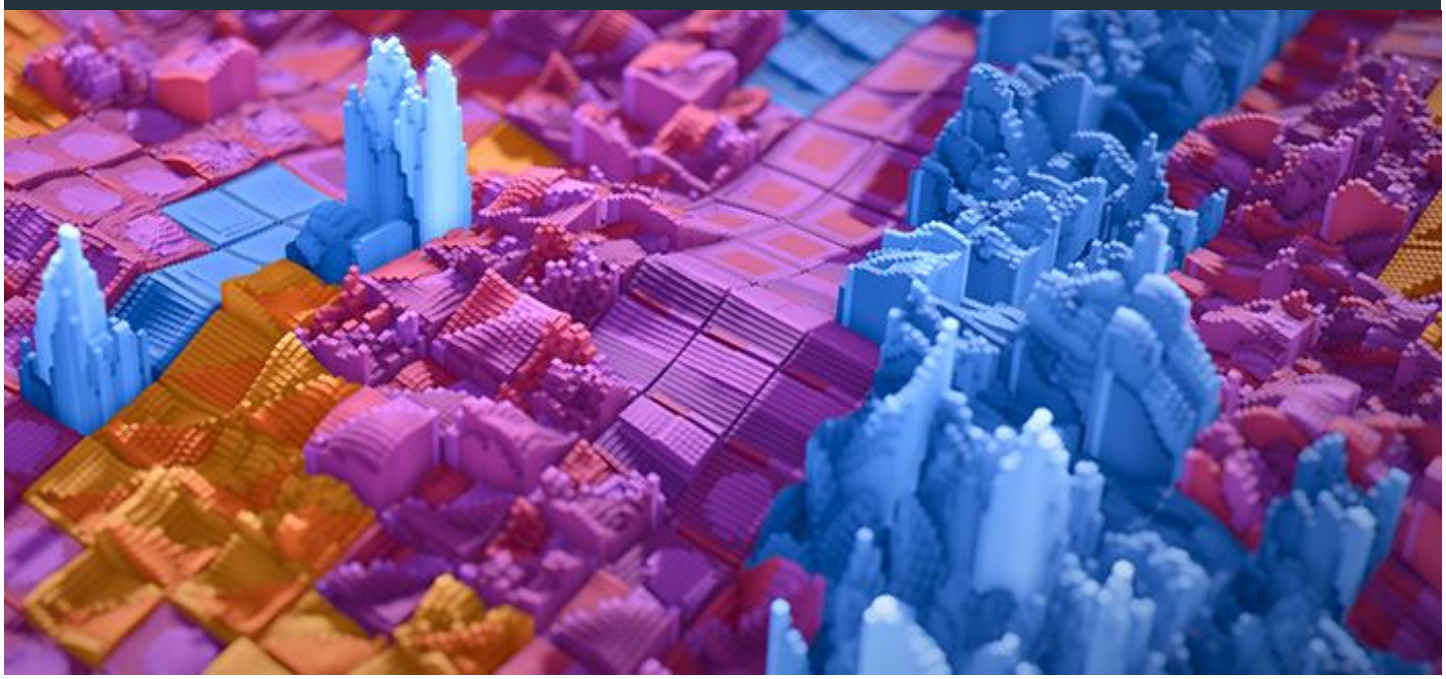
Maintel

Business Continuity Policy with policy detail

Prepared by:
Maintel Compliance Team



Contents

1. Policy framework

Maintel consider Business Continuity aspects as a top priority for customer confidence, contractual compliance, and the protection of our brand. Accordingly, we commit to ensuring all business continuity events within scope are handled in an appropriate manner whilst maintaining the Maintel Integrated Management System (IMS) to meet the requirements of regulations and elected certifications and accreditations. This framework describes Maintel approach to Business Continuity, it defines.

- The organisation for Business Continuity; roles and responsibilities.
- the business context for Business Continuity and alignment to business objectives
- the definition of Business Continuity
- the Business Continuity Strategy
- the individual policy description and link to detail

This Policy applies to.

- All Maintel employees
- Contractors and temporary workers
- Third party Suppliers

1.2 Business context and objectives

Maintaining our operational business is a key priority within Maintel and we are always committed to ensuring working practices are in place to protect Maintel and, that emergency preparedness and response for environmental, technological and health and safety events which may occur and affect the normal business operations within Maintel are documented, tested, improved upon and regularly reviewed.

The Maintel Business Continuity position encompasses a range of stakeholders and interested parties. Our Business Continuity plan is designed to ensure Maintel functionality is maintained to an appropriate level to support our objectives of.

- Identifying the impact of an outage and restoring services to the widest extent possible in a minimum time frame and maintain the ability to provide services to employees and customers.
- Effectively managing a Business Continuity event.
- Communicating effectively within our organisation and with external parties.
- Avoiding confusion that may be experienced during a Business Continuity event by documenting, regularly testing and reviewing recovery procedures.
- Ensuring information security controls remain in place to always protect classified information.
- Having defined Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objective (RTO)

    - MTPD: The time frame from the start of BCP event that recovery outside of, would become unacceptable for Maintel operations.
    - RTO: The time frame from the start of the BCP event to the minimal requirements for business operations to continue.

- Defining what will happen once a BCP event is resolved, and the team is stood down

to deliver.

- Contracted products and services
- Compliance with regulatory and certification/accreditation requirements

As part of our Business Continuity management, we have deployed the Maintel Integrated Management System which includes IMS Risk tool that the Management Team utilise with the aim of maintaining existing known risks at their current low level and ensuring that new and changing risks are managed in an equally consistent and professional manner.

1.3 Definition of Business Continuity

Business Continuity refers to the processes and methodologies which are designed and implemented to protect Maintel provision with the minimum of disruption. Any loss of utility, service, connectivity, or catastrophic event that causes an interruption to normal operations and has one or more of the following attributes is contained within the Business Continuity Plan.

- Requires additional communication resource outside of normal incident management procedures to resolve
- Impacts more than 50% employees
- Impacts one or more Maintel locations
- Impacts multiple customers connected to the Service Provider infrastructure.

1.4 Business Continuity Events

The list of Business Continuity Events is reviewed annually, and should an incident occur that is not covered and subsequently assessed as requiring inclusion, a process for resuming business will be included within the Business Continuity Plan.

- Building Inaccessibility
- Civil Unrest
- Cyber Attack
- Fire Event
- Flood or Water Event
- IT Infrastructure and 3rd Party applications outage
- Service Provider Infrastructure and associated hosted applications outage
- Natural Disaster
- Pandemic / Epidemic
- Prolonged Power Outage
- Service Desk outage
- Severe Weather Disruption
- Terrorist Attack

The following events are beyond the scope of BCP and if any of the following events occur Maintel will follow national guidance for the safety of Maintel personnel and management of operations:

- Civil War
- Major Terrorism
- National Disaster
- National Grid power outage
- Nuclear war

1.5 Organisation for Business Continuity

The overall responsibility for Business Continuity rests at the highest management level. However, it is the responsibility of every employee to co-operate in providing and maintaining Business Continuity. This part of our policy allocates responsibilities to line managers to provide a clear understanding of individuals' areas of accountability in controlling factors that could lead to deviation from the Business Continuity Policy. Managers are required to provide clear direction and accept responsibility to create a positive attitude and culture towards Business Continuity.

The following positions have been identified as having key responsibilities for the implementation of our Business Continuity arrangements:

Chief Executive Officer

The Chief Executive Officer has overall responsibility for ensuring our compliance with Business Continuity contractual arrangements and certifications but delegates the responsibility for implementation to the Data Protection and Compliance Officer, assisted by the Director of Information Systems and the Head of Infrastructure Services**.** The Chief Executive Officer will ensure that:

- our Business Continuity Policy is implemented, monitored, developed, communicated effectively, reviewed, and amended as required
- A Business Continuity review plan of continuous improvement is created and that senior management monitor progress against agreed targets
- suitable and enough funds, people, materials, and equipment are provided to meet Business Continuity requirements
- senior management designated with Business Continuity responsibilities are provided with support to enable objectives to be met
- a positive Business Continuity culture is promoted, and senior management develop a pro-active culture which will permeate into all activities undertaken and reach all personnel
- a system of communication with employees is established and effective training programmes have been put into place
- regular Business Continuity reports are presented to the Board.

Data Protection and Compliance Officer

Assisted by Director of Information Systems and Head of Infrastructure Services and designated with day-to-day responsibility for ensuring our compliance with Business Continuity regulations and selected certifications. They will ensure that**:**

- our Business Continuity Policy is implemented, monitored, developed, communicated effectively, reviewed, and amended as required
- A Business Continuity plan of continuous improvement is created, and progress monitored
- suitable and enough funds, people, materials, and equipment are provided to meet Business Continuity requirements

- an adequate system of maintenance exists and operates to keep Business Continuity information in hard and soft copy in a safe condition and access controlled
- there is regular communication with staff on Business Continuity
- an effective training programme is established to ensure staff are competent in Business Continuity actions
- Business Continuity incidents and suspected incidents are raised, thoroughly investigated and, when necessary, further effective controls implemented and communicated to staff and interested parties
- effective contingency plans are in place with a designated person in charge of the planning and control measures for situations involving Business Continuity events
- objectives are set and their achievement is measured and reported.

Director of Information Systems & Head of Infrastructure Services

They are responsible for ensuring that:

- they support the Data Protection and Compliance Officer and complete delegated tasks
- there is regular communication to all employees regarding Business Continuity
- Business Continuity issues raised by employees are investigated, remediated and improvements put in place where appropriate
- Business Continuity throughout the business is monitored
- trends in Business Continuity incidents are identified and appropriate actions taken
- Business Continuity is promoted, and new initiatives are considered to progressively improve standards in all areas
- Business Continuity testing is regularly undertaken, and actions initiated to maintain business functions within minimum recorded standards
- A business impact analysis is maintained, considering all Business Continuity risks
- employees are aware of significant changes to our Business Continuity Policy and associated Business Continuity Plan, processes, and relevant documentation.

Office Leaders and Line Managers

Will ensure that in their areas of control:

- they actively lead the implementation of our Business Continuity Policy and rules are followed by all
- they supervise their staff to ensure that they work within the confines of the Business Continuity policy
- risk assessments, where required, are completed, recorded, and regularly reviewed

- incidents and suspected incidents are reported immediately through Auto Task
- Business Continuity training for staff is undertaken within timescales set and recorded as requested

All Employees

All employees must:

- comply with the Business Continuity Policy and observe all procedures and processes as well as any additional guidelines established
- report all suspected and actual Business Continuity incidents through Auto Task
- complete as requested any Business Continuity training

Contractors

All contractors must:

- comply with the Business Continuity Policy and observe all procedures and processes
- use all equipment and information only as directed or allowed
- report all suspected and actual Information Security incidents through Auto Task or to local host

1.6 Policy review and amendments

This policy is amended from time to time from regular review, annual internal and external audits, request for amendments following change to the organisation or technology.

The IMS Management team meet quarterly to discuss the policies in place.

Employees wishing to request a change should notify a member of the IMS Management team, detailing the changes as per the Document and Data Control process within the IMS Framework.

The latest version of this policy is available in the IMS portal, copies that are downloaded are uncontrolled.

2 Policy Statement

This policy applies to all Maintel employees.

Maintaining our operational business is a key priority within Maintel and we are always committed to ensuring working practices are in place to protect Maintel and, that emergency preparedness and response for environmental, technological and health and safety events which may occur and affect the normal business operations within Maintel are documented, tested, improved upon and regularly reviewed. The Maintel Business Continuity position encompasses a range of stakeholders and interested parties. Our Business Continuity plan is designed to ensure Maintel functionality is maintained to an appropriate level.

Maintel take compliance with this policy very seriously. The importance of this policy means that internal failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. Maintel will:

- Ensure that Maintel management, employees and any other individuals acting on behalf of Maintel will comply with the requirements of the Business Continuity Policy
- Minimise the risk of damage to company assets, customer assets within scope, information, reputation, hardware, software, or data.
- Set out clearly the company's policies relating to all aspects of the Business Continuity Policy through a documented Management System contained within the IMS Portal.
- Maintain a systematic approach to risk assessment within the Maintel Integrated Management System (IMS), setting policy and objectives for the IMS to reduce risks to acceptable levels.
- Maintain Business continuity plans and test them as appropriate (as far as practicable)
- Provide Appropriate training for all employees
- Maintain the IMS by a schedule of Internal audits carried out by competent auditors

The overall responsibility for ensuring that the Policy is implemented, developed, and reviewed effectively rests with the Chief Executive Officer. This responsibility will be delegated throughout the management structure reflecting our continued commitment to Business Continuity at all levels throughout Maintel.

- The Data Protection and Compliance Officer has direct responsibility for maintaining the Business Continuity Policy and providing advice and guidance on its implementation.
- All managers are directly responsible for implementing the Business Continuity Policy within their business areas, and for adherence by their staff.
- It is the responsibility of each member of staff to adhere to the Business Continuity Policy.

This statement represents our general position on Business Continuity and the policies and practices we apply in conducting our business.

Signed by:
Daniel Davies
CA8EBC2671D3464...

Dan Davies

Chief Executive Officer

07/31/2025

3 Policies, Processes and Plan

3.1 Policies and Processes

The following policies are associated with the Business Continuity Plan.docx Use the policy name hyperlink to view policy and process detail in this document.

Process name	Description
Auditing Policy.docx	Guidance to safeguard the objectivity, independence and effectiveness of its external auditor
Business Continuity Plan.docx	The overarching plan outlining the scope, criteria, command structure, contacts, and processes for enactment of the Maintel Business Continuity procedures
Business Continuity Staff Guidance.docx	An outline of what to do during a business continuity event
Communications Policy.docx	How and what we communicate both internally and externally and for effective management and direction of IMS Management system and company certifications and accreditations.
Competency, Training and Awareness Policy.docx	This policy sets out the organisation's commitment to perform an induction and IMS training program for all employees with associated description and frequency
Exchange of Information Policy.docx	The consideration to be given and actions to be taken, to ensure continued security, when information is to be exchanged externally.
Information Classification Policy.docx	Details what is classified for documentation, electronic information and hardware. 4 main levels of classification in operation; Encrypted Data, Restricted, Confidential and Public.
Information Security Incident Policy.docx	How security incidents are categorised, the reporting mechanisms and actions to be taken should an event occur.
Improvement Process.docx	This process outlines how to identify and record non-conformances as well as implement preventive and corrective action.
Internal Audit Process.docx	How Internal Audits are organised, completed and linked to improvement process
Legal and Regulatory Compliance Policy.docx	Management of legislative updates in relation to the requirements of the IMS standards.

Process name	Description
Management Review Process.docx	Details the process for conducting a review of the Integrated Management System by Management.
Operational Control Process.docx	Headline process for implementation of Services and Equipment across Maintel offerings
Privacy Policy - External.docx	How we manage personal data for customers
Privacy Policy - Internal.docx	How we manage personal data for employees
Retention, Disposal and Destruction Policy.docx	Maintel management of Equipment, Records and Documents including retention periods and methods of destruction
Risk Management Policy.docx	The overall approach to risk management within Maintel and a framework for ensuring consistency in the identification, assessment, reporting and on-going review of risk
Staff Vetting and Exit Policy.docx	Requirements for vetting all new staff and the mechanisms in place for staff leavers, with the return of equipment and the revoking of access rights.
Sustainable Procurement and Supplier Management Policy.docx	The principles, policies and procedures on which sustainable procurement activity within Maintel is based and the criteria for on-boarding, vetting and ongoing management of Suppliers

3.2 Auditing Policy

The purpose of this policy is to define the mission and objectives of the internal audit function.

The policy is designed to support the strategic direction of the internal audit function and ensure that internal audit's ways of working are agreed and communicated across our organisation.

Scope

This policy applies to all assurance activity led by the Maintel internal audit function. This includes:

- Risk based internal audit reviews undertaken as part of the annual internal audit cycle,
- Advisory reviews for less established processes or emerging risk areas.

Underpinning the scope of Maintel assurance activity is a detailed methodology which sets out how internal audit work should be conducted by the internal audit team members.

Definitions

Internal audit

The Certified Institute of Internal Auditors defines internal audit as:

> "An independent, objective assurance and consulting activity designed to add value and improve an organisations operation."

It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

Advisory review

This type of assurance activity aims to provide support to management in developing a robust control framework in areas that are less established or in their infancy in an advisory nature,

It is expected that after this type of work a follow up internal audit will take place to assure the effective implementation of recommendations provided as part of the initial advisory review.

Mission, Principles and Objectives

Mission and Principles

For an internal audit function to be considered effective, all core principles should be present and operating effectively.

It is recognised that how internal audit demonstrates the achievement of the principles may be different from organisation to organisation, but failure to achieve any of the principles would imply that an internal audit activity was not as effective as it could be in achieving internal audit's mission.

Maintel internal audit team have adopted the core principles outlined below when undertaking assurance work:

- Demonstrating integrity.
- Demonstrating competence and professional due care.
- Being objective and free from undue influence (independent).
- Being aligned with the strategies, objectives & risks of the organisation.
- Being appropriately positioned and adequately resourced.
- Clear demonstration of quality and continuous improvement.
- Effective communication.
- Providing risk-based assurance.
- Being insightful, proactive, and future-focused.
- Promotes organisational improvement.

The principles will be reviewed on an annual basis and will form part of internal audit's self-assessment process.

Objectives

The strategic objective of Maintel internal audit team is to provide adequate assurance to the Audit & Risk Committee and relevant stakeholders that the organisation's system of internal control is suitably designed and is operating effectively in a manner that will mitigate the key risks facing Maintel operations.

Underpinning this objective are the following detailed requirements:

- Reviewing and appraising the soundness, adequacy and application of accounting, financial, non-financial and other controls (both existing and proposed) throughout Maintel to promote effective and efficient internal control at reasonable cost,
- Ascertaining the appropriateness of (and the level of compliance with) established policies, plans and procedures,
- Ascertaining the effectiveness with which Maintel assets are accounted for and safeguarded from losses,
- Ascertaining the reliability of management data produced within Maintel for internal and external consumption,
- Conducting special investigations as directed by the Operating Board or Audit and Risk Committee.

Annual Audit planning

Between September and December each year a review of the current management and team structure takes place and is updated to the annual audit plan. The relevant Operating Board members assist in identifying:

- Potential audit projects
- Risk assessing potential projects,
- Prioritising potential projects by risk
- Calculating available resources
- Creating the annual audit plan

Identification of potential projects – The Audit Universe

The planning process begins with the identification and high-level risk assessment of potential audit projects. The projects will originate from several sources including:

- Changes to organisational structure
- Financial reporting
- Integrated risk management processes (IMS risk)
- Suggestions from the Audit and Risk Committee
- Suggestions from the Operating Board
- Queries and/or complaints from customers and external stakeholders
- Other sources including External Audit, Whistle-Blowing records etc.

The Audit Universe is a live document, being continually updated as the Compliance team gain additional information or identify additional risks within departments.

Risk Assessment

In addition to the normal routine of Operational and Corporate risk review, the Audit Universe is subjected to risk assessment to identify those potential audit projects that could have the most significant impact on the achievement of Maintel objectives.

The potential projects in the Audit Universe are assessed and prioritised using the following factors:

- **Financial**: The value of a department's expenditure budget
- **People**: The number of employees working in an area or project
- **Identification of risk**: The number of previous interviewees who identified the potential project as an area they felt was important to be audited.

The following table outlines the factors and associated parameters used to quantitatively assess potential audit projects set out in the Audit Universe.

Factor	Description	Detail	
Financial	Revenue, Operating Expenditure, Capital Expenditure per head per month	High = 20 Medium = 10 Low = 0	>£12,000 £5,001 to £11,999 <£5,000
People	Number of employees	High = 20 Medium = 10 Low = 0	>10 staff 4 to 10 staff 1 to 3 staff
Identification of risk	Identified by previous interviewees	High – 20 Medium = 10 Low = 0	Two or more interviewees One interviewee Not identified by interviewees

Prioritised list of potential audit projects

The potential projects generated by the risk assessment are reviewed by the Operating Board to create a prioritised list of potential audits.

