.

9.2 Internal IMS Audits

Mandata have put an audit programme in place and all sections of the IMS are audited at least once a year to ensure that the IMS

a) conforms to the requirements of the relevant standards and any other legal, regulatory or contractual requirements

b) meets all identified information security and business continuity requirements

c) is effectively implemented and maintained

d) performs as expected

The programme of audits and audit information (such as audit reports) is retained for a minimum of two years after creation. Audits are carried out by representatives from our cyber security partner in order to ensure objectivity and impartiality.

![mandata - Software that delivers.]	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	18 of 25

9.3   Management review of the ISMS

A review is undertaken every quarter to review the IMS. The review shall make recommendations for improvement which shall then be implemented and monitored by Mandata.

The Management System Forum is responsible for ensuring this review is organised and recorded. The Senior Management receives the output from the review.

The standing agenda for the management review is as follows:

Agenda

1. Actions from previous management reviews.
2. Changes in internal and external issues that are relevant to the IMS
3. Feedback from customers and interested parties.
4. Feedback on IMS performance including trends in:
   - Non conformities and corrective actions (from audits and incidents)
   - Monitoring and measuring results
   - Audit results
   - Fulfilment of objectives
   - Customer satisfaction
   - Process performance and conformity of products and services
   - The performance of external providers
5. Results from risk assessment and the progress of risk treatment plans.
6. Opportunities for continual improvement.
7. Resource issues and planning
8. Review of Information Security and Quality policies
9. Review of the objectives (six monthly).
10. Review of audit schedule.
11. Any other business.

Date and time of next meeting.

	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	19 of 25

10 IMS improvement

10.1 Corrective Action

Non-conformities are identified at either internal or external audits or by identifying non conforming products or services. Appropriate action is taken to eliminate the cause of those non-conformities.

This is achieved by reviewing the nonconformity, determining the cause(s) of the nonconformity wherever possible, determining if similar nonconformities exist, or could potentially occur, evaluating the need for corrective action, determining and implementing corrective action needed, reviewing the effectiveness of any corrective action taken, making changes to the IMS or product specification, if necessary.

Any action needed is implemented and such action reviewed for effectiveness including changes to the IMS. Appropriate documented information on the action taken is retained.

10.2 Continual Improvement

The organisation seeks to continually improve the suitability, adequacy and effectiveness of the ISMS. The Continual Improvement Log (IMSREC10001 Continual Improvement Register.xlsx) is the repository for all improvement opportunities which fall into the following categories and come from a number of sources:

- Non conformances from internal audit
- Non conformances from external audit
- Non-conforming product
- Opportunities for improvement raised at audit (internal or external)
- Opportunities for improvement raised at Management Review
- Improvement ideas from staff
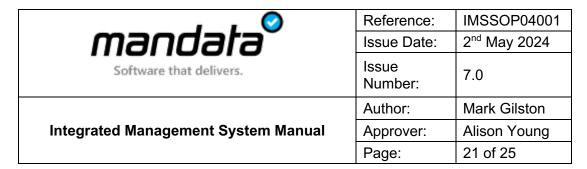- Lessons learned as a result of an event or incident

The continual improvement log is monitored and reviewed monthly by the Information Security Manager.

Classification : Public

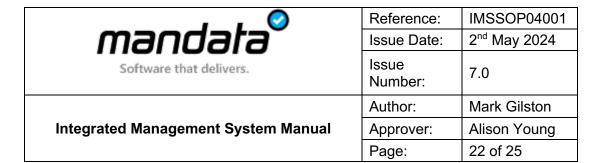|	Reference:	IMSSOP04001
mandata *Software that delivers.*	Issue Date:	2nd May 2024
	Issue Number:	7.0
	Author:	Mark Gilston
Integrated Management System Manual	Approver:	Alison Young
	Page:	20 of 25

Appendix A – Statutory Retention Periods

The main UK legislation regulating statutory retention periods is summarised below. If in doubt, it's a good idea to keep records for at least 6 years (5 in Scotland), to cover the time limit for bringing any civil legal action.
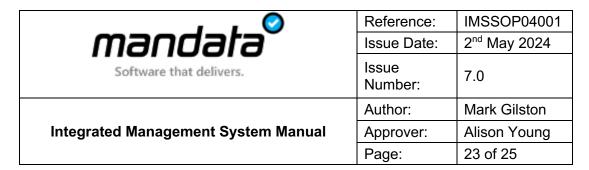
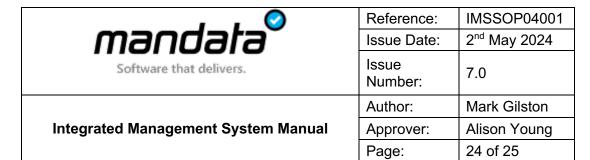| Record types	Statutory retention period:	Statutory authority:
Accident books, accident records/reports (See below for accidents involving chemicals or asbestos)	3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21).	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances (see below).
Accounting records	3 years for private companies, 6 years for public limited companies.	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006.
Coronavirus Job Retention Scheme records of the furlough agreement including: the amount claimed, claim period for each employee, the claim reference number and calculations in case HMRC need more information. For employees on flexible furlough - usual hours worked and the calculations required.	6 years for furlough records. (The guidance says employers should retain the written furlough agreement for 5 years. But HMRC can retrospectively audit all claims so it is important to keep a copy of all records for 6 years minimum.)	The record keeping requirement appears to be in the statutory guidance 'Claim for wages through the Coronavirus Job Retention Scheme'.