Where applicable, the technology risk of possible auditable topics, areas or existing projects is also considered, such as dependency on IT, use of emerging technologies and strength of controls.

Calculating available audit resources

The Internal Audit function sits within the Finance Division, Compliance Team with 2 days per calendar month dedicated to departmental internal audits.

Resource is allocated within diary time slots and work completed as per the Audit Universe schedule.

Annual Audit Plan for Approval

The final step is to develop the annual audit plan to consolidate the results of risk-based prioritising and audit resource availability.

The draft audit plan is presented to the Operating Board for approval.

Reporting

As part of the Internal Audit responsibility to the Operating Board, periodic reporting is provided in line with the frequency set out below:

- Annually: Internal audit plan
- Quarterly: Progress against plan
- Quarterly: Results of audit and advisory activity

Performance of internal audit

Key performance indicators

To achieve the objectives set out in this document the internal audit function and Maintel stakeholders must adhere to its assurance responsibilities.

To measure this, the following key performance indicators will be monitored and reported through the Integrated Management System (IMS) objectives and targets process.

Key performance indicator	Audit cycle	Evidence	Responsible owner
Annual audit plan to be prepared	The process of drafting the internal audit plan is undertaken annually between September and December.	Operating Board approval of internal audit plan.	Internal Audit

Key performance indicator	Audit cycle	Evidence	Responsible owner
	All senior managers across the business will have the opportunity to contribute to the plan. Draft versions of the plan are presented to the Operating Board for review and sign off in December Operating Board meeting	Minutes or email.	
All terms of reference to be issued within two weeks of the scoping meeting	All internal audit assignments will begin with a formal notification of the audit being issued to the Operating Board sponsor. This will be followed by a scoping meeting during which the scope of the audit will be agreed. Formal terms of reference will be issued to confirm the scope of works	Email issuing terms of reference to relevant stakeholders	Internal Audit
Audit evidence to be provided to internal audit within two weeks of information being requested	Once fieldwork dates agreed, an information request is issued setting out the information and evidence required for the audit	Uploading information to SharePoint/Teams location	Operating Board and Department Leads
Audit closing meeting to be held for all audits	Once fieldwork is complete and evidence received a closing meeting is held with the relevant stakeholders where audit findings and subsequent actions are agreed	Closing meeting calendar invites and meeting minutes	Internal Audit

Key performance indicator	Audit cycle	Evidence	Responsible owner
Audit report issued within two weeks of audit closing meeting	A report issued promptly following the closing meeting which sets out the findings and proposed remedial actions to address identified risks. Remedial actions added to Improvement log within the IMS Portal	Email of report to stakeholders	Internal Audit
Stakeholder confirmation of completion dates for remedial action	Stakeholder provides confirmation of dates for actions to be completed and add to the Improvement log entries	Improvement log showing target completion date	Operating Board and Department Leads
Quarterly progress report	Provide latest status of internal audits and improvements to Operating Board	Operating Board pack	Internal Audit

3.3 Business Continuity Plan

Introduction

The Business Continuity Plan (BCP) has been documented to prepare Maintel, its employees and contractors in the event of extended service outages and vulnerabilities caused by factors beyond Maintel control and to restore services to the widest extent possible in the minimum time frame and recommends necessary measures to prevent and mitigate extended service outages.

The BCP covers emergency preparedness and response for environmental, technological and health and safety events which may occur and affect the normal business operations within Maintel and works in conjunction with the Disaster recovery plan and associated processes.

Maintel employees are engaged with implementing preventative measures whenever possible to minimise failure and recover as rapidly as possible when a failure occurs.

The procedures set out in this document should be used only as guidance when responding to a BCP event. The exact nature of a BCP event and its impact cannot be predicted with any degree of certainty. It is important that a good degree of common sense is used when deciding actions to take. It is intended that the plan set out here will prove useful in allowing the correct actions to be taken more quickly and based on more accurate information. All members of staff named in this document are provided a copy which they must have available when required.

All personal information collected as part of the business continuity plan and contained in this document will be used purely for the purposes of business continuity plan planning and enactment and, is subject to current data protection regulations. Maintel BCP is subject to internal and external audit and testing at regular intervals each year and the BCP is material to the successful continuance of Maintel business operations, ISO, PCI and specific certifications and accreditations.

Scope

The scope of the BCP includes all Maintel offices, Maintel employees, the Maintel Corporate IT infrastructure and 3rd party cloud service applications and, the Maintel Service Provider Infrastructure and associated hosted applications are included within the within the scope of BCP.

The following events are beyond the scope of BCP and if any of the following events occur Maintel will follow national guidance for the safety of Maintel personnel and management of operations:

- Civil War
- Major Terrorism
- National Disaster
- National Grid power outage
- Nuclear war

Objectives

- To identify the impact of an outage and restore services to the widest extent possible in a minimum time frame and maintain the ability to provide services to employees and customers,

  - To serve as a guide for Maintel recovery teams to effectively manage a BCP event,
  - To explain how communication within the organisation and with external parties will be handled,
  - To avoid confusion that may be experienced during a BCP event by documenting, regularly testing and reviewing recovery procedures,

- To ensure that information security controls remain in place to always protect classified information
- To have defined Maximum Tolerable Period of Disruption (MTPD) and Recovery Time Objective (RTO)

  - MTPD: The time frame from the start of BC event that recovery outside of, would become unacceptable for Maintel operations,
  - RTO: The time frame from the start of the BC event to the minimal requirements for business operations to continue.

- To define what will happen once a BCP event is resolved, and the team is stood down

BCP definition

Any loss of utility, service, connectivity, or catastrophic event that causes an interruption to normal operations and has one or more of the following attributes,

- Requires additional communication resource outside of normal incident management procedures to resolve,
- Impacts more than 50% employees,
- Impacts one or more Maintel locations,
- Impacts multiple customers connected to the Service Provider infrastructure

BCP events

- The list of BCP Events is reviewed annually, and should an incident occur that is not covered and subsequently assessed as requiring inclusion, a process for resuming business will be included.
- Building Inaccessibility
- Civil Unrest
- Cyber Attack
- Fire Event
- Flood or Water Event
- IT Infrastructure and 3rd Party applications outage
- Service Provider Infrastructure and associated hosted applications outage,
- Natural Disaster
- Pandemic / Epidemic
- Prolonged Power Outage
- Service Desk outage
- Severe Weather Disruption
- Terrorist Attack

Assumptions

- Key people will be available following a BCP event declaration.
- This document and all vital records are stored in electronic and paper copy,

- **Paper copy:** With each member of the BCP teams
- **Electronic copy:** IMS Portal

- All Maintel locations and Infrastructure providers relevant to Maintel IT Infrastructure and Maintel Service Provider Infrastructure implement preventive measures whenever possible to minimise operational disruptions and to recover as rapidly as possible when an incident occurs.
- Teams have been trained in the BCP and disaster recovery mechanisms.

Invoking the BCP

This plan becomes effective when a BCP event within scope occurs. Normal incident and problem management procedures initiate the BCP event and the BCP remains in effect until operations are resumed and control is returned to the appropriate functional management. In all cases the safety of Maintel employees is paramount and the prime consideration

How a BCP event is identified

Proactive Identification
Where monitoring and/or pro-active vulnerability and threat assessment has identified a potential BCP event, the details are reported through the Service Management System or directly to the managing department, for example, IT, Operations, Office Leaders. BCP is enacted using the appropriate process.

Major Incident Threshold Limit
Where monitoring identifies a non-tenable event on the same technology, which would exceed the agreed threshold. the details, where not already reported are reported through the Service Management System or directly to the managing department, i.e. CX, Facilities, Office Leader, IT or Operations. BCP is enacted using the appropriate process.

Reactive identification
Where a reported event is identified to be within the scope of the BCP or a building has been evacuated, the details, where not already reported are reported through the Service Management System or directly to the managing department, i.e. Facilities, Office Leader, IT or Operations. BCP is enacted using the appropriate process.

Declaring a BCP event
Gold Command is responsible for declaring a BCP event and authorising Silver Command which is led by the person initiating the conference call to proceed with communication and recovery activities detailed in Disaster Recovery Plans and associated processes.

Business Hours
Contact is made with Gold Command to advise of the situation and request to enact the BCP. A member of Silver Command or any employee dealing with a suspected business continuity event contacts the relevant Gold Command team member, to obtain authority to proceed and discuss and receive information for priorities of repair and invoking departmental/local disaster recovery activities.

Out of Hours
The Duty Manager is responsible for making the decision to initiate the BCP and, using the out of hour's contacts, coordinates a conference call with the relevant Gold Command members to obtain

authority to proceed, discuss and receive information for priorities of repair and invoking departmental/local disaster recovery activities.

Recovery teams

Maintel utilises a Gold and Silver Command structure ensuring that during an event the appropriate levels of decision making, and responsibilities are in place. The membership of the Gold and Silver Command teams may change, dependant on the time of day, day of week and availability of contact.

- **Gold command**: has overall control of Maintel resources and formulates the strategy for recovery of the BCP event and is likely to be a member of Maintel Executive or Senior Management Team
- **Silver command**: Manages the tactical implementation following the strategic direction provided by gold command and turns the strategic direction into a set of actions for appropriate resources to complete. This may include being directly involved in carrying out technical actions.

Silver Command team

Normal office hours: Mon to Fri 9am to 5.30pm

The Silver Command team members are available to provide support to departments during the early identification of a BCP event.

Primary Contact	Contact Details	Office/Area	Secondary Contact Details
Office Leader	Redacted	Blackburn	Redacted
Facilities	Redacted	Blackfriars	Redacted
Head of IT	Redacted	IT Infrastructure and Applications	Redacted
Operations	Redacted	Service Provider Infrastructure and Applications	Redacted
Operations	Redacted	Service Desk	Redacted

Outside normal office hours: Mon to Fri 5.30pm to 9am & Sat to Sun 24x7

Contact	Contact details
Duty Manager	Redacted

Gold Command team

The Gold command team to be engaged when a BCP event occurs to declare a BCP event and agree strategic direction.

All employees whether members of Silver Command or not can contact Gold Command team members in the suspected or actual BCP event.

Primary Contact	Lead for	Contact Details	Secondary Contact	Contact Details
Redacted	Operations events	Redacted	Redacted	Redacted
Redacted	H&S and Environmental events	Redacted	Redacted	Redacted
Redacted	IT events	Redacted	Redacted	Redacted

Event team leads

Each event listed within the scope of BCP has a prime owner within the Gold and Silver Command structure who takes responsibility for leading and coordinating the activities, with the assistance of other team members and departments as directed:

Event title	Gold Command	Silver Command
BCP Access finance applications.docx	Redacted	Redacted
BCP AKJ Affinity.docx	Redacted	Redacted
BCP Autotask.docx	Redacted	Redacted
BCP Building Inaccessibility Process.docx	Redacted	Redacted
BCP CIPHR People Team System.docx	Redacted	Redacted
BCP Civil Unrest – Act of Terrorism.docx	Redacted	Redacted
BCP Civil Unrest.docx	Redacted	Redacted
BCP Corporate File Server.docx	Redacted	Redacted
BCP Cyber Attack.docx	Redacted	Redacted
BCP Data Loss.docx	Redacted	Redacted
BCP Data Loss.docx	Redacted	Redacted
BCP Fire Event.docx	Redacted	Redacted

Event title	Gold Command	Silver Command
BCP Flood or Water Event.docx	Redacted	Redacted
BCP Fortinet Firewall and VPN Connection.docx	Redacted	Redacted
BCP Infrastructure – Loss of Chassis.docx	Redacted	Redacted
BCP Infrastructure – Loss of Network Connectivity to DC.docx	Redacted	Redacted
BCP Infrastructure – Loss of Network Connectivity to Goswell Data Centre.docx	Redacted	Redacted
BCP Infrastructure – Loss of Power at Data Centre.docx	Redacted	Redacted
BCP Infrastructure – Loss of SAN Storage.docx	Redacted	Redacted
BCP Infrastructure – Loss Redundant Equipment.docx	Redacted	Redacted
BCP Infrastructure - Ransomware Customer Recovery.docx	Redacted	Redacted
BCP Infrastructure – Unauthorised Access potential Vandalism or Theft.docx	Redacted	Redacted
BCP Infrastructure Loss of Storage Network.docx	Redacted	Redacted
BCP Internet Circuits.docx	Redacted	Redacted
BCP LAN IN OFFICES.docx	Redacted	Redacted
BCP Microsoft Office 365.docx	Redacted	Redacted
BCP Natural Disaster.docx	Redacted	Redacted
BCP Office Communication Outage.docx	Redacted	Redacted
BCP Pandemic _ Epidemic Process.docx	Redacted	Redacted
BCP Patch Management.docx	Redacted	Redacted
BCP Prolonged Power Outage.docx	Redacted	Redacted
BCP Salesforce applications.docx	Redacted	Redacted
BCP Service Desk Avaya AXP.docx	Redacted	Redacted
BCP Severe Weather Disruption.docx	Redacted	Redacted
BCP WiFi (Wireless LAN).docx	Redacted	Redacted

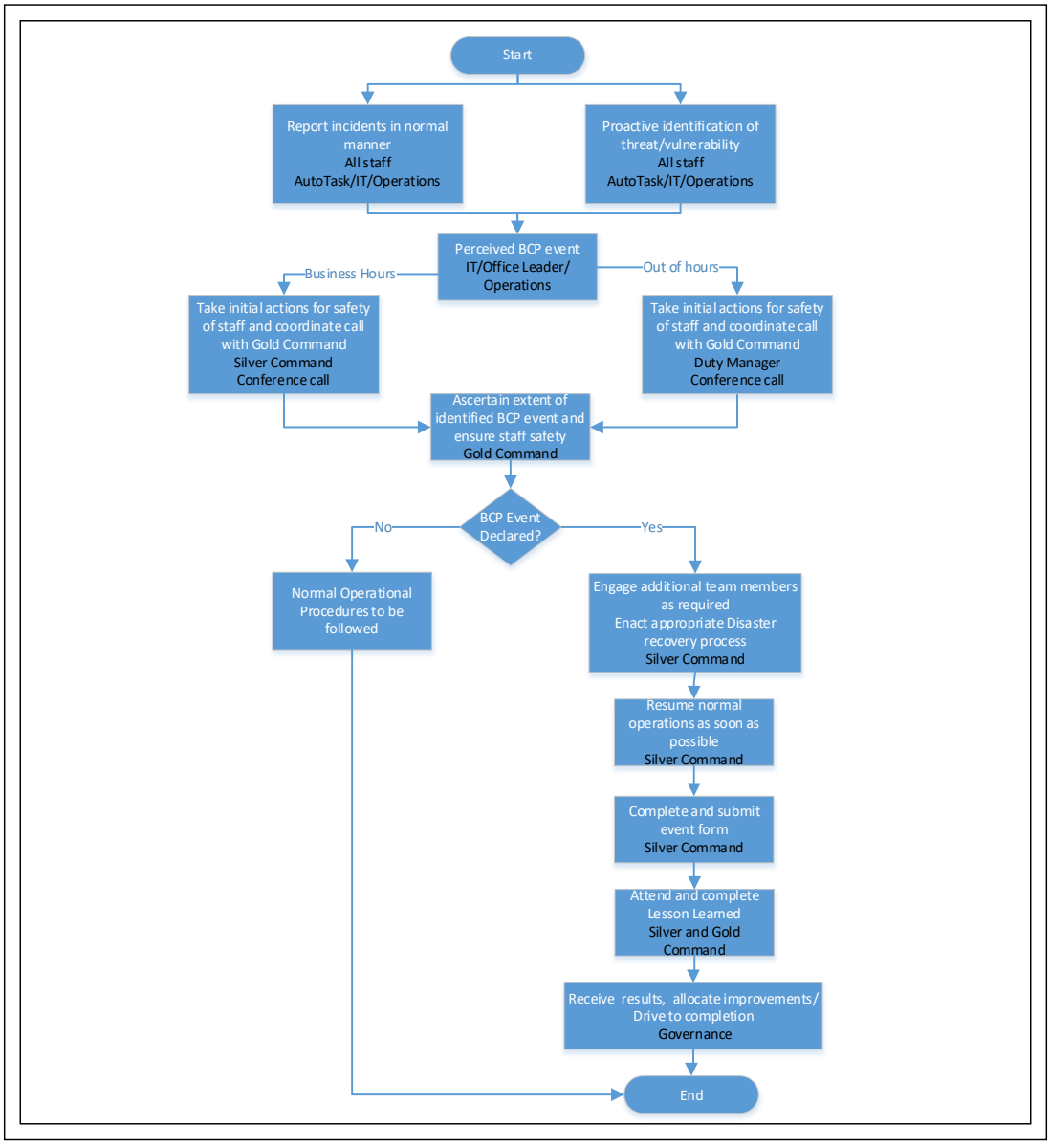
Responsibilities

Item	All Staff	Silver command	Gold command
Reporting	Identify and report an event that is (or may be) within the scope of the BCP. **Inform Gold Command of BCP event.** **Identify and agree recovery needs and priorities with Gold Command.**		**Evaluate information provided.** **Authorise a BCP event** **Agree Restoration priorities with Silver Command.**
Immediate Action	Take immediate action for staff safety, i.e. building evacuation.		**Confirm staff safety**
Communication	Receive and act on communication / instructions.	Communicate recovery progress and timeline to impacted departments, Customers, Supplier, Employees and Gold Command.	Communicate with the Media.
Recovery	Implement instructions and take actions as directed	Utilise the BCP and associated processes to successfully manage the BCP event. Work with departments, customers and suppliers providing instructions to aid recovery. Facilitate technology recovery and restoration activities, providing guidance on replacement equipment and additional expenditure required to Gold Command Provide mechanism to move staff and systems to alternate location as necessary.	Lead decision making process as BCP event recovery progresses. Authorise actions outside of Silver Command remit, i.e. Purchase of equipment, transport to alternative site.
Review	Provide feedback during and following a BCP event when requested.	Prepare post BCP account and complete a lessons learned session including recording detailed timings of the BCP event and improvements identified.	Review post BCP Event debrief report and attend lessons learned session.

Green text in the table above identifies items that are discussed during an initial telephone or conference call.

BCP Process

Headline Process Flow



BCP Management Procedures

The processes and procedures located within the IMS Portal shall be followed in the event of a BCP event. Processes and associated documentation are provided to enable personnel to complete an activity in a timely manner while ensuring theirs and all staff safety is maintained and communication with the appropriate teams, contractors, customer, and service providers is managed. Use the Process name hyperlink to view process detail

Event title	Description
BCP Access finance applications.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP AKJ Affinity.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP Autotask.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP Building Inaccessibility Process.docx	The process to be undertaken when the normal office location cannot be accessed or becomes inaccessible when staff are present
BCP CIPHR People Team System.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP Civil Unrest – Act of Terrorism.docx	Procedures and national guidance for threats of or actual Terrorist at Maintel offices and when travelling to and from work.
BCP Civil Unrest.docx	The process and procedures to be undertaken during civil unrest (Civil Disorder or Chemical Attack or Spillage) that could potentially affect normal business operations, including considering wellbeing of staff when travelling to and from work.
BCP Corporate File Server.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP Cyber Attack.docx	This process covers Cyber Attack and Heavy Traffic on Firewall
BCP Data Loss.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP Data Loss.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP Fire Event.docx	The steps to take when Fire is identified and ensuring staff are safe.
BCP Flood or Water Event.docx	The process when a water leak, water event or flood is identified.

Event title	Description
BCP Fortinet Firewall and VPN Connection.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP Infrastructure – Loss of Chassis.docx	Process to be undertaken when disruption has occurred within the Service Provider Infrastructure and Associated hosted applications
BCP Infrastructure – Loss of Network Connectivity to DC.docx	Process to be undertaken when disruption has occurred within the Service Provider Infrastructure and Associated hosted applications
BCP Infrastructure – Loss of Network Connectivity to Goswell Data Centre.docx	Process to be undertaken when disruption has occurred within the Service Provider Infrastructure and Associated hosted applications
BCP Infrastructure – Loss of Power at Data Centre.docx	Process to be undertaken when disruption has occurred within the Service Provider Infrastructure and Associated hosted applications
BCP Infrastructure – Loss of SAN Storage.docx	Process to be undertaken when disruption has occurred within the Service Provider Infrastructure and Associated hosted applications
BCP Infrastructure – Loss Redundant Equipment.docx	Process to be undertaken when disruption has occurred within the Service Provider Infrastructure and Associated hosted applications
BCP Infrastructure - Ransomware Customer Recovery.docx	Process to be undertaken when disruption has occurred within the Service Provider Infrastructure and Associated hosted applications
BCP Infrastructure – Unauthorised Access potential Vandalism or Theft.docx	Process to be undertaken when disruption has occurred within the Service Provider Infrastructure and Associated hosted applications
BCP Infrastructure Loss of Storage Network.docx	Process to be undertaken when disruption has occurred within the Service Provider Infrastructure and Associated hosted applications
BCP Internet Circuits.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP LAN IN OFFICES.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP Microsoft Office 365.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP Natural Disaster.docx	Actions to be taken when a variety of natural disasters are identified impacting business operations, including Storm, Lightning, Heat Wave, Landslides, Wildfire and Volcano disruption.
BCP Office Communication Outage.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications

Event title	Description
BCP Pandemic _ Epidemic Process.docx	The process to be used when notified of an epidemic or pandemic to ensure staff safety and continued business operations
BCP Patch Management.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP Prolonged Power Outage.docx	Steps to be undertaken during a prolonged power outage and the reliance upon Data Centre providers BCP where the prolonged power outage occurs at a data centre.
BCP Salesforce applications.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP Service Desk Avaya AXP.docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications
BCP Severe Weather Disruption.docx	The steps to be taken in conjunction with the Adverse Weather policy to ensure all staff are safe and wherever possible attend work.
BCP WiFi (Wireless LAN).docx	The process to be undertaken when disruption has occurred within the IT Infrastructure and 3rd party applications

Recovery Timeline

Unless otherwise stated within the relevant BCP process the following will be used as a timeline for the normal resumption of business within Maintel from the point of Gold Command BCP event declaration:

RTO	MTPD	Recovery Event
30 Mins	1 Hour	Department Contacts advised of situation and need to implement local BCP process
1 Hour	4 Hours	Identified impacted customers contacted
4 Hours	6 Hours	Service Provider infrastructure / communications available Service Desk available
12 Hours	24 Hours	IT infrastructure / communications available
24 Hours	36 Hours	Core departmental Managers and team leaders re-connected remotely
36 Hours	72 Hours	Secondary office site functional for day-to-day business operations

Communications

A BCP event has the potential to impact Maintel reputation and as we consider our reputation very seriously this section of our plan provides guidelines for communicating details and updates of an event.

Communication templates

The templates for Suspected and Actual incidents can be located within the IMS Portal and only accessible in the Maintel network:

- Communication - Initial - Actual Incident.docx
- Communication - Initial - EXTERNAL Suspected Incident.docx
- Communication - Initial - INTERNAL Suspected Incident.docx

Teams BCP site

A Teams site has been created for Gold and Silver Command to communicate during a BCP event. Additional members will be added as required.

CG - Compliance | Gold and Silver Command - BCP Event Records | Microsoft Teams

The Teams chat maintains a log of progress throughout the suspected or actual event.

Internal Communications

Silver Command are responsible for ensuring that, wherever possible, emails are sent to Maintel Executive and Senior Management distribution lists and relevant office distribution lists to advise that:

- A BCP event has been declared, including what the event is, what/where is impacted and when to expect the next update
- Where appropriate, the steps that employees should take
- The steps being taken to restore service and anticipated time to restore service/s

Where email is not available, contact the Office Leader /Location department managers to advise situation and request that onward communication to those impacted is undertaken.

Email example

- **Subject**: Business Continuity Event declared
- **Event description**: i.e. Blackburn Office evacuated, Service Desk no incoming calls etc.
- **Impact**: Include detail of what will not work, i.e. Outgoing voice calls not available, Blackfriars office not accessible etc.>
- **Action required by employees**: <i.e. Do not travel to Blackfriars office, Use mobile communications etc.>
- **Next steps:** Briefly describe steps being taken to remedy situation
- **Next Update**: <State time for next update, i.e. 1 hour, 4 hours etc.>

External Communications: Media/Regulatory

The nominated Gold Command team member is designated as the principal contact with the media (radio, television, and print), regulatory agency, government agencies and other external organisations following a BCP event declaration.

Media enquiries must be handled quickly and professionally. The media works to tight deadlines and failure to respond can result in inaccurate coverage and can damage relationships and Maintel reputation.

Any member of staff being approached by the Media or other authority should decline to comment, capture the following information, and pass the details to the nominated Gold Command member:

- Name of journalist
- Publication name
- Journalist's role (e.g. insurance correspondent, property correspondent etc.)
- A list of the questions the journalist is asking or the broad theme of the query
- Are they looking for an on the record comment from a spokesperson or just background information?
- Telephone number and e-mail address
- The deadline for responding

External Communications: Customers

Frequency

Communications are provided to customers as per contracted arrangements with general communication broadcast provided, as a minimum, every 4 hours.

In Hours

The Silver command team lead is ultimately responsible for ensuring customer broadcast and regular communication is provided through messaging on the Maintel Service Desk and/or Maintel external web site and directly to customers.

The Customer Success Management team (where associated to an impacted customer) and Account Managers are responsible for communicating with their allocated customers utilising the information provided by silver command.

Out of Hours

The Silver command team member is ultimately responsible for ensuring customer broadcast and regular communication is provided through messaging on the Maintel Service Desk and/or Maintel external web site and directly to customers.

Where additional resource is engaged during a BCP event to assist with communication, for example the Customer Success team, they will work and communicate with customers following the direction of the Silver Command team representative.

Supporting Documentation and Lifecycle

The BCP is supplemented with the detailed documentation for risk, process, and critical information. Documents (or associated link) are available within the IMS Portal and are reviewed, as a minimum, annually and after an event.

Annual review of documents and post BCP event review of processes and lessons learned assists with continual improvement of our BCP. Detailed BCP processes are securely stored within the IMS Portal.

BCP event register

The BCP event register, stored in the IMS Portal, records the summary detail of events and tests including:

- Date of test/event
- Test/Event description
- Start Time
- Finish Time
- Impact – Including location as appropriate
- Recovery Actions
- Review and Lessons learned output
- Improvements added to improvement process

Review and maintenance

To manage and continually improve, the following reviews take place and are recorded within the IMS Portal documentation:

Detail	Review time frame	Participants
BCP Event Register	Monthly	Compliance, Silver and Gold Command teams
Team member contacts*	6 monthly	Compliance Team
BCP event/s processed	Annually	Silver and Gold Command team
BCP event test scenario's	Annually	Silver and Gold Command team
BCP objective review	Annually	Silver and Gold Command team
Business Impact Analysis	Annually	Silver Command team
Business Continuity Plan	Annually	Silver and Gold Command team

** Changes to contact or other relevant details that are identified and occur outside of scheduled checks should be sent to* Redacted *as soon as possible.*

Risk and Maturity

To maintain the BCP objectives in line with Maintel service offering and continually improve the structure and knowledge/output of processes and teams, a Business Impact Analysis is maintained within IMS Risk to provide detail of current risks and a baseline for measurement.

The BCP events/risks are reviewed with Top Management and selected teams at least annually to measure the progress and maturity across all areas and services of Maintel with the addition of objective

update following a post event review, where a new business impact, BCP scenario or improvement required.

Maintel Risk Management Policy identifies the approach, methodology, appetite and responsibilities for risk.

Testing

A range of testing takes place during each annual cycle within the scope of BCP events using the BCP processes. The exercises may be in the form of a scenario-based desktop exercise, walk-through, mock disaster, call-tree testing or component testing.

Members of the Gold and Silver Command are responsible for arranging, co-ordinating and recording the exercises and, exercises may be notified to relevant personnel in advance or completed as a blind test.

All exercises are recorded in the BCP event register within the IMS Portal and reviewed as a real disaster event to complete the full process. Where an exercise review identifies that a process is not fully effective, the requisite process will be updated to reflect the lessons learned.

Business Impact Analysis critical status is used to identify the minimum testing recurrence:

- Gold = minimum annually
- Silver = minimum every two years
- Bronze = minimum every 5 years

Training

The Compliance Team is responsible for providing training information to;

- Ensure Maintel employees are aware of BCP, why we have a BCP and the benefits to Maintel, our staff, customers and suppliers.
- Ensure all Maintel employees are familiar with who to contact and what to do during a BCP event.
- To remove cause for panic during a BCP event
- To familiarise all staff with the benefit and use of process and documentation

The training is continuous by way of newsletter, conference call, webinar, questionnaire, face to face team and individual training. Training needs are identified from staff feedback, and compliance with best practise, regulations and ISO standards.

3.4 Business Continuity Staff Guide

Maintel has in place a Business Continuity Plan (BCP) to ensure we are prepared in the event of a range of disasters beyond our control that could impact normal operations for us and our customers. This guide provides an overview of the BCP and what you should do if there is a BCP event. Use this document for guidance only. The full BCP is available within the IMS Portal.

What we cover in the Business Continuity Plan

A range of events have been assessed as having an impact to Maintel normal operations.

The assessment of events considers the degree of impact at each of the Maintel offices and services used.

- Building Inaccessibility
- Civil Unrest
- Cyber Attack
- Fire Event
- Flood or Water Event
- IT Infrastructure and 3rd Party applications outage
- Service Provider infrastructure and associated hosted applications outage
- Natural Disaster
- Pandemic/Epidemic
- Prolonged Power Outage
- Service Desk outage
- Severe Weather Disruption
- Terrorist Attack

What should you do if there is a BCP event?

- Do not panic and never do anything that may put you or others in danger
- Ensure you and colleagues are safe
- If necessary, use the Fire Alarm to evacuate the building
- If Emergency Services are required contact them by telephoning 999 or 112: If you are unsure that the Emergency Services should be contacted, please ask your Line Manager or Office Leader.
- If safe to do so, carry out immediate actions to minimise the disaster, i.e. Cordon off any damaged area if possible
- Report the event to initiate Disaster Recovery using one of the following methods:
    - Advise your line Manager and/or Office Leader
    - Report to IT using Auto Task
- Follow instructions provided by the Silver Command team

Managing a business continuity event relies on a common-sense approach and all guides provided are to assist in returning to normal operation as soon as possible.

Business Continuity Process steps

Identifying a Business Continuity event

Some events such as Flood and Fire are easy to identify, other incidents that could lead to an event, such as issues with the telephone system or VPN connectivity may increase over time and not be immediately obvious that a business continuity event is underway.

IT, Office Leaders and Managers can assess the range of incidents being reported and identify if a disaster event may occur and engage Silver Command.

Managing a disaster

Once a business continuity event has been identified and immediate action taken to ensure staff safety, i.e. building evacuation, the Silver Command team liaise with the Gold Command team and initiate a recovery plan which includes communicating to each affected Office via the Office Leader to ensure that staff are provided with up-to-date information and instruction for any changes to normal working arrangements, i.e. an alternate location.

Wherever possible regular emails are sent to all staff advising the recovery progress.

Resolving an event

Silver Command team members collaborate with suppliers and teams throughout Maintel to resolve the event and/or provide temporary arrangements to ensure staff can complete, as a minimum, work that has been prioritised within their department.

On completion of the recovery, Silver Command advise all staff to return to normal working arrangements.

Post event review

All business continuity events, including test events, are reviewed for how well they were completed and the overall impact to Maintel business operations so that necessary changes to process or systems can be implemented and Maintel employees are better prepared should another event occur. Silver and Gold Command teams are included in the post event review.

Communication

Where a business continuity event has the potential to impact Maintel reputation, Gold Command is responsible for coordinating external communications with the Media (TV, Press, Radio), Customers, Suppliers, and Interested Parties. If you receive an enquiry from the Media, please take full contact details and forward to your Office Leader or a member of the Gold Command.

Responsibilities

	All staff	Silver command	Gold command
Reporting	Identify and report an event that is (or may be) within the scope of the BCP.	Inform Gold Command of BCP event. Identify and agree recovery needs and priorities with Gold Command.	Evaluate information provided. Authorise a BCP event Agree Restoration priorities with Silver Command.
Immediate Action	Take immediate action for staff safety, i.e. building evacuation.	Ensure staff safety.	Confirm staff safety.
Communication	Receive and act on communication / instructions.	Communicate recovery progress and timeline to impacted departments, Customers, Supplier, Employees and Gold Command.	Communicate with the Media.
Recovery	Implement instructions and take actions as directed	Utilise the BCP and associated processes to successfully manage the BCP event. Work with departments, customers and suppliers providing instructions to aid recovery. Facilitate technology recovery and restoration activities, providing guidance on replacement equipment and additional expenditure required to Gold Command Provide mechanism to move staff and systems to alternate location as necessary.	Lead decision making process as BCP event recovery progresses. Authorise actions outside of Silver Command remit, i.e. Purchase of equipment, transport to alternative site.
Review	Provide feedback during and following a BCP	Prepare post BCP account and complete a lessons learned session including recording detailed timings of the BCP	Review post BCP Event debrief report and attend lessons learned session.

	event when requested.	event and improvements identified.	

Green text in the table above identifies items that are discussed during an initial telephone or conference call initiated by Silver Command.

Communications Policy

To communicate key inputs and outputs of the Integrated Management System (IMS) Maintel have established the following communications policy.

External Communications

All IMS documents are classified as per the Information Classification Policy; only documents that are classified as Public may be distributed externally when requested.

Should any interested party request access to other classifications of documents they are to be invited to Maintel premises, have a non-disclosure agreement (NDA) in place and supervised whilst viewing the documents.

- No copies are allowed to be transferred to external parties.
- Redacted and therefore declassified versions of documents may be distributed to relevant external parties.
    - Documents may only be redacted by the authorised personnel.
- Only documents in protected Word or PDF format are permitted to be communicated to relevant external parties.

Internal Communications – Departmental

Each department relies on effective lines of communication. Key lines of communication utilised include:

- Regular employee updates: Email, Presentation, All Hands Calls
- Email
- Telephone
- Meetings; Video conferencing, Face-to-face
- Reports
- Systems

Internal Communications - IMS

All IMS and other certificate/accreditation related matters are communicated as detailed in the table below. Key to table:

- Roles: Who is responsible for communicating
- What: Outputs that are to be communicated

- When: Frequency of communication
- Who: Intended audience for the communication
- Method: How information is communicated

Roles	What	When	Who	Method
Management (Board)	Objectives	Annually (FY)	All Staff	Objectives and Targets in ESG at Maintel Website and IMS Teams area
Management (Board)	Management Review	Annually	SMT	Management Review Minutes
Management Representatives	Management Review	6 monthly	SMT	Operational Management Review Minutes
Management Representatives	Compliance	6 monthly	SMT	IMS Portal
Management Representatives	Information Security Risk Assessment	6 monthly	SMT	IMS Risk Improvement Form
Management Representatives	Health and Safety Risk Assessment and Environmental Impact Significance Assessment	Annually	Office Leaders	IMS Risk
Management Representatives	External Audits	Annually	Operating Board , SMT	Audit Reports Improvement form
Management Representatives	Internal Audits	Annually	Operating Board , SMT	Audit Reports Improvement Form
Management Representatives	BCP	Annually/Upon Changes	Gold and Silver Command	IMS Portal

Roles	What	When	Who	Method
Management Representatives	Policies	Annually/Upon request	All Staff, Certification Body, Designated Interested Parties	IMS Portal Email
Management Representatives	Processes	Annually/Upon request	All Staff, Certification Body, Designated Interested Parties	IMS Portal Email
All Employees	Incidents	Ongoing	IT, Security Team, CX Team, HR, Board	Email Accident Book Autotask
All Employees	Events	Ongoing	CX Team, HR, Board	Email Accident Book Autotask
All Employees	Non- conformances	Ongoing	SMT, CX Team, Board	Email Autotask
All Employees	Improvements	Ongoing	SMT, CX Team	Email Autotask

3.5 Competency, Training and Awareness Policy

Maintel recognises that all new employees and staff that are promoted or transferred will require adjustment in their new roles and provide the required support to these employees through the generic induction programme as well as addressing any individual needs that have been identified through the recruitment and selection process and/or discussion as part of regular 1-1 reviews or annual Performance Reviews. We recognise that effective learning and development offers benefits to the individual and the company, which ultimately contribute to the achievement of our KPI's, goals and overall success. The benefits include.

- higher standards of work performance
- greater understanding and appreciation of factors affecting work performance.
- sharing of ideas and good practice
- effective management and implementation of change
- encouragement of team spirit
- increased motivation and job satisfaction for the individual
- greater understanding of our business

In addition, Maintel regularly educate employees about the Maintel Integrated Management System (IMS), Privacy Protection, Health and Safety, Security, ISO Certifications and associated Regulations and Accreditations, ensures all employees understand how the company and IMS works, the policies and procedures and are provided the knowledge to be able to recognise risks and areas of improvement, i.e.

- Security awareness assists employees in recognising possible risks and vulnerabilities and aids Maintel in identifying new threats from the feedback they provide.
- Training in health and safety is a legal requirement and helps create competent employees at all levels within Maintel to enable them to make a far more effective contribution to health and safety, whether as individuals, teams, or groups.

Competence of individuals through training helps individuals acquire the necessary skills, knowledge and attitude which will be promoted by managers and supervisors throughout our organisation.

The Scope

All employees are subject to this policy and are required to complete induction training and IMS refresher programmes and policy acknowledgements, at start of employment, at annual refresher and at change of job role. Training needs will be reviewed because of job changes, promotion, new activities, or new technology, following an accident/incident and performance appraisal.

Employees must:

- participate in the induction training activities they have been required to attend or carry out.
- work according to the contents of any training they receive.
- ask for clarification of any points they do not fully understand.
- not operate hazardous plant or equipment, use hazardous chemicals, or carry out any hazardous activity unless they have been appropriately trained and instructed.

Responsibilities

- The Governance Team Leader is responsible for planning the annual IMS and associated Accreditation/Certificate refresher training programme.
- Human Resources are responsible for the provision of the new starter induction programme.
- Individual managers and directors are required to release their staff to undergo training.
- All employees take responsibility for their adherence to the Competency, Training and Awareness policy.

Induction Program

All employees included in the induction programme will be given support throughout their induction.

The induction ensures that all new starters can network and meet employees and understand:

- How the organisation operates
- The work of the different departments
- The support networks available to them
- The culture of the organisation including Values
- The history of the organisation
- The Benefits available to employees
- The Integrated Management System
- The Policies and Procedures that shall be adhered to
- The goals and aspirations of the organisation
- How their role fits in with the team and the organisation as a whole
- The Office, Space and Access
- Health and Safety: fire procedures, warning systems, actions to be taken on receiving warning, locations of exits/escape routes, evacuation and assembly procedures, first aid/injury reporting procedures, names of first aiders/appointed persons, instruction on any prohibition areas (i.e., no smoking), issue of protective clothing/equipment and its use, instruction under COSHH, mandatory protection areas, thorough instruction applicable to their particular duties at work etc.
- IT Equipment and System Access
- Key performance indicators

To ensure that all employees who have been promoted or transferred understand:

- How the new department works and its plans.
- Their job role and how it fits in with the team and the organisation.

Operations

Specific areas have additional requirements, predominately the technical areas where definition and recording of specific skill sets and requirements take place to provide the products and services within the Product portfolio. The Chief Operating Officer shall ensure the necessary number of employees are available with the skills required to deliver Maintel services. The consequences of not having enough skills available include increased downtime of systems, slower turnaround of requests and increased risk to the business.

To determine whether there is a requirement for training, a skills questionnaire was created based on the skills identified as required using the following definitions.