Classification : Public

![mandata - Software that delivers.]	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
	Author:	Mark Gilston
Integrated Management System Manual	Approver:	Alison Young
	Page:	21 of 25

First aid training	6 years after employment.	Health and Safety (First Aid) Regulations 1981.
Fire warden training	6 years after employment.	Fire Precautions (Workplace) Regulations 1997.
Health and Safety representatives and employees' training	5 years after employment.	Health and Safety (Consultation with Employees) Regulations 1996; Health and Safety Information for Employees Regulations 1989
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate.	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631).
Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry.	The Control of Lead at Work Regulations 1998 (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676).
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry.	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).
Medical records under the Control of Asbestos at Work Regulations: medical	40 years from the date of the last entry (medical records); 4 years from the	The Control of Asbestos at Work Regulations 2002 (SI 2002/ 2675).

mandata Software that delivers.	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	22 of 25

records containing details of employees exposed to asbestos and medical examination certificates	date of issue (medical examination certificates).	Also see the Control of Asbestos Regulations 2006 (SI 2006/2739) and the Control of Asbestos Regulations 2012 (SI 2012/632).
Medical records under the Ionising Radiations Regulations 1999	Until the person reaches 75 years of age, but in any event for at least 50 years.	The Ionising Radiations Regulations 1999 (SI 1999/3232).
National minimum wage records	3 years after the end of the pay reference period following the one that the records cover.	National Minimum Wage Act 1998.
Payroll wage/salary records (also overtime, bonuses, expenses)	6 years from the end of the tax year to which they relate.	Taxes Management Act 1970.
Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out.	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place.	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence (also shared parental,	3 years after the end of the tax year in which the maternity period ends.	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended, Maternity &

mandata	Reference:	IMSSOP04001
Software that delivers.	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	23 of 25

paternity and adoption pay records)		Parental Leave Regulations 1999.
Subject access request	1 year following completion of the request	Data Protection Act 2018.
VAT deferral (COVID-19) – to support businesses through the COVID-19 pandemic, the government allowed VAT payments due between 20 March and 30 June 2020 to be deferred until 31 March 2021.	6 years.	HMRC VAT deferral guidance.
Whistleblowing documents	6 months following the outcome (if a substantiated investigation). If unsubstantiated, personal data should be removed immediately.	Public Interest disclosure Act 1998 and recommended IAPP practice.
Working time records including overtime, annual holiday, jury service, time off for dependents, etc	2 years from date on which they were made.	The Working Time Regulations 1998 (SI 1998/1833).
Coronavirus Job Retention Scheme	6 years for furlough records. The written furlough agreement should be retained for 5 years, but HMRC can retrospectively audit all claims, so employers should keep a copy of all records for 6 years minimum. This should include the amount	The statutory guidance 'Claim for wages through the Coronavirus Job Retention Scheme'

Classification : Public

![mandata logo — Software that delivers.]	Reference:	IMSSOP04001
	Issue Date:	2nd May 2024
	Issue Number:	7.0
Integrated Management System Manual	Author:	Mark Gilston
	Approver:	Alison Young
	Page:	24 of 25

	claimed, the claim period, claim reference number, calculations, usual hours worked (including any calculations for furloughed employees) and actual hours worked for flexibly furloughed employees.	

Signed by

Alison Young - COO

Date 7th March 2024

	Reference:	IMSSOP04001
mandata	Issue Date:	2nd May 2024
Software that delivers.	Issue Number:	7.0
	Author:	Mark Gilston
Integrated Management System Manual	Approver:	Alison Young
	Page:	25 of 25

Change History Record

Issue	Description of Change	Approval	Date of Issue
1.0	Initial issue	Allan Farrell	11th Oct 2022
2.0	Inclusion of SWOT post internal audit	Mark Gilston	6th Jan 2023
3.0	Updated Information Classification	Mark Gilston	20th Feb 2023
4.0	Updated Scope	Mark Gilston	18th April 2023
5.0	Updated IMS Forum attendees and Frequency , & Exec member	Mark Gilston	7th Mar 2024
6.0	Updated to include Eureka business in context, updated job Title of Service Quality member of IMS	Mark Gilston	1st May 2024
7.0	Added additional document type IMSPRO to cover process maps where no policy exists	Mark Gilston	2nd May 2024