Skill Level	Summary	Description
3	Support Level	Completed accredited training and recognised as an expert
2	Trained	Complete training or knowledge transfer
1	Semi-Skilled	Understanding of the product set but no formal training or knowledge transfer
0	No Skills	No knowledge of the product

- Individual's skills are recorded in the skills matrix.
- Technician's certifications with Manufacturers are available through the Manufacturer web site, the Development & Accreditation document and employee's record achievement on My Maintel.
- The skills matrix is updated at least once during each financial year for all technical staff.
- Annual appraisals and one to ones are used to update the matrix and develop individuals.

For each of the services provided an assessment is made regarding:

- the technical skills required to support that service.
- the minimum number of employees needed at a medium skill level or above.
- the highest skill level required.

Services requirement is compared with the current level of skill in the skills matrix and recommendation for training, risk management and involvement of third parties is made.

Risk and Analysis is undertaken using the Skills matrix with attention to.

- the number of people who have a skill level of Medium or higher in a specific area.
- the highest skill level in a specific area

This enables risks to be identified and recorded where there are not enough people with a working knowledge of a specific area (i.e., medium level or above) making the relevant service vulnerable to staff unavailability perhaps through workload or absence and where the level of expertise within the team is not judged to be sufficiently high to support the service in all circumstances e.g. when advanced configuration is required

To address identified risks, the following alternatives are considered, and the most sensible/practical option adopted:

- Informal training by existing staff with a higher level of skill
- Formal training via online or classroom courses
- Recruitment of additional staff with the relevant skills
- Use of third-party resources on an ad-hoc basis e.g., contractors or consultancy
- Use of third-party resources via an agreed support contract which gives guaranteed access to the required level of skill.

Integrated Management System

The IMS training objectives cover three areas: the organisation, the job, and individuals. All employees will need to know about:

- the relevant policies.
    - health and safety
    - business continuity
    - information security
    - environmental
    - quality
- the structure and system for delivering this policy: IMS Portal.
- Employees need to understand which parts of the IMS system are relevant to them, to understand the major risks in our activities and how they are controlled.

Managers and supervisor training needs include:

- leadership and communication skills
- management techniques for safety, security, business continuity, data protection, environment etc.
- skills on training and instruction
- risk assessment
- legislation, i.e., health and safety and data protection
- knowledge of our planning, measuring, review and audit arrangements.

All our employees training needs will include:

- relevant health and safety hazards and risk
- the health and safety arrangements relevant to them
- communication lines to enable problem solving.
- business continuity
- Data Protection
- Information Security & Cyber Security

Card holder data environment

Enhanced training is provided to employees who will work with cardholder data, have access to the cardholder data environment, or have access to any system that can affect the security of the cardholder data to comply with PCI-DSS.

Development options

The performance review process encourages discussion about putting into place actions to focus development options. Development is not just about attending a training course or workshop. To help identify the most suitable option, there are several development solutions which should be considered.

Option	How this helps development
Coaching and Mentoring	Coaching and mentoring are good development options because you tend to get the benefit of someone else's expertise and experience. A mentor can often be more senior and focuses on behavioural development, whilst coaching can be more informal and can be at the same level.
Attending a courseor workshop	Courses focus on both behavioural and technical development. Workshops are great because they develop knowledge and skills to take back and apply in the job role and delegates also get the opportunity to share experience and best practice with other peers.
Delegation andprojects	We can also further develop by undertaking a project or additional tasks. This can provide us with invaluable experience and really helps when seeking to develop specific skills or if we have a desire to develop out careers. By being given the opportunity to champion or lead tasks gives valuable experience and exposure, it can also raise their profile.
Performance Review	The review process is a good way of receiving constructive feedback that will identify development aims and actions to improve knowledge, skills and also, confidence in work.
Feedback	Gaining feedback from others in your network generally broadens your understanding of how you are perceived. Generally known as 360
Gaining a qualification	Gaining a qualification can be an essential aspect for some roles, whilst onother cases, qualification may not an essential requirement, but will undoubtedly enhance an individual's knowledge and skills.
Books and Journals	For some books, journals and online reading are another way to increase knowledge and expand understanding.
Work shadowing	Spending time with an existing jobholder is a great way to get a usefulinsight into the skills and make up of a job role.
Attending seminars	Many professional bodies hold seminars and events focused around particular subject areas. This is a good way to expand your understandingof the issues and current trends in particular industries. You can get exposure to specialist speakers and a networking opportunity.
Subscribing to websites	There are many websites available, including profession specific sites designed to give you insight and current thinking across industry disciplines. Many websites offer a mailing service where they offer regular electronic newsletters

Training needs analysis

Training needs are identified through 1-2-1 meetings, business needs, annual review and changes to regulations and certification compliance requirements.

Delivery and Records

Where possible the awareness training is provided by means of the Maintel Learning Management system (LMS), an online e-learning tool for which each employee has a specific account.

Records of completion and where appropriate, achievement, are maintained within the LMS.

Yearly reminders are sent out to complete the online mandatory training and review of Maintel policies.

Additional training is provided through.

- Team meetings
- Weekly company newsletter
- Email information messages

Training Process

Where training requires budgetary spend, the following procedure should be followed:

- Any employee wishing to undertake any form of training should, in the first instance, contacttheir manager to explain the benefits to themselves and the company, the type of course, syllabus, qualification to be achieved and related costs (if this has not already beencompleted as part of the Performance Review process).
- The Manager should then use Focal Point to request budgetary sign off for these costs. This should detail the priority and business justification as well as the details of the course.
- Once complete, the form will go through the relevant electronic authorisation process, on completion a purchase order number will be sent to the requesting manager.

It is recommended that employees maintain their Training and Development record on the People Team system.

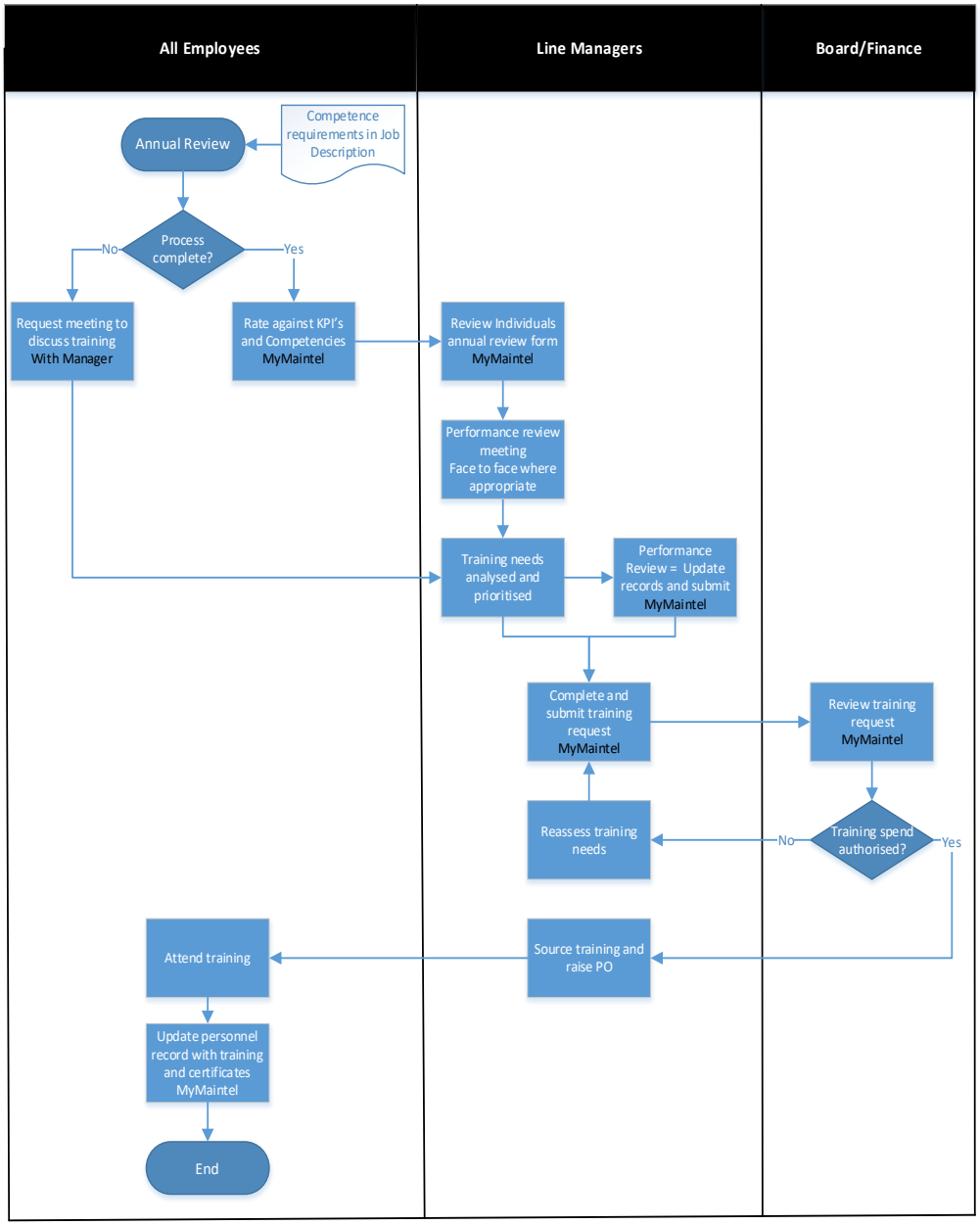
Education/Qualification Support

Maintel supports the principle of training its staff for the job and it is our practice to help you improve performance and develop your potential by education/qualification as the business grows and changes. In the event that the Company pays for you to attend a course of study (excluding levy apprenticeship funding) and you then leave the Company, the following amounts will be due from you upon leaving the Company:

- Leave within 3 months of completing the qualification: Repay - 100% of course fees.
- Leave within 6 months of completing the qualification: Repay – 75% of course fees.
- Leave within 9 months of completing the qualification: Repay – 50% of course fees.
- Leave within 12 months of completing the qualification: Repay – 25% of course fees.

Expenses incurred by attending an approved course of training or further education will be paid back to you, but you must first obtain approval from your manager. You may also reclaim the costof required textbooks bought for the course.

Annual Review process



3.6 Exchange of Information Policy

This policy sets out the process to be followed in Maintel both within the Country and outside by all employees.

Electronic Media

- When media is in electronic format all documents shall be virus checked prior to delivery.
- All information shared with Customers and third parties, i.e., Copy of Presentation completed shall have all internal notes removed and be presented in a PDF format.
- All electronic media is adequately protected to ensure no damage can ensue during transportation.
- All electronic information is in a format which can be encrypted
- All electronic information that contains personal data shall be encrypted.
- A classification, i.e., Confidential, Public etc. as per the Classification Policy shall be used and all information clearly marked

Hand Delivery

- All media will be securely handled as per the Mobile Equipment Policy. This includes hard copy media.
- Media will only be exchanged in a secure manner. This means in the client's premises / office.
    - A signature is required for the receipt of any information delivered in this manner.

Log ins and Passwords

Providing Logins and passwords electronically should be avoided where at all possible. On the few occasions it is necessary to provide the login and password in electronic format, i.e., Email, the following guidelines shall be adhered to:

- The identity of the recipient shall be confirmed prior to sending information
- All e-mails sent must be encrypted and sent to the intended recipient, not groups nor service desks and their equivalents
- Log In credentials and complete Passwords shall not be included in the same email
- Advise recipient that information contained within Emails is insecure when transmitted through the medium
- Use secure sending platforms e.g., Bitwarden where possible, password protect and encrypt any data sent
- Ensure recipient has received initial email, i.e., Log In name/credential, prior to sending password
- If possible, separate the media for Login credential and password, i.e.
    - Login Credential/Name sent by E-mail
    - Partial password sent by text to the recipients confirmed mobile device and the rest provided verbally over the phone to the recipient.

Postal Service

- When electronic media is to be sent via the postal service all confidential documents contained on the media (be it CD/DVD or a Pen Drive) must be password protected and encrypted.
- Publicly available uncontrolled electronic media is sent through normal postal channels. Media containing non-public data must be sent via trackable, direct delivery, not normal postal channels
- All electronic media is adequately protected to ensure no damage can ensue during transportation.

Incoming post

- All incoming post addressed to Maintel should be opened by the Receptionist, date stamped and passed to the relevant member of staff. Post marked for the attention of an individual will be passed directly to the relevant member of staff unopened. Any post marked as 'Private and confidential' will be passed unopened to the addressee, a director or to the Head of Department.
- Junk mail should be discarded.
- In the absence of the Receptionist a designated member of staff will deal with incoming post.
- Particular attention should be paid to urgent and important communications.
- All cheques received by post should be immediately passed to the Finance Department to be date stamped and logged. Cheques must be banked within 5 working days.

Outgoing post

- All outgoing correspondence should be written in correct English, should be free from errors, neatly typed and bearing the company logo.
- Any Private and Confidential correspondence should be clearly marked as such.
- Important letters should be copied to relevant staff members for their information.
- Large mail outs (e.g., client results dispatch) requiring mail sacks must be kept in the collation area when they will be moved to the post area for collection.

Telephone Messages

- In all cases take down the name of the caller, his/her telephone number, company name (if relevant) and a clear and understandable message. Telephone numbers should be repeated to the caller so that they are correctly taken. The message should then be passed on to the relevant person via email immediately.
- Any important messages should be immediately communicated to the relevant member of staff via phone or in person.
- All messages should be dealt with and responded to the same day.

Faxes

- If you send a fax, it is not always necessary to send a hard copy. Use your discretion and avoid unnecessary duplication. Only important documents or letters sent by fax should have a hard copy sent by mail.
- Faxes received should be immediately passed on to the relevant person.

Hardcopy Files

- Files should be kept neat and in date order.
- Duplicate copies of letters or documents should not be placed in files.
- Filing must not be accumulated, and all items must be filed in the correct file at the end of the day and secured appropriately:
    - Cabinets with documents containing personal data shall be locked
- From time-to-time files need to be "pruned" in accordance with retention periods:
    - Personal Information which is no longer necessary for the purpose it was collected shall be destroyed.
    - Older material that does not contain personal information which is no longer necessary and/or has reached its retention period is destroyed or archived to a secure storage facility.

3.7 Information Classification Policy

This policy outlines information classification at Maintel. Classification of information acts as a mechanism to ensure that all information is organised appropriately, for ease of storage, management, and security.

What can I share?

Only Public information shall be shared with external parties; should an external party request a document with an Internal classification, this can be viewed with a representative from Maintel present, after approval from the document and process owners, alongside any controls specific to the information document.

No documents can be removed from Maintel's site(s), and notes cannot be taken on the content of these documents.

Classification levels

Maintel has four levels of information classification.

The classifications cover all information, including but not limited to, electronic, digital and hard/physical copy media.

These classifications apply to Maintel's information and information received from clients and/or suppliers.

All IMS documentation held on the IMS portal is classified as per this policy.

The table covers

- Classification/Label of information,
- Description of information
- Handling of information.

Classification / Label	Description	Handling
Restricted	Information that is extremely sensitive and confidential, requiring strict controls to ensure need-to-know access. It may include data that if its confidentiality is compromised, or unauthorised access is gained, could lead to significant charges, fines and/or irreparable damage to the company and/or its customers.	Information must be encrypted when stored and transmitted, if it is digital or electronic. If physical and stored or transferred, this must be done using a process comparable to encryption, preventing any unauthorised person's access. Information must not be released to any person outside of the restricted permissions set.

Classification / Label	Description	Handling
	For example: proprietary company or customer information, information covered by an NDA.	Only authorised persons must have access to restricted information in line with Role Based Access Control.
Confidential	Information that requires specific access authorisation, often to a limited audience, must be internal to the company and may include sensitive data. **For example**: financial details, national insurance numbers, contracts, pricing documents, test reports, annual review information. Employees have access to confidential information that is relevant to their job in line with Role Based Access Control.	Information must be encrypted when stored and transmitted, if it is digital or electronic. If physical and stored or transferred, this must be done using a process comparable to encryption, preventing any unauthorised persons access. Information must not be released to any person outside of Maintel without prior permission from Maintel compliance lead. Confidential information must not be shared nor transferred to any public forum or publication.
Internal	Information strictly for internal company staff who are granted permission to the content. **For example**: internal update of company's financial position, business plans, newsletters, company project updates	Information for Maintel staff. This information shall be for internal consumption only.
Public	Information accessible to all employees and classified as Public by its author/owner. **For example**: a company press release by the Marketing team, information within the IMS Portal that has been reviewed and allocated a public classification.	Information that is public can be freely used by all, and/or distributed without repercussion.

Responsibilities

All employees, contractors and temporary employees shall abide by the Information Classification Policy when handling and accessing information.

It is the departmental manager's ultimate responsibility to ensure that these classifications are adhered to by their staff.

3.8 Information Security Incident Policy

To effectively maintain the confidentiality, integrity and availability of information assets, security of personal data and identify vulnerabilities Maintel proactively identify threats and have in place this policy to provide all staff with guidance on the process for recording suspected and actual security incidents including personal identifiable information (PII) breach. All security incidents are identified and handled in a timely and effective manner and actions recorded within the Improvement process.

This policy establishes management direction and accountability for information security incident management and is to ensure the identification and resolution of security incidents, minimising their business impact and reducing the risk of occurrence of other similar security incidents such as:

- Information being corrupted, destroyed, stolen and/or lost.
- Compromised passwords
- Policy and Privacy (PII) breach.
- Computer performance being disrupted and/or degraded.
- Financial and reputational loss.
- Productivity losses being incurred.
- Vulnerability identification

This policy applies to all Maintel employees, including temporary staff, contractors, consultants, subsidiaries that share the Maintel technology infrastructure, third parties and service providers utilising Maintel network resources. The policy covers the following resources.

- Network devices
- Firewalls
- IDS/IPS
- FIM
- Anti-Virus
- Servers
- Computers/Laptops
- Applications
- Databases
- Operating systems
- Printers
- Email
- Internet access
- Physical access
- Logical access
- Audit logging
- Segmentation controls (where used)
- Personal Data (PII)
- ICON Environment
- IT Environment
- Cloud Services

All security incidents, no matter how minor, are recorded on Autotask.

What is an Information Security Incident?

An information security incident is defined as a breach of policy or an adverse event that has led or could lead to a compromise in the confidentiality, integrity or availability of information owned or processed by Maintel. Incidents could be accidental or malicious.

The following lists examples of security incidents but is not an exhaustive list.

- Unauthorised access to information.
- Personal information (PII) data breach or suspected breach.
- Identifying and/or spreading of a Malware on the network; (computer viruses, worms, Trojan horses, most rootkits, spyware, and other malicious and unwanted software).
- Denial of Service attack (DoS / DDoS) or Action that leads to unauthorised denial of service.
- Unauthorised modification of information.
- Unauthorised disclosure of information.
- Discovering a rogue Wi-Fi Access Point.
- Loss or theft of assets containing information.
- Failure to protect information in line with the relevant policy (e.g., Visitors Policy, Acceptable Usage and Secure Disposal Policy).
- Malicious or careless employees.
- Social engineering.
- Spam.
- Spoofing and phishing.
- Man-in-the-middle attacks.
- Password compromise

Proactive monitoring

New viruses and malware programs are discovered every day, these include but are not exclusively, viruses, Trojans, worms, spyware, adware, and toolkits.

To protect Maintel from emerging threats we utilise regular threat intelligence to identify new viruses and malware programmes, add these to our risk register and implement mitigating actions as required. We use reputable sources for obtaining threat information.

Identified threats are risk assessed in accordance with the Risk Management Policy and, where applicable, are recorded within IMS risk. Each risk is allocated a Low, Medium, High, or Very High-risk value based on the Risk Score, Risk Indicator and Maturity level of controls.

Reporting an Incident

Employees report all security incidents via Autotask. Should the IT department deem the incident requires further investigation or escalation this will be conducted initially within Autotask, and where appropriate recorded within the Improvement Form.

Autotask has been configured with an escalation criteria and permissions set for viewing the information.

When reporting an incident using Autotask this should be completed as soon as possible and immediately where personal data is involved.

Maintel's Security partner, RelianceCyber report security incidents impacting Customers using Maintel operational network on Autotask Trouble Ticketing System. Reporting a security incident impacting a customer can be performed proactively (i.e., from a Maintel initiative, before the Customer would have noticed the breach) or as a mandatory consequence of getting alerted by the Customer (reactive support). An Autotask ticket is raised, and an Initial investigation is completed and where changes/improvements are identified, the work is completed works and an improvement log entered.

The investigation also considers reporting to relevant supervisory authorities and completing the supervisory authorities risk assessment.

Cyber Security Incident

In the event of a cyber-security incident and/or identification of an actionable vulnerability the Cyber Attack Process detailed within the Business Continuity Plan stored within the IMS Portal is followed by IT and the Disaster and Emergency Management teams.

Remediation plan

Maintel remediation plan follows a 5 steps process to make sure we deal with an issue.

When an information security incident is discovered, it is essential to act comprehensively and quickly.

It is important to bear in mind that these steps are not sequential – in practice, it will be necessary to think about most of them in parallel, particularly in the initial aftermath of the incident where the priorities will be to contain it to mitigate any risk of further damage or loss of data.

1- Mobilise an incident response team

An incident response team is formed and includes all relevant internal stakeholder groups, such as the Engineering team to investigate the breach, the Data Protection Officer, our security partners, and the Information Security Team.

When the breach affects a Maintel Customer, Operations has the lead of managing the incident, whereas when the vulnerability impacts the Maintel IS network, the Head of IS takes responsibility of mitigating the impact and reporting any resolution's progression to the Board. In every information security incident reported, a unique senior member is nominated to lead the incident response team.

For all Personal Data breaches, the Data Protection Officer is engaged.

Data is classified for recovery;

- Non-archived Restricted data recovery is considered to have a priority of Very High
- Archived Restricted data is considered to have a priority of High.
- All data classified as Confidential is considered to have a priority of Medium.
- All data classified as Public is considered to have a priority of low.

2- Secure systems and ensure business continuity

Following a security incident, the first key step taken from a technical perspective is to secure the Systems to contain the breach and ensure it is not on going. This could mean that Maintel would need to take the decision to isolate or suspend a compromised section of its network temporarily or even the entire network. This can, of course, be extremely disruptive and potentially costly for the business.

3- Conducting a thorough investigation

An investigation is carried out as to the facts surrounding the breach, its effects and remedial actions taken. The designated senior member or Data Protection Officer shall then take the lead on the

upcoming investigation. Where there is potential employee involvement in the breach, the investigation will also need to consider any applicable labour laws, and the investigation team should therefore consult and involve HR representatives as appropriate.

4- Manage public relations with Customers and legal authorities

The following work stream taken by the incident response team is around managing external communication with our customers and to the competent authority, i.e.

- Information Commissioner Office
- Communication regulator OFCOM
- Local or National Government or Enforcement agencies
- Card Payment Brands

    - Amex
    - Visa
    - Mastercard

particularly where it involves personal identifiable information being compromised and being in the public domain, or where the relevant data protection legislation requires the affected individuals to be notified. Maintel will use its reasonable endeavour in being timely when managing announcements to the public and being accurate in the messages that we will be given.

For all Personal Data breaches, the Data Protection Officer is engaged and manages the communication to the Supervisory Authority within 72 hours of the incident and the Data Subjects as soon as possible and without any undue delay.

5- Incurring liability

There are many ways in which Maintel could incur liability. There will very often be regulatory liability resulting from personal data and cyber security breaches. Current law requires organisations to have in place appropriate technical and organisational security measures to protect personal data.

The Data Protection Officer and/or Board representative in conjunction with the Maintel Legal Department manage liability claims that may arise.

Incident Descriptions

Physical Security Incident

A physical security incident is defined as any event where an unauthorised person attempts to gain or does gain access to any Maintel property, including buildings and estates. It also relates to events such as security-relevant access and exit points being left insecure or any incident which would be considered a crime, such as criminal damage, assault, or fraud. Examples.

- Unlocked or open gates on the estate boundary
- Unlocked or open doors to a secure internal area, which could lead to unauthorised access not only by external people but also by employees.
- Employee is injured or threatened by another.

- Property is destroyed or damaged intentionally or recklessly.
- Failure to comply with the physical security requirements (e.g., allowing unknown people to 'tailgate' through security barriers).

Technical Security Incident

A technical security incident is defined as any event that has resulted in or has the potential to result in the loss or theft of technical equipment belonging to Maintel and which does not contain data.

Incident of Theft

An incident of theft is defined as an event to permanently deprive the owner of their property.

3.9 Improvement Process

The main purpose of the Improvement Process is to drive continual improvement within Maintel by identifying and rectifying all potential and actual incidents or process failures.

Maintel have ascertained that the following elements are to be considered for enabling improvements within our Integrated Management System (IMS). This lists the terms used to ascertain nonconforming materials, products, services, processes, incidents and how improvements are defined.

- **Nonconforming Process**: Process is not being followed or has been incorrectly documented
- **Nonconforming material, product or service**: the material, product or service has been ascertained as not being fit for purpose or to requirements.
- **Incidents**: An action or activity that can potentially affect business operations, such as:
  - Supplier Deficiencies
  - Customer Complaint
  - Security Incident
  - Environmental Incident
  - Accident / Near miss
  - Improvement
  - Customer feedback
  - Lessons learned
  - Knowledge
  - Service Desk system
  - Personal Data Breach
- **Opportunity for Improvement**: An action or activity that will enhance the process, product or service to ensure it remains compliant with the IMS requirements

Should any nonconforming products, services, or materials (including equipment) result in a disruption tonormal business service, which are deemed to not be resolvable through normal processes then the Business Continuity Plan (BCP) is enacted. Should the company image be affected by any nonconforming products, services, or materials then this is a Business Continuity incident and the BCP should be followed.

Responsibility

- The Compliance Team has overall responsibility for this procedure.
- Employees are required to highlight areas for potential improvement and suspected non-conformitieswithin any aspect of the IMS

Corrective Action

The is to establish and outline the process for identifying, documenting, analysing, and implementing corrective actions to eliminate actual or potential nonconformity of the processes, products,services or materials.

Preventative Action

Maintel consider preventative action throughout the Integrated Management System through such mechanisms as

- Risk assessment
- Objectives and how we achieve themManagement review
- Internal audits
- Constant monitoring and measurements of the processes and activities detailed in the IMS.

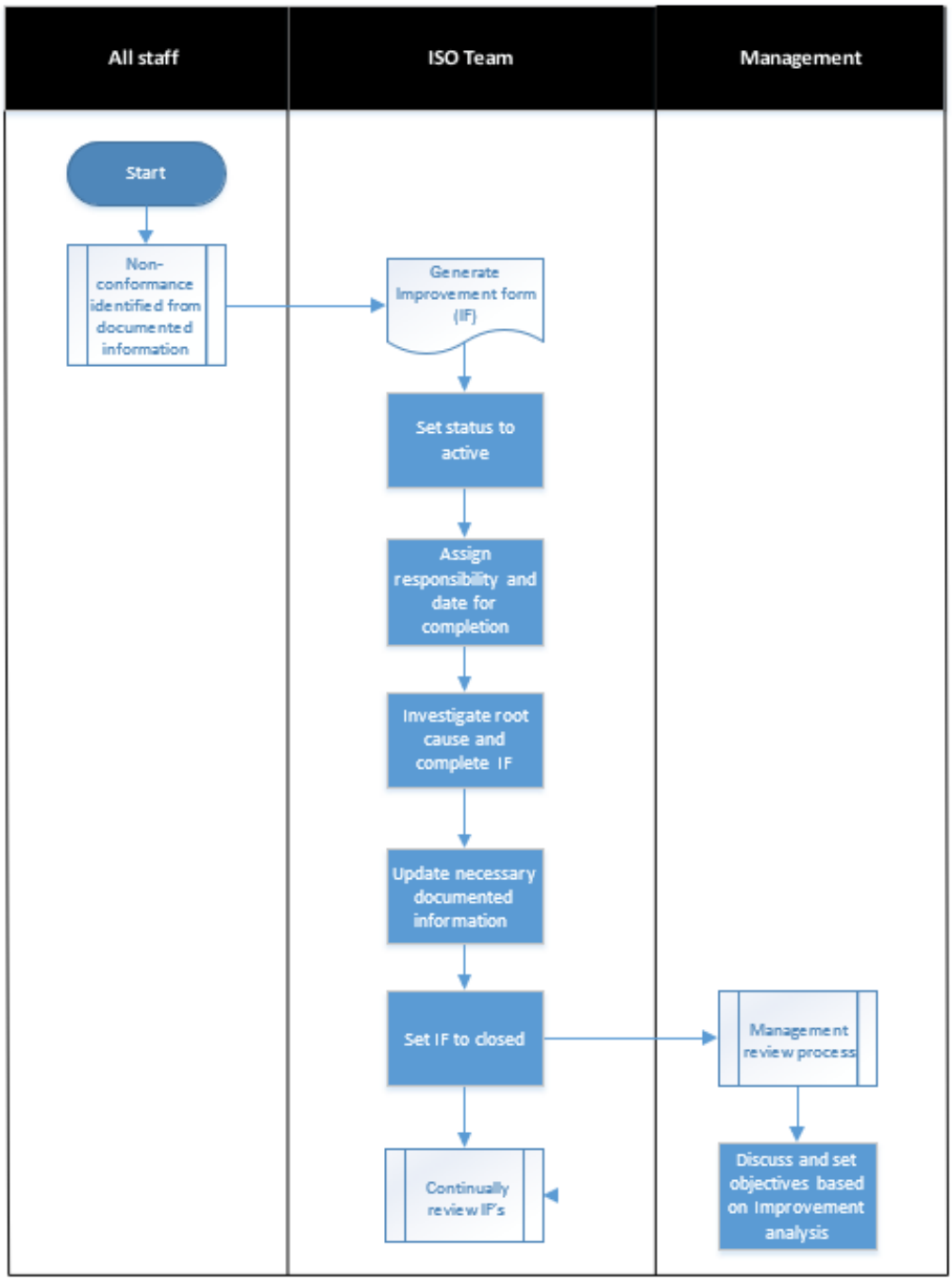
Documented information

Information	Recording mechanism
Accident / near miss	Autotask Improvement form
Customer complaints	Improvement form Emails Service Management System
Customer Feedback	Email Social media Service Management System and Reports Improvement form
Environmental Incident	Improvement Form IMS Risk
Knowledge	My Maintel(Staff Handbook/Job Descriptions) LMS IMS Portal
Lessons Learned	Improvement form Service Desk system
Nonconforming process	Improvement form
Nonconforming material	Improvement form

Information	Recording mechanism
Nonconforming product	Improvement form IMS Risk
Nonconforming service	Improvement form IMS Risk
Personal Data Breach	Autotask Improvement Form
Supplier deficiencies	Supplier evaluation form Improvement form
Security Incident	Improvement form Autotask
Service Desk System	Auto Task Autotask

Reporting non-conformances

Reports of non-conforming processes, materials, products, or services may result from internal or external audits, or as part of routine operations, where an individual or department may identify noncompliance. This procedure is applicable to corrective/preventative actions related to non-conformance and is to befollowed by all employees



3.10 Internal Audits Process

The purpose of this document is to describe the process for undertaking internal audits to assess the effectiveness of the application of the Integrated Management System (IMS). This promotes effective management of the IMS through the provision of information with analysis, appraisals, recommendations, and pertinent comments concerning the activities reviewed.

Responsibility and Authority

The Compliance Team and Management Representatives are responsible for

- Preparing and managing the audit programme and schedule
- Defining the criteria, scope and method of internal audits
- Defining audit duties with the Internal Auditors
- Providing feedback on the internal audit report

The Internal Auditors are responsible for:

- Undertaking internal audits in accordance with relevant standards
- Observing all requirements relating to privacy and confidentiality
- Providing an internal audit report to management for consultation
- Ensuring management comments are included in the final audit report

Employees are responsible for:

- Attending interview when requested
- Providing feedback on the draft internal audit report
- Incorporating findings of the internal audit into operational activities
- Ensuring that Internal Auditors are given full access to records.

Scope

- All members of the company will be audited in their day-to-day role and possibly required to audit other employees.

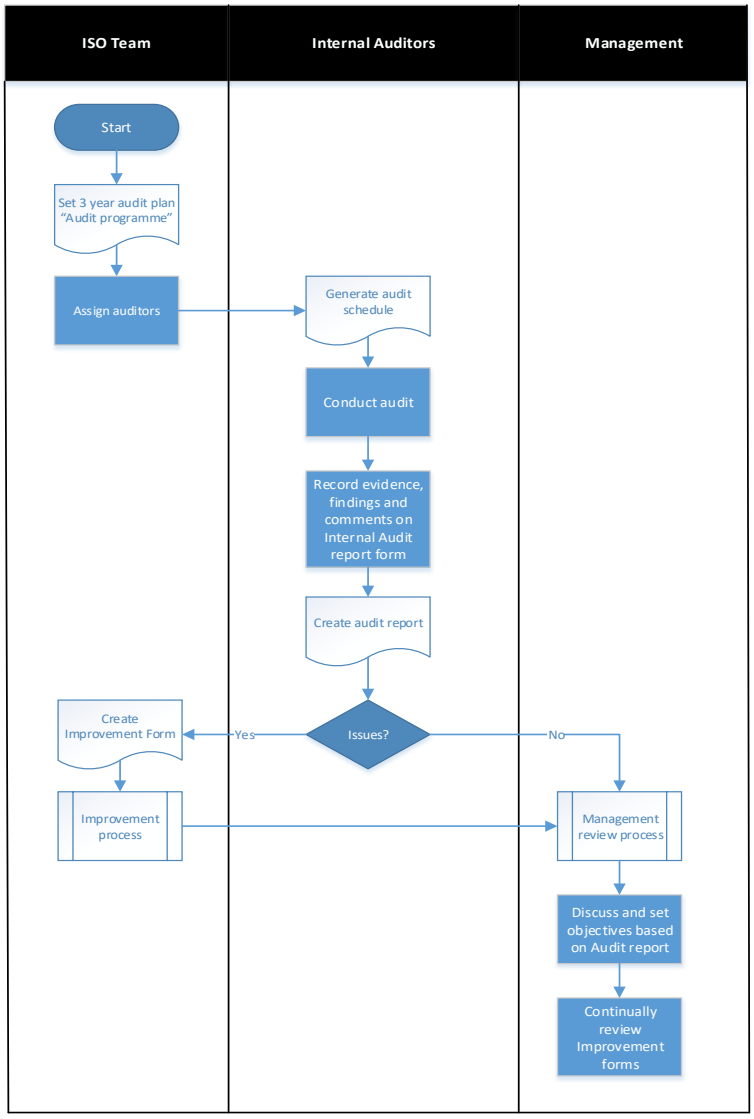
- All evidence gathered during the internal audit is categorised by the following levels of conformity to documented information, activities, and ISO or other certification compliance: -

Conformity categories

Category	Description
Compliant	No issues found. Process and actual practice witnessed to be working effectively
Major	Evidence of a total breakdown in a process or practices that result in non-conforming product or services

Category	Description
Minor	Evidence of a process or activity not being fully followed, multiple minor non-conformances can result in an escalation to a Major non-conformance
Opportunity for Improvement (OFI)	Evidence that whilst a process or activity is being followed, there is room to improve the actions taken. An OFI is also considered if the current activity could result in a minor nonconformity being raised in the future.
Compliment	Evidence that suggests that the activity is above and beyond what is documented. This is also a sign of "Best Practice" being utilised

Process diagram



3.11 Legal and Regulatory Compliance Policy

The Operations Board and Senior Management, in conjunction with the Legal team, are responsible for identifying and ensuring Maintel complies with all relevant Legal Requirements relating to environmental, health and safety, information security and business issues.

The objective of this policy is to ensure that all relevant legal and regulatory requirements are effectively identified and communicated throughout [Company]. All members of staff are required to comply with legal and regulatory requirements.

Relevant national legislation is identified through the risk management policy. Where the scope of operations is outside the national legislative remit, then other relevant legislation for the country of operations should be identified and communicated.

All legislation that is reasonably applicable to Maintel shall be kept within the Legal Register together with a brief description of its requirements.

The mechanisms used to ascertain relevant legislation within the UK and the European Union are: -

UK Legislation- http://www.legislation.gov.uk/

EU Legislation - http://eur-lex.europa.eu/en/index.htm (as it may continue to apply to the UK under sections 7A or 7B of the European Union (Withdrawal) Act 2018).

EU Legislation Summaries - http://europa.eu/legislation_summaries/index_en.htm

Legislation is reviewed on an annual basis, or as required when significant changes occur, such as the European Union (Withdrawal) Act 2018. All members of the Compliance Team are encouraged to sign up to relevant updates for their sphere of knowledge and update the team at the Management Review Meetings. At these meetings, if actions are to be carried out following legislative updates, this information is to be escalated to Board level for decisions on communication.

The Legal Register provides a list of key legislation applicable to Maintel and is utilised to undertake regular reviews and is reviewed as part of the Management Review of the Integrated Management system to ensure that all legislation is correctly identified and communicated. The legal requirements of Maintel are communicated as per our Communications Policy.

Responsibility

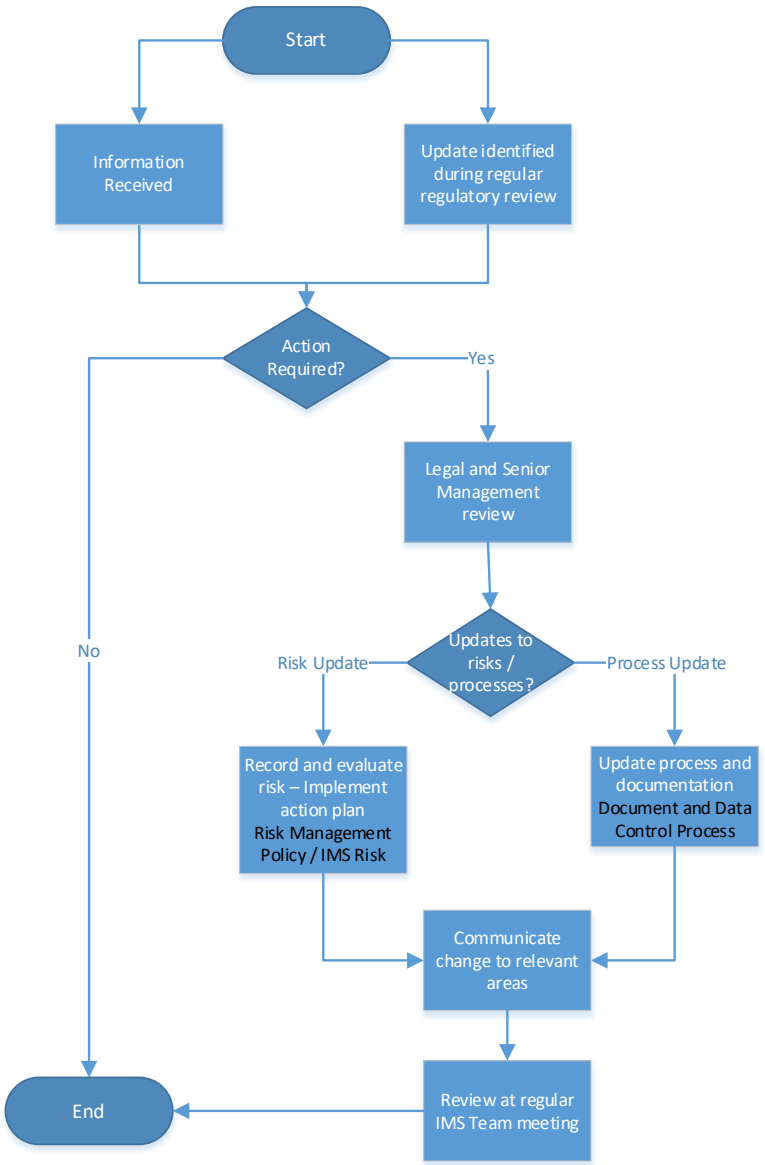
The responsibility for Regulatory compliance review and communication is shared between:

- Operations Board
- Legal Team
- Senior Management

Procedure

This procedure is to be followed by all personnel. Non-compliance to statutory requirements and regulatory requirements could lead to fines, penalties or custodial sentences depending on severity

Legal and Regulatory Compliance Process



3.12 Management Review Process

Scope

The scope of this process covers all management and relates to the review of the effectiveness of the Integrated Management System.

Purpose

The purpose of this process is to describe how the management review the effectiveness of the Integrated Management System against a pre-determined agenda conforming to the Standard.

At this review, Targets and Objectives for the coming year are set as well as ensuring a continuing improvement ethos.

Responsibility

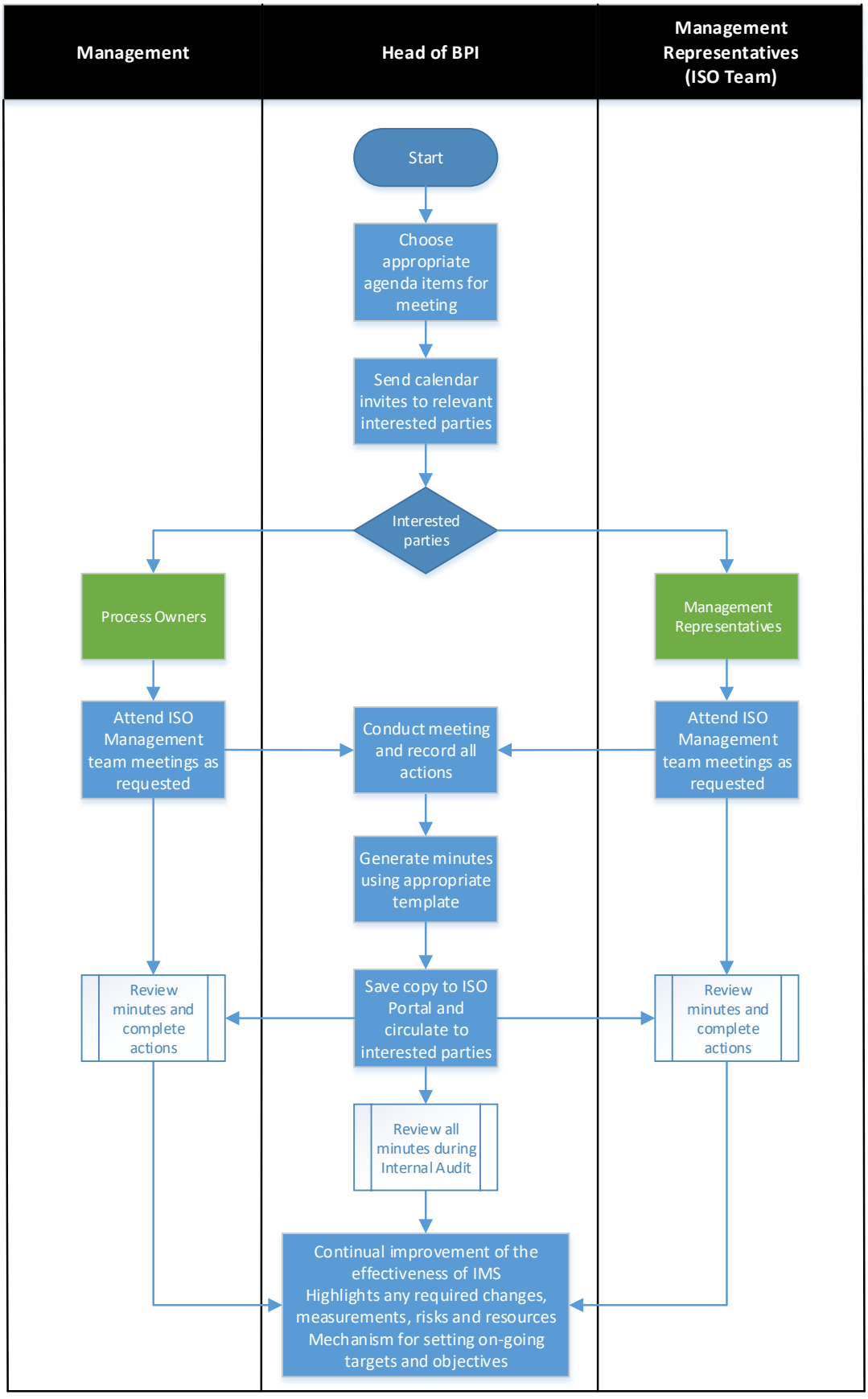
- The Governance Team Leader is responsible for ensuring that an annual review, as a minimum, of the Integrated Management System takes place.
- The Governance Team Leader is responsible for documenting the Management Review Minutes using the appropriate document template and ensuring they are filed within the IMS Portal.
- All staff should be made aware of the results of the Management Review
- Management is responsible for reviewing the requisite inputs and outputs defined as part of the Management Review Process.
- Representatives from the following areas can contribute to the Management Review:
    - Board Representative/s
    - Information Systems
    - Legal
    - Human Resources
    - Product Management
    - Supplier Management
    - Operations
    - Business Continuity
    - Sales

Detail

All items required by the standard must be discussed on a regular basis. The table below details the Inputs and Outputs required by the standards:

Process	Inputs	Outputs
Context	Scope and Boundaries Legal and Regulatory Compliance Policy Statements	Legal Register Policy Statement reviews Scope of operations review
Leadership	Objectives Changes Previous Reviews Any Other Business	Objectives and responsibilities Change reviews
Planning	Risk Assessment Business Continuity	Risk Assessment Level of Risk Business Continuity provision
Support	Resource Levels Participation and Consultation	Resource review and responsibility Participation review
Operations	Process Audit Results on Processes Policies	Update necessary processes Confirm further audits and plans Policy reviews and updates
Performance	Audits Customer Feedback Suppliers	Confirm further audits and plans Customer feedback review and actions Supplier evaluation review
Improvement	Audit Analysis Other Analysis	Review of prior audit results and root causes Data analysis and actions to be taken as per objectives

Maintel use an Integrated Management System (IMS) and all standards are treated as one entity. The requisite inputs and outputs listed in the Table above are identified by the relevant Annex SL process and not standard specific, unless otherwise stated within comments of the meeting record.



3.13 Operational Control Process

The purpose of this process is to detail, at high level, how services and equipment solutions are implemented, tested, maintained, and invoiced.

This document covers sales of equipment and services for all Maintel offerings and identifies the areas of activity to fulfil the customer order and considers Security, Quality, Personal Data and Privacy risks.

Responsibility

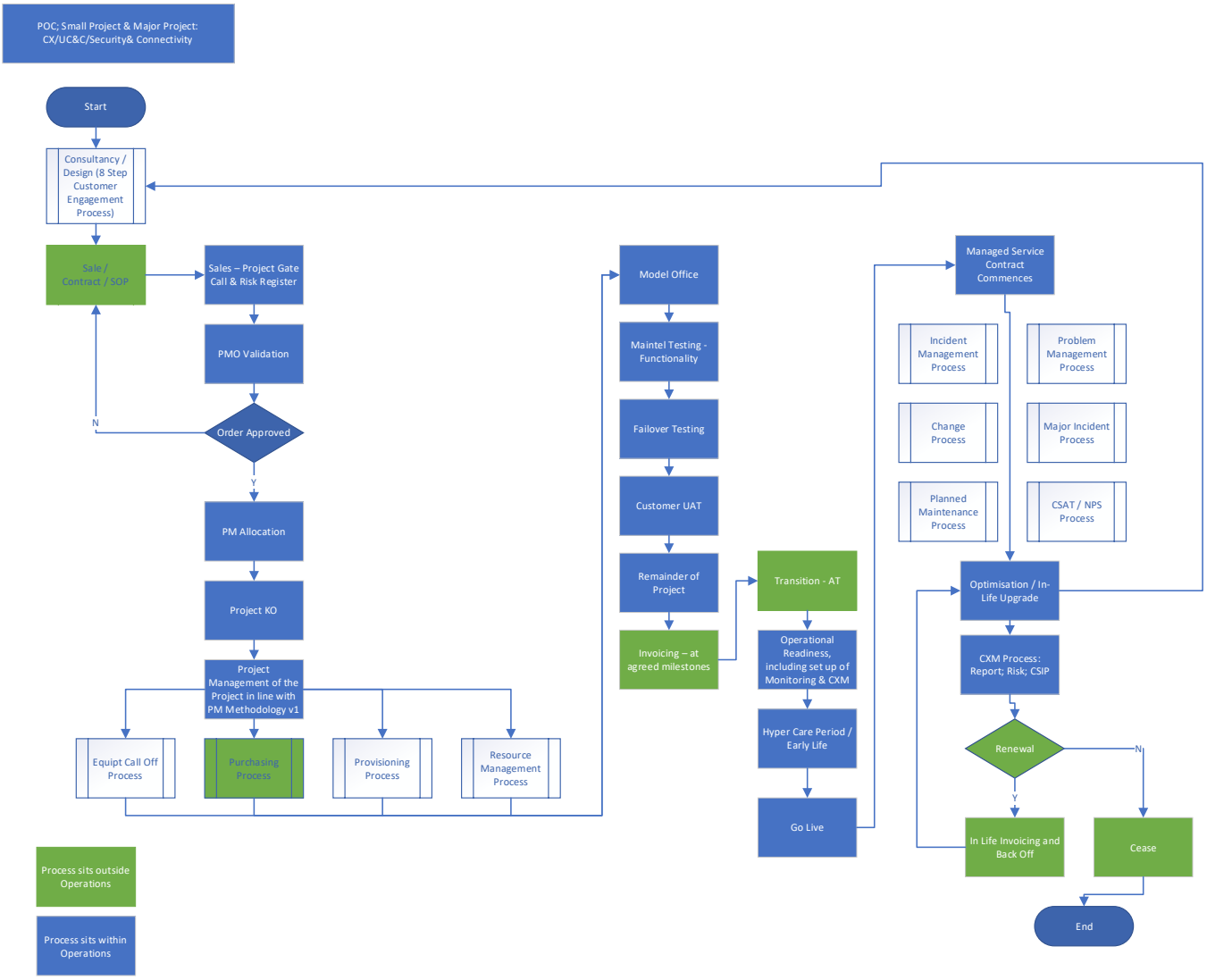
Across all pillars responsibility is shared between the following departments:

Responsibility	Growth	Operations	Finance	Legal
Sale	Yes			
Contract	Yes			Yes
Solution Design		Yes		
Project Management		Yes		
Project Delivery		Yes		
Test		Yes		
Invoice		Yes	Yes	
Transition / Cease	Yes	Yes		
Optimisation		Yes		
In Life Management	Yes	Yes		
Renewal	Yes	Yes	Yes	Yes

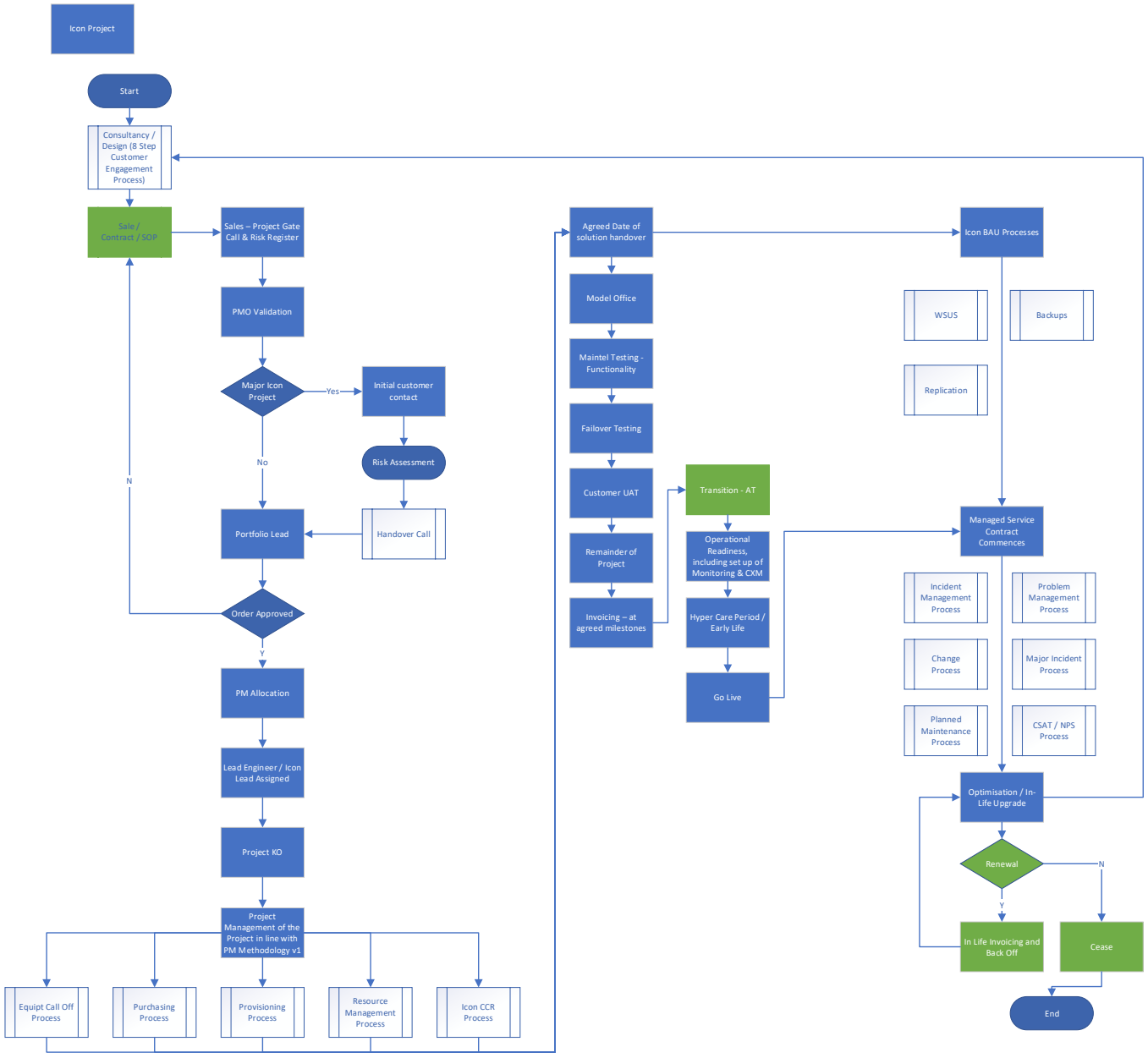
Processes

Across the three technology pillars

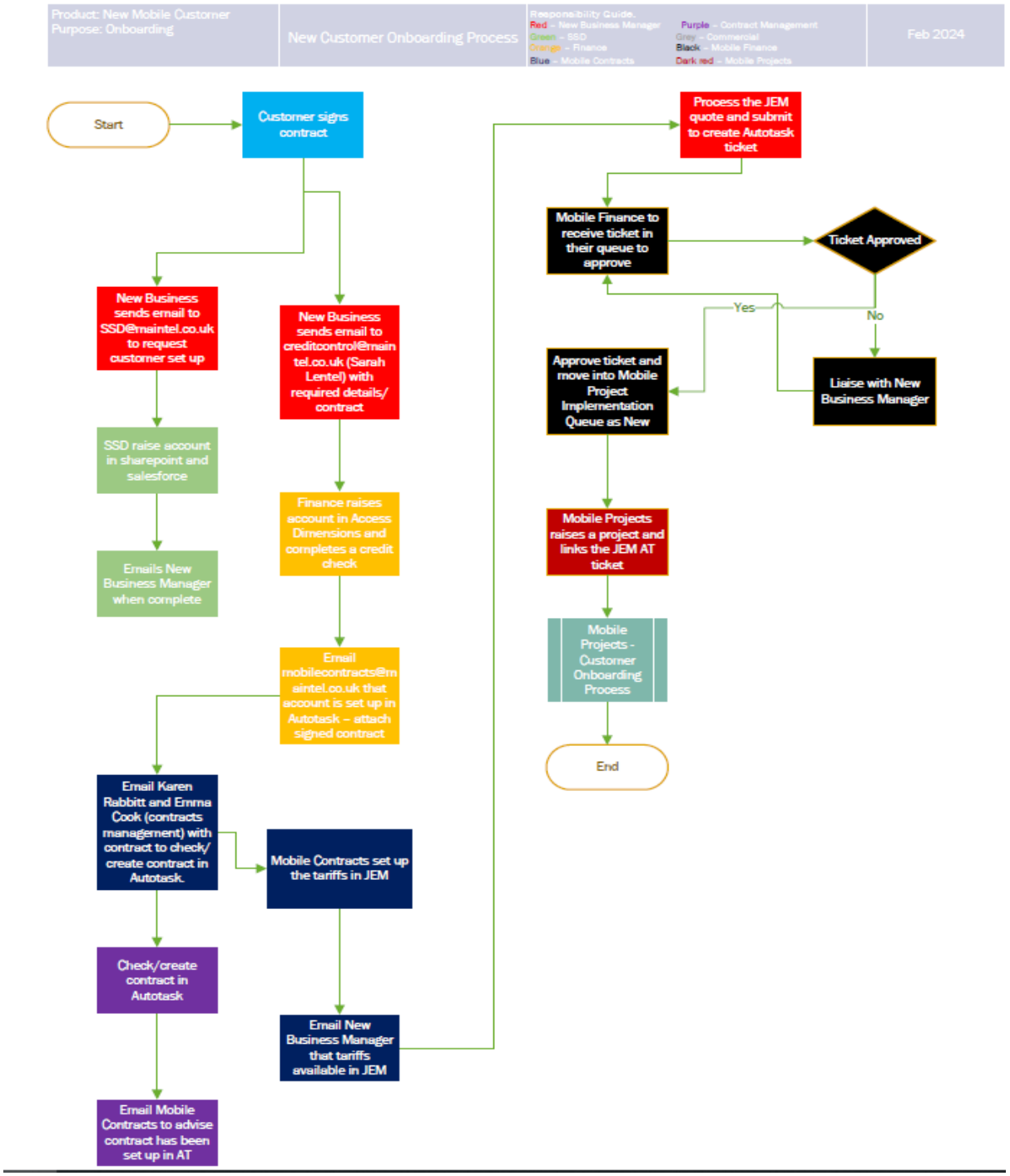
- UC & Collaboration
- Customer Experience
- Security & Connectivity



Maintel Infrastructure Process



Mobile



3.14 Privacy Policy - External

Maintel consider privacy as a top priority for customer confidence, legal, regulatory, and contractual compliance, and the protection of the Maintel brand.

We understand that your privacy is important to you and that you care about how your personal data is used and shared. Maintel respect and value the privacy of everyone and where required in its ordinary course of business, Maintel must often control and process information about data subjects, for example Prospects, Customers, Suppliers and Employees.

When handling information, Maintel or any party that controls or processes personal data on Mantel's behalf, must comply with current Data Protection regulations and relevant contractual obligations.

This policy should be read in conjunction with Maintel Cookie Policy which can be found in the Policies section of our website.

Maintel take compliance with this policy very seriously. The importance of this policy means that internal failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

Company Contact details

Maintel Europe Ltd is incorporated in England and Wales with registered number 02665837 with registered office at 69 Leadenhall Street, London, EC3A 2BG, England. You may contact us:

- By post using the registered office address above
- By telephone at: 0344 871 1122
- By email at: info@maintel.co.uk for general enquiries

Data Protection Officer

- Name: Joanne Ballard
- Job Title: Data Protection and Compliance Officer
- Email: gdpr@maintel.co.uk
- Telephone: 0344 871 1122
  Address: 69 Leadenhall Street, London, EC3A 2BG, England

The personal data we collect

Maintel may collect some or all the following personal data and non-personal data, please also see the Cookie Policy on Maintel website.

- Name
- Business/Company Name
- Job Title
- Business Contact Information such as email addresses and telephone numbers
- Main location, site/installation, and billing Address(es) and Postcode(s)
- IP Address
- Call Records
- Employee Number / Identification Number

How and why, we collect personal information

Maintel collect personal data from the point you enter communications about our products and services, implement a contract, elect to attend an event, request marketing communications or through our website.

Our use of your personal data will always have a lawful basis as defined within current data protection regulations. Maintel may use your data for the following purposes:

- Providing and managing your Account.
- Supplying products and/or services to you
- Entering a contract with you
- Personalising and tailoring Maintel products and services for you and your business
- Replying to emails from you.
- Supplying you with Marketing emails that you have opted into
- As stated in the Cookie Policy where you have used our website.

How and where we store your data

Data security is very important to Maintel, and to protect your data we have taken suitable measures to safeguard and secure data collected. Some or your data may be processed outside of the UK. If Maintel process data outside the UK, we take all reasonable steps to ensure that your data is treated as safely and securely as it would be within the UK and in accordance with current Data Protection regulations. Steps Maintel take to secure and protect your data include.

- Contractual agreements with Third Parties
- Technical and Organisation security measures
- ISO 27001 – Information Security
- Payment Card Industry Data Security Standard (PCI-DSS)
- Cyber Essentials certification
- Supplier Security and Privacy risk assessment and review:
    - Transfer impact assessment
    - Data Protection Impact Assessment (where required)

Sharing your data

In certain circumstances, Maintel may be legally required to share certain data held by us, which may include your personal data, for example, where Maintel are involved in legal proceedings, where we are complying with legal obligations, a court order, or a governmental authority instruction.

We may sometimes contract with third parties to supply products and services to you on our behalf.

These may include payment processing, delivery and support of goods and services, search engine facilities, advertising, and marketing. In some cases, the third parties may require access to some or all your data.

Where any of your data is required for such a purpose, we will take all reasonable steps to ensure that your data will be handled safely, securely, and in accordance with your rights, our obligations, and the obligations of the third party.

Sub processor information is provided on our website.

Retention of personal data

Maintel do not keep your personal data for any longer than is necessary considering the reason(s) for which it was first collected. Data is retained for the following periods

- Marketing contact information: Until consent is withdrawn
- In accordance with contractual obligations; normally full term of agreement plus 7 additional years
- Cardholder data is not retained for any reason

Your Rights

As a data subject, you have the following rights which this policy and Maintel use of personal data have been designed to uphold.

- The right to be informed about Maintel collection and use of personal data.
- The right of access to the personal data Maintel hold about you.
- The right to rectification if any personal data Maintel hold about you is inaccurate or incomplete
- The right to erasure / be forgotten in certain circumstances
- The right to restrict (prevent) the processing of your personal data in certain circumstances
- The right to object to Maintel processing using your personal data in certain circumstances
- The right to data portability for obtaining a copy of your personal data to re-use with another service or organisation
- Rights with respect to automated decision making and profiling.

Please note that Maintel does not ordinarily utilise automated decision making, including profiling in the normal course of its activities.

Data Protection Principles

All employees and sub-contractors of Maintel shall abide by the Data Protection Principles when carrying out any activity that contains Personal data. All personal data shall be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Retained only for as long as is necessary.
- Processed in a manner that ensures security

Regular training is provided to employees for current data protection regulations and handling of personal data.

What happens if Maintel changes hands

Maintel may, from time to time, expand or reduce the business and this may involve the sale and/or the transfer of control of all or part of our business.

Any personal data that you have provided will, where it is relevant to any part of our business that is being transferred, be transferred along with that part and the new owner or new controlling party will,

under the terms of this Privacy Policy, be permitted to use that data only for the same purposes for which it was originally collected by Maintel.

How you can control your data

We aim to give you strong controls on our use of your data for direct marketing purposes (including the ability to opt-out of receiving emails from us which you may do by unsubscribing using the links provided in emails and at the point of providing your details).

You may also wish to sign up to one or more of the preference services operating in the UK: The Telephone Preference Service ("the TPS"), the Corporate Telephone Preference Service ("the CTPS"), and the Mailing Preference Service ("the MPS"). These may help to prevent you receiving unsolicited marketing. These services will not prevent you from receiving marketing communications that you have consented to receiving.

How you can access your data

You have the right to ask for a copy of any of your personal data held by Maintel.

A fee is not charged for reasonable requests, and we will provide information in response to your request within timescales stated within the current data protection regulations.

Please contact Maintel using the contact details in this policy.

Complaints

If you have any cause for complaint or would like to talk to us about Maintel use of your personal data, please contact us using the details provided.

You have the right to lodge a complaint with the UK's supervisory authority, the Information Commissioner's Office.

For further information about your rights, please contact the Information Commissioner's Office or your local Citizens Advice Bureau.

ICO Contact details:

- Address: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
- Helpline: 0303 123 1113
- Website: www.ico.org.uk

Reporting data breaches

All actual or potential personal data breaches shall be reported as soon as they become known using Maintel Information Security Incident process.

Breaches shall be reported to the Supervisory Authority within 72 hours and to the Data Subject/s as soon as possible.

Changes to policy

We regularly review our policies and may change them from time to time, for example, if the law changes.

Any changes will be immediately posted on our website.

We recommend that you check regularly to keep up to date.

3.15 Privacy Policy - Internal

Maintel understands that your privacy is important to you and that you care about how your personal data is used and shared. Maintel respect and value the privacy of everyone and where required in its ordinary course of business, Maintel must often necessarily control and process information about data subjects, for example Prospects, Customers, Suppliers and Employees.

When handling such information, Maintel or any party that controls or processes personal data on Mantel's behalf, must comply with current Data Protection regulations and relevant contractual obligations. Please read this policy carefully and ensure that you understand it. If you have any questions or concerns, do not hesitate to contact your line manager, the People Team, or our Data Protection and Compliance Officer.

Scope and Compliance with our policy

This policy applies to all Maintel employees and contractors.

Maintel take compliance with this policy very seriously. This means that internal failure to comply with any requirements may lead to disciplinary action. Unauthorised disclosure of personal data is considered a disciplinary matter and may, in some cases be considered gross misconduct.

Please read this Policy carefully and ensure that you understand it. If you have any questions or concerns, do not hesitate to contact your line manager, the People Team or our Data Protection Officer.

Data Protection Officer (DPO)

Maintel is not required to nominate a Data Protection Officer but has chosen to do so

- Name: Joanne Ballard
- Job Title: Data Protection and Compliance Officer
- Email: gdpr@maintel.co.uk
- Telephone: 0344 871 1122
- Address: 160 Blackfriars Road, Southwark, London, SE1 8EZ

The DPO is available to all employees and works to:

- Inform and advise on Data protection matters
- Monitor compliance to Data Protection Regulations, identify and mitigate risks
- Provide advice about data protection impact assessments
- Cooperate with and be the main liaison point for the supervisory authority

The DPO is assisted by Head of IT, Legal Counsel, Head of Marketing, Head of People Team, Head of Product Management

Employee Responsibilities

Adhering to Data Protection Principles

All employees and sub-contractors of Maintel shall abide by the Data Protection Principles when carrying out any activity that contains Personal data. All personal data shall be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Retained only for as long as is necessary.
- Processed in a manner that ensures security.

Maintenance of Information provided to Maintel

All employees shall:

- Ensure that all personal data which they have provided to Maintel in connection with their employment is accurate and up to date.
- Inform Maintel, using the appropriate systems, i.e. MyMaintel, of any changes to information.
- Review the information which Maintel hold, in written or automated form, and inform Maintel of any errors or, where appropriate, follow procedures for up-dating entries.
- Maintel shall not be held responsible for errors of which it has not been informed.

Maintel may have a requirement to collect employee health data which falls within a special category of data for the purpose of protecting your vital interest, i.e., details of allergies, medication information or medical condition such as asthma or diabetes.

Maintel will only use such information to protect the health and safety of the individual, for example, in the event of a medical emergency and appropriate consent will be sought prior to the collection of special category data.

Processing Information

All employees shall ensure that:

- All personal data is kept securely in accordance with instructions and processes.
- All personal data is only used for the specific purposes it was provided for.
- The retention period for personal data is adhered to.
- No Card holder data shall be recorded or stored
- Personal data is not disclosed either orally or in writing, to any unauthorised employee or third party
- Identity checks are completed where disclosure of personal information is approved.

Using information controlled by Maintel

Customer Information - Employees shall ensure that:

- They are aware that they are the designated controller when working on customer platforms
- unless expressly given permission to, through consent or contract, they will not attempt to process customer personal data or information
- Whilst working on customer platforms, the system is always as protected and secured as possible
- No card holder data is recorded, retained, or stored

Employee Information – Employees shall ensure that:

- Where their role provides access to employee information, this is managed and used in accordance with the Information Security Policy, regulations, and local processes
- Employee information is not to be shared, other than between authorised personnel and, in any case, minimised or redacted as far as possible to remove personal identifiable information.

Reporting Data Breaches

All employees shall report actual or potential personal data breaches using IT Help desk Portal, this enables us to:

- Investigate the potential or actual failure and take remedial steps
- Maintain a register of compliance failures
- Notify the Supervisory Authority and Data Subjects of any personal data breaches

> It is a requirement of current regulations that ALL relevant data breaches, are proactively reported to the Supervisory Authority within 72 hours and the Data Subject/s as soon as possible. For Maintel to comply with this requirement you must report all suspected or actual data breaches immediately.

The Information Security Incident Policy details how security incidents, including data breaches are categorised, the reporting mechanisms and actions to be taken should an event be suspected or occur.

Training Completion

Employees

All employees receive Data Protection training during the annual refresher, at Induction and during job role changes and are responsible for completing the training provided.

Line Managers

Line Managers are responsible for ensuring information and training is provided to all members of their team as well as ensuring team members are provided time to complete the mandatory annual refresher training.

The annual refresher training is managed by the Compliance team.

Data Processing

How we collect your information

We collect data about you in a variety of ways. This will usually start when you apply for a position with us. During the recruitment process, we will collect data from you directly. This includes information you would normally include in a CV or cover letter, or notes made during a recruitment interview. Further information will be collected when you complete forms at the start of your employment, for example your bank and next-of-kin details. Other details may be collected directly from you, in the form of official documentation such as your driving licence, passport, or other evidence of your right to work in the UK.

In some cases, we will collect data about you from third parties, such as:

- · The Disclosure and Barring Service (DBS) where applicable
- · Providers of references, where required (and with your agreement)
- · Any other third parties providing us with services or acting on our behalf.

Types of data we collect and process

Maintel collect data relevant to your employment which includes some or all the following:

- your name, address and contact details, including email address and telephone number, date of birth and gender.
- the terms and conditions of your employment.
- details of your qualifications, skills, experience, and employment history, including start and end dates.
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover.
- details of your bank account and national insurance number.
- information about your marital status, next of kin, dependants, and emergency contacts.
- information about your nationality and entitlement to work in the UK.
- information about your criminal record (for specific roles).
- CVs or resumes.
- ID and entitlement documentation, i.e., Passport and Driving license copy.
- Benefits nomination.
- Correspondence relating to your employment, i.e., Forms completed, Interview notes.
- details of your schedule (days of work and working hours) and attendance at work.
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave.
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence.

- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence.
- information about medical or health conditions, including whether you have a disability for which Maintel needs to make reasonable adjustments.
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.

Legal basis for processing

All personal data is only ever processed and stored securely, for no longer than is necessary and for the purpose for which it was first collected. Maintel always comply with our obligations and safeguard your rights under Data Protection Regulations in force.

Our use of your personal data will always have a lawful basis, i.e., because it is necessary for the performance of a contract with you, because you have consented to the use of your personal data and/or because it is in our 'legitimate interests' as defined and prescribed in the current regulations.

Maintel collects and processes personal data relating to its employees to manage the employment relationship. Maintel is committed to being transparent about how it collects and uses that data and to meeting its data protection obligations.

Maintel does not utilise automated decision making, including profiling in the normal course of its activities.

Personal data means any information relating to an identified or identifiable natural person.

Most commonly we rely on the following legal bases for processing your personal data:

- To perform the employment contract that we are party to.
- To carry out legally required duties (legal obligations).
- Where the processing is necessary for the purposes of our legitimate interests or by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms.
- To protect your vital interests, such as where an emergency arises at work and medical assistance is urgently required.
- Where something is done in the public interest by way of public task.
- Where we have obtained your consent.

All processing we carry out falls into one of the lawful grounds indicated above. Generally, we will rely on the first three reasons set out above to process your data. For example, we need to collect your personal data to:

Carry out the employment contract that we have entered into with you; and

- Ensure you are paid.

We also need to collect your data to ensure we are complying with legal requirements such as:

- Ensuring tax and other legal deductions are made; and
- Ensuring that you have a lawful right to work in the UK.

We must process special categories of data in accordance with more stringent guidelines. Special category personal data includes the following:

- personal data revealing racial or ethnic origin
- personal data revealing political opinions
- personal data revealing religious or philosophical beliefs

- personal data revealing trade union membership
- genetic data
- biometric data (where used for identification purposes)
- data concerning health
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

Most commonly, we will process special categories of personal data in the following circumstances:

- You have given your explicit consent to the processing.
- For employment, social security, and social protection (if authorised by law).
- To protect your vital interests in an emergency.
- You have already made your data public.
- For legal claims.
- For reasons of substantial public interest (with a basis in law).
- For the provision of health or social care (with a basis in law).
- For reasons of public health (with a basis in law).

Further legal controls apply to data relating to criminal convictions and allegations of criminal activity. We may process such data on the same grounds as those identified for "special categories" referred to above.

We do not need your consent if we process special categories of personal data to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your decision to give or withhold consent. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withheld or withdrawn.

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out our duties in line with your contract of employment. If you do not provide us with the data needed to do this, we will be unable to perform those duties, e.g. ensuring you are paid correctly. We may also be prevented from confirming, or continuing with, your employment with us in relation to our legal obligations if you do not provide us with this information, e.g. confirming your right to work in the UK or, where appropriate, confirming your legal status for carrying out your work via a criminal records check.

How we will process your data

We will use your data for a variety of reasons during your employment with us (or for the purposes of processing your application for employment):

- Making decisions about who to offer initial employment to, and subsequent internal appointments and promotions, including collecting references, etc.
- Making decisions about salary and employee benefits.
- Providing contractual benefits to you.
- Maintaining comprehensive, up-to-date personnel records about you to ensure, among other things, that effective correspondence can be achieved and appropriate contact points in the event of an emergency are maintained.
- Effectively monitoring both your conduct and your performance and to undertake procedures regarding both, if the need arises.
- Offering a method of recourse to you against decisions made about you, via a grievance procedure.

- Assessing training needs.
- Managing statutory leave systems such as maternity leave.
- Organisational planning and restructuring exercises.
- Dealing with legal claims made against us.
- Preventing fraud.
- Ensuring our administrative and IT systems are secure and robust against unauthorised access.
- Providing employment references to prospective employers, in which case it is in the legitimate interest of the prospective employer to receive this information.

We will use your special category data for various reasons, including (but not limited to):

- For the purposes of equal opportunities monitoring.
- In our sickness absence recording and management procedures.
- Implementing an effective sickness absence management system, including monitoring the amount of leave and subsequent actions to be taken, including making reasonable accommodation for disabled individuals.
- Getting expert medical opinion when making decisions about your fitness for work.
- Determining reasonable accommodation in the case of disability.

Change of purpose

We will only process your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another related reason; and that reason is compatible with the original purpose. If we need to use your data for an unrelated purpose, we will seek your consent to use it for that new purpose. Please note that we may process your data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

How and where we store your Data

Data security is very important to Maintel, and to protect your data we have taken suitable measures to safeguard and secure data collected. Some or your data may be stored outside of the UK. If Maintel do store data outside the UK, we take all reasonable steps to ensure that your data is treated as safely and securely as it would be within the UK and under the current Data Protection regulations

Steps Maintel take to secure and protect your data include:

- Contractual agreements with Third Parties
- Technical and Organisation security measures provided within.
    - ISO 27001 – Information Security
    - Payment Card Industry Data Security Standard (PCI-DSS)
    - Cyber Essentials certification
- Supplier Security and Privacy risk assessment and review
    - Transfer impact assessment
    - Data Protection Impact Assessment (where required)

No data shall be transferred outside of the UK without approval **from the DPO following completion of the appropriate data protection impact assessments**

Sharing Data

In certain circumstances, Maintel may be legally required to share certain data held by us, which may include your personal data, for example, where Maintel are involved in legal proceedings, where we are complying with legal obligations, a court order, or a governmental authority request.

We may sometimes contract with third parties to supply products and services to you on our behalf, i.e., Happy People benefits selection. In some cases, the third parties may require access to some or all your data.

Where any of your data is required for such a purpose, we will take all reasonable steps to ensure that your data will be handled safely, securely, and in accordance with your rights, our obligations, and the obligations of the third party under the law.

Your Rights

As a data subject, you have some, or all the following rights which this policy and Maintel use of personal data have been designed to uphold:

- The right to be informed about Maintel collection and use of personal data.
- The right of access to the personal data Maintel hold about you.
- The right to rectification if any personal data Maintel hold about you is inaccurate or incomplete
- The right to erasure / be forgotten in certain circumstances
- The right to restrict (prevent) the processing of your personal data in certain circumstances
- The right to object to Maintel processing using your personal data in certain circumstances
- The right to data portability for obtaining a copy of your personal data to re-use with another service or organisation
- Rights with respect to automated decision making and profiling.

Please note that Maintel does not ordinarily utilise automated decision making, including profiling in the normal course of its activities.

Complaints

If you have any cause for complaint or would like to talk about Maintel use of your personal data, please contact gdpr@maintel.co.uk or raise an HR ticket on IT, Facilities & HR portal

You also have the right to lodge a complaint with the UK's supervisory authority, the Information Commissioner's Office.

For further information about your rights, please contact the Information Commissioner's Office or your local Citizens Advice Bureau.

ICO Contact details:

- Address: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
- Helpline: 0303 123 1113
- Website: www.ico.org.uk

What happens if Maintel changes hands?

Maintel may, from time to time, expand or reduce the business and this may involve the sale and/or the transfer of control of all or part of our business. Any personal data that you have provided will, where it is relevant to any part of our business that is being transferred, be transferred along with that part and the new owner or newly controlling party will, under the terms of this Policy, be permitted to use that data only for the same purposes for which it was originally collected by Maintel.

Subject Access Requests

Maintel aims to comply with all reasonable and compliant requests for access to personal data as quickly as possible and provide information within one calendar month of the receipt of a request.

Where necessary, considering the complexity, number of and duplication of requests, Maintel may extend this period by two further months. Any extension will be notified to the data subject within one month of receipt of the request and include the reasons for the delay.

The Subject Access Request Process within the IMS Portal details how to initiate a Subject Access Request.

Maintel do not normally charge for provision of information related to a Subject Access Request unless the requests from a data subject are manifestly unfounded or excessive, due to their repetitive nature. Where it is necessary to charge, a reasonable fee to consider administrative costs will be raised.

The right to obtain a copy of information shall not adversely affect the rights and freedoms of others.

Retention of Data

Maintel keep different types of data and limit the data storage amount and retention time to that which is required for legal, regulatory and/or business requirements. The Data Retention policy and associated schedule contains the details.

- Personal data is not stored for longer than is necessary.
- Card holder data is not retained for any reason.
- Data is deleted when no longer required based on the retention period.

Cookies

Please see the separate Cookie Policy within the IMS Portal for information relating to Cookies when using the Maintel website.

3.16 Retention, Destruction and Disposal Policy

The purpose of this policy is to detail the procedures for the retention, disposal, and destruction of information to ensure that necessary records and documents are adequately protected and maintained and that records and documents that are no longer needed or are of no value are kept to a minimum and discarded at the proper time. This Policy is also for the purpose of aiding employees in understanding their obligations in retaining electronic documents - including e-mail, Web files, text files, PDF documents, and all Microsoft Office or other formatted files in accordance with current requirements, including but not limited to:

- Data Protection Regulations
- WEEE Waste Regulations and IEEE Standards
- Companies Act 2006
- Health and Safety at work etc. Act 1974

Unless otherwise specified this policy refers to equipment containing information and both hard and soft copy records and documents.

Our Policy

It is Maintel policy to efficiently manage records for the effective delivery of our services, to document our activities and to maintain corporate memory while complying to the law and regulations in all our business activities, including applicable Data Protection laws. We are committed to using all appropriate technical and organisational measures to ensure the protection of both customer and employee personal data. The benefits of records management are:

- protecting our business-critical records and improving business resilience
- ensuring our information can be found and retrieved quickly and efficiently,
- complying with legal, regulatory and certification requirements
- reducing risk
- minimising storage requirements and reducing costs.

Maintel ensure, using the records retention schedule, that records, including personal data records and records within the PCI-DSS Cardholder Data Environment, are not kept any longer than is necessary for the purpose they were originally collected.

Consideration is given to:

- The categories of information
- Minimum legal retention periods for each type of record
- Document lifecycle from a business perspective
- Secure destruction once the retention period is over.

Details of the document and retention periods are shown in the Retention schedule within the IMS Portal

The retention schedule is reviewed at least annually to ensure records are not retained beyond their stated retention period.

Disposal and Destruction methods

Paper materials: On site secure recycling bins, located at each office,

- All printed copy paper is to be placed in the secure recycling bins located in all office areas,
- Regularly collected and shredded at site,
- Recycling note issued for all collections.

Electronic folders and documents: Permanently deleted,

- Rendering information non-recoverable even using forensic data recovery techniques

Electronic equipment containing information: Information removed, and equipment destroyed,

- Software wipe: secure wipe program in accordance with industry-accepted standards
- Degaussed: process of decreasing or eliminating a remnant magnetic field
- Physically destroyed: device physically crushed,
- Certificate of destruction / waste transfer note issued by licensed recycling company,
- When equipment is being donated or recycled the IS Department will wipe all data (several times) and restore to factory default.
- Hardware information is removed or marked as decommissioned within the asset register.

The following table acts as a guideline for disposal of certain devices.

Classification	Type of Security	Device	Disposal Method
Restricted High Value Strict Legal Requirements High Sensitivity High Criticality to Maintel	Encrypted	Focal Point Server Customer environments	Software wiped Degaussed Physically destroyed
Restricted	Role based permissions	Data Server	Software wiped Degaussed Physically destroyed
Confidential	Role based permissions	PC's Laptops Data Servers Tablets Removable hard drives	Software wiped Degaussed Physically destroyed

Responsibilities

- **Employees:** Responsible for ensuring their documents and records are managed in compliance with this policy
- **Information Systems:** Responsible for monitoring the identification and destruction of equipment, records, and documents in accordance with this policy.

Non-compliance to this policy will be managed through Maintel Disciplinary procedures.

Good management tips for records and documents

- Store documents in a company shared location, not on your laptop or desktop,
  - Access restrictions can be set up depending upon the classification of the document,
  - Teams and SharePoint are the preferred storage areas.
- Use Email tools to:
  - Remove duplicates – Clean up folder,
  - Permanently delete files – Empty Folder
- Share links to centrally held documents to avoid creating duplicates when attaching to email,
- Include version control within your document or through system allocation, i.e., SharePoint,
- Managing Teams in line with Project/Requirement completion: Delete when complete.

3.17 Risk Management Policy

Risk Management

Risk management is a process which aims to help businesses understand, evaluate and act on all their risks with a view to increasing the probability of achieving objectives and reducing the likelihood of failure. Risk management gives comfort to stakeholders that the business is being effectively managed and helps the business confirm its compliance with corporate governance requirements.

This Policy sets out our approach to risk management and Maintel appetite for taking risk. The implementation of this Policy is the process by which we:

- identify risks in relation to:
    - the achievement of our objectives
    - specific categories of activity/asset
    - emerging threats and vulnerabilities
- assess their relative likelihood and impact,
- respond to the risks identified, considering our assessment and risk appetite,
- review and report on risks to ensure that Maintel risk profile is up to date, to provide assurance that responses are effective, and identify when further action is necessary.

By successfully implementing our Risk Management Policy we expect to:

- successfully achieve our objectives and minimise the risk of failure,
- take a proactive approach, anticipating and influencing events before they occur,
- facilitate better informed decision making,
- improve our contingency planning.

The Risk Management Policy will be reviewed annually as part of our compliance routine and scrutinised by the Board bi-annually. In addition, an immediate review is completed following major changes policy.

Risk Appetite

Defined as the amount of risk that an organisation is willing to seek or accept in the pursuit of long-term objectives. Maintel appetite for risk is set out below.

Maintel approach is to minimise its exposure to reputational risks, financial risks, regulatory and compliance risks, and risks relating to the security of systems and data, whilst being more open to risks relating to the pursuit of innovating our services, building our customer base, and increasing our competitive strength in the market.

Risk Registers

- **Corporate Risk Register**: Owned by the Board with input from agreed meetings and IMS Risk register.

- **IMS Risk**: Compiled of the Information Security, Health and Safety, Environmental and Business Continuity risk registers and owned by the Governance team to manage operational risk with input from across the business. Risks identified as High or Very High within IMS risk are escalated to the corporate risk register.

Accountability and Responsibility

Roles and Responsibilities

Body	Roles and Responsibilities include:
Board	• Set the tone for risk management including risk appetite and has overall responsibility for the risk management arrangements and the effectiveness of the arrangements. • Periodic review the corporate risk register, • Receive reporting of any new major risks and significant breaches of risk appetite • Horizon scanning and consideration of emerging risks
Audit and Risk Committee	• Responsible to the Board for oversight of the risk management activities • Ensure the approach to risk management is sound and operating as intended, • Challenge the Corporate risk register, the scoring, and the risks on the register, • Monitor actions and processes to ensure compliance and assess the level of assurance on the controls in place, • Horizon scanning and consideration of emerging risks
Chief Executive Officer	• Accountable for the effectiveness of Maintel risk management and ensuring the approach to risk management is sound and operating as intended. • The CEO is supported by the Operating Board and Governance Team Leader.
Operating Board	• Periodically review, update, and amend the entire corporate risk register, • Challenge the risks, scores, and mitigations of other risk owners, • Recommend where further mitigating actions may be required
Data Protection and Compliance Officer	• Act as an advocate for risk management across all levels of the business • Responsible for development of the business's risk management procedures subject to approval by the Board • Drafting the Risk Management Policy for Board approval, presenting it for periodic review and approval and monitoring the application of the policy • Co-ordinate risk management activities of the management and compliance teams and escalating new risks to the appropriate risk register, • Compile risk information and reports for the Operating Board and Board

Body	Roles and Responsibilities include:
Compliance Team	• Responsible for the Operational Risk Assessment “IMS Risk” which includes Security, Health and Safety, Business Continuity and Environmental aspects, • Identify specific categories of activity/asset and the threats that can impact them, • Set “rules of engagement” for the use of the asset or whilst conducting the activity, • Record the appropriate legislation, location, and owner for each risk, • Identify precautions and recommend actions to be taken to protect activity/asset
Risk Owners	• Embed the risk management culture within the business, • Identify and score risks at gross and net levels, • Monitor the operation of controls to ensure that they are operating with enough effectiveness to justify the residual/net risk score, • Identify and report changes in the external or internal environment that can influence the risk profile
First Aiders	• Responsible for regularly reviewing Health and Safety risk and acting as a confidential conduit (where required) for staff raising Health and Safety risks in conjunction with ISO45001and providing risk update regarding Health and Safety.
All Staff	• Responsibility for risk management and internal control in their own areas of operation; Understand, accept, and implement risk management process, • Be alert to risks associated with the activities that they perform, • Report to Risk Owners inefficient, unnecessary, or unworkable controls • Report to Risk Owners losses and near misses • Some employees may be a nominated risk owner responsible for ensuring the mitigating actions are in place.

Risk Management Procedures

Risk Identification

Maintel risk registers are populated by individual risks being identified from 4 main sources:

Source	Detail
New risks identified from business planning processes	Risk Owners are required to assess the risks that threaten the achievement of their objectives and identify specific exposures whilst planning for appropriate mitigation, e.g., management controls and actions to reduce probability and/or impact of the risk exposure. This must include both risks

Source	Detail
	that could prevent objectives being achieved and additional exposures that arise because of pursuing these objectives. Identifying risks from the business planning process should include a review of the key performance issues experienced over the last financial year and include all material environmental trends that potentially impact upon Maintel and its main objectives.
Risks identified from new project appraisal	New project appraisal is an on-going activity where business proposals are formulated. Project specific risks are identified during this process.
Risks identified from existing operations	Risks relating to compliance with regulations and nominated standards and certifications that Maintel adhere to are identified, managed, and monitored as part of Maintel core operations including Assets, Activities, Services, COSHH (If required), Vulnerabilities and Interested parties.
Risks identified from the external environment.	Sector analysis and horizon scanning techniques are used to identify potential (external) risks arising from Maintel operating environment

Risk assessment

Identified risk is measured with respect to its severity (consequence) on the business and the probability of its likely occurrence. These scores are used to calculate the Significance value of the risk:

Value	Severity (Consequence)		Value	Probability
4	Major impact		**4**	Very likely to happen
3	Medium impact		**3**	Impact may happen
2	Minimal impact		**2**	Impact may not happen
1	Negligible impact		**1**	Unlikely to happen

Significance value = (severity * probability)

1 to 6	Low
7 to 9	Medium
10 to 12	High
13 to 16	Very High

A residual significance value based on the same formula is calculated and recorded within the risk assessment to identify the significance of the risk after mitigation/treatment has been completed.

Interpretation of risk scores

Risks with a Significance value of 10 and above are deemed to be the main exposures facing the business. These need to be managed and the aggregate impact of their potential occurrence needs to be effectively mitigated.

Where an Operational risk with IMS Risk register has a Significance value of 10 or above it is transferred to the Corporate Risk Register and reported in the monthly corporate risk report.

Significance Value	Resulting action
1 to 6 - Low	Unlikely to require specific application of additional resources. Manage through existing controls. Monitor and review.
7 to 9 - Medium	Unlikely to cause much damage and/or threaten the company. Risk controls and actions to be developed and implemented by operational managers. Monitor and review.
10 to 12 - High	Likely to cause some damage, disruption, or breach of legislation. Prompt senior management attention is required. Risk controls and actions to be developed and reported to the Board.
13 to 16 - Very High	Likely to threaten the survival or continued effective functioning of the business, financially or significantly impair its reputation. Immediate action required; Must be managed by Operating Board with an effective control and action plan reported to the Board.

Remediation

It is intended that risks are terminated, treated, or transferred within the timescales stated to bring them to a tolerable level by increasing control strengths and mitigating the identified risk:

- **Very High risks**: Within 1 month of identification
- **High**: Within 3 months of identification
- **Medium**: Within 9 months of identification

Tolerating a risk refers to when Maintel retain the enterprise risk as it is within acceptable limits when the probability and severity of the risk are low.

Critical status

Items listed within IMS Risk register are provided a gold, silver, or bronze criticality status for the purpose of prioritising return to service during a Business Continuity event.

Gold identifies the most critical systems or aspects and are managed first during a return to service followed by silver and bronze.

Vulnerability Scans

In addition to manual risk assessment, Maintel undertakes a range of Internal and External vulnerability scans as part of its compliance scheme, which is carried out, as a minimum, on a quarterly basis.

Maintel utilise the industry standard Common Vulnerability Scoring System (CVSS) to rank the severity of vulnerabilities with scores for vulnerabilities reported between 0 and 10 to provide an idea of how easy it is to exploit the vulnerability and how damaging it could be to the Maintel business.

The CVSS scores indicate a rating and Maintel have assessed the following criteria, in line with industry standard, for addition of Vulnerabilities to IMS risk if they cannot be mitigated within 4 hours of identification.

- Internal interfaces with scores of 7 and above
- External interfaces with a scores of 4 and above

CVSS Score	Rating
0	None
0.1 to 3.9	Low
4.0 to 6.9	Medium

7.0 to 8.9	High
9.0 to 10	Critical

Monitoring, Reporting and Review

The Audit and Risk Committee receive an update on the corporate Risk Register at each meeting, including details of any changes in risk scores and any new risks. The Audit and Risk Committee will make recommendations to the Board twice a year and will be responsible for the approval of the risks and risk scores included in the Risk Register.

All items within the risk assessments are reviewed, as a minimum, on an annual basis unless an event has occurred which requires the items risk level to be adjusted.

Where the control and mechanisms implemented to mitigate a risk have been determined to be ineffective a full review of the items will be conducted, and a treatment plan initiated in order to control and manage the risk.

All employees are provided the facility to report changes or new risks for the risk assessments by emailing; riskmanagement@maintel.co.uk

Escalation Mechanism

Should there be a significant change to the business risk profile, or should a very high net risk be identified, this will be escalated to the Board for discussion at the next Board meeting.

Resources and training

The Compliance Team will act as the coordinator of the risk management framework and will assess, from time to time, whether specific training is required for staff to ensure they understand and adhere to Maintel risk management framework requirements.

3.18 Staff Vetting and Exit Policy

This policy sets out the criteria and actions to be taken for effective vetting of new staff and the exit actions to be taken at the end of employment.

Vetting and Probationary Period

All new members of staff receive induction training and are placed on at least, a 3-month probationary period when they commence employment with Maintel. The following initial information is given/received:

- C.V.
- New Starter Forms
- Passport or form of identification
- Right to work in the UK confirmation
- Reference and qualification checks
- Health and Safety briefing.
- Information Security and Data Protection Briefing
- Issued a fob key for access (if required).
- Username and password for the network and the company client database (if applicable).
- Access given for resources to carry out their duties, relevant to the level of access required.
- Allocated any necessary equipment, which is registered in the Asset register.
- They will be given Staff Awareness training to inform them of the IMS system operating within Maintel.
- Engineers to undergo DBS check where appropriate to job role
- Copy of driving licence - everyone who has a car, car hire, driving for the company

Contractors / Sub-contractors can be subject to the same confirmation and security checks as employees. All contractors / sub-contractors are also required to sign a Non-disclosure Agreement prior to engagement.

Right to work in the UK

It is vital that checks are completed to ensure any person being recruited is legally eligible to work within the UK.

All offers of employment are therefore conditional on eligibility to work in the UK being satisfied.

Maintel abides by all relevant regulations including The Immigration, Asylum and Nationality Act 2006 this includes:

- Completing checks on acceptable, original documents before a person starts working for us
- Where a time limit is imposed on the person's right to work, document checks are always completed at least every 12 months and prior to the expiry of documentation and right to work.
- Where a restriction on the type of work or hours of work is present the Maintel contract is aligned to the requirements

Where documents identify that a person is not permitted to work within the UK, then Maintel will refuse to employ that person.

Documented Control

The documents required are listed in appendix A of this policy and included in the offer of employment. These documents may change from time to time as detailed within The Immigration, Asylum and Nationality Act 2006. Maintel confirm eligibility of persons and compliance to Sections 15 to 25 of The Immigration, Asylum and Nationality Act 2006 by

- checking any photographs are consistent with the appearance of the person; and
- checking any dates of birth listed are consistent across documents and that we are satisfied that these match up with the appearance of the person; and
- checking that the expiry dates of any limited leave to enter or remain in the UK have not passed; and
- checking any UK government endorsements (Biometric Residence Permits, stamps, stickers, visas) to see if the person can do, or can continue to do, the type of work you are offering; and
- satisfying ourselves that the documents are genuine, have not been tampered with and belong to the holder; and
- asking for a further document in explanation if we are given two documents which have different names. The further document could, for example, be a marriage certificate or a divorce decree absolute, a deed poll or statutory declaration.

Copies of the relevant pages of documentation are kept and stored with the date of collection identified. Documents are retained for the duration of the persons employment and for a period not less than 2 years following termination of employment contract.

Exit - Personnel without System Administrator access

On termination of employment an Exit Interview is completed. This is carried out by the Departmental Manager of the person who is leaving the company, unless the situation is of a severe nature then a member of the People Team will carry out the interview.

- Complete exit interview form on My Maintel
- Complete leaver form on My Maintel which automatically informs the IT department who will:
    - Turn on Out of Office.
    - Give time limited email access to the Departmental Manager.
    - General tidy up of email account.
    - Removal from Maintel email distribution lists.
    - Removal of office PC for reformatting if not a shared PC.
    - Determine period when user can be deleted from the system, which includes emails.
- Designated leaving day recorded which flags the last working day to retrieve all remaining equipment

All equipment held by the employee will be returned to the IS Department and registered on the Asset register as having been returned. This will include their security key fob. If the employee has been authorised to access the building outside of normal office hours, they must, where applicable, also return both external & internal keys, while IT Department will remove remote access.

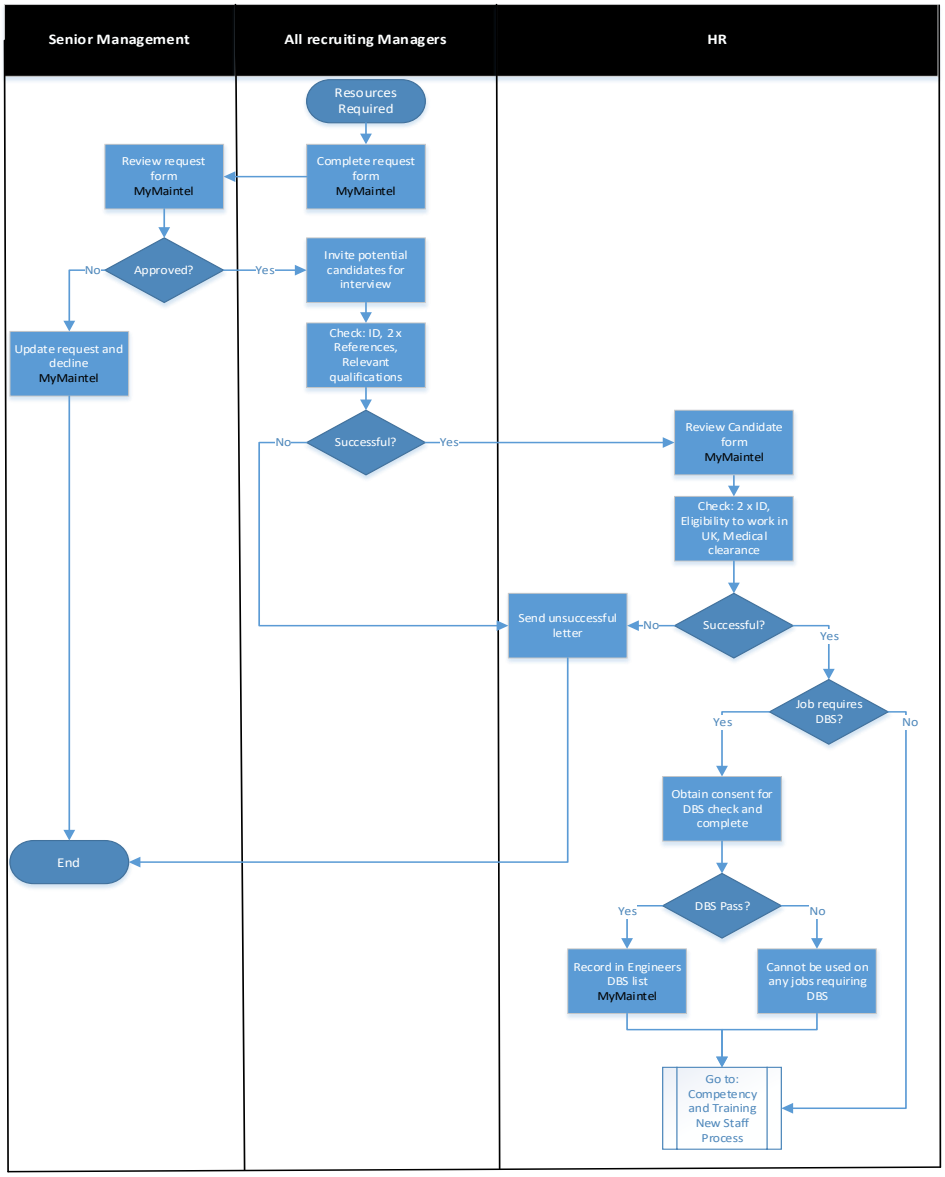
Exit - Personnel with System Administrator access

On termination of employment, the normal exit procedures will be adhered to, however as personnel within the IS Department have access to the System Administration accounts special processes must be used to mitigate any risk this may cause.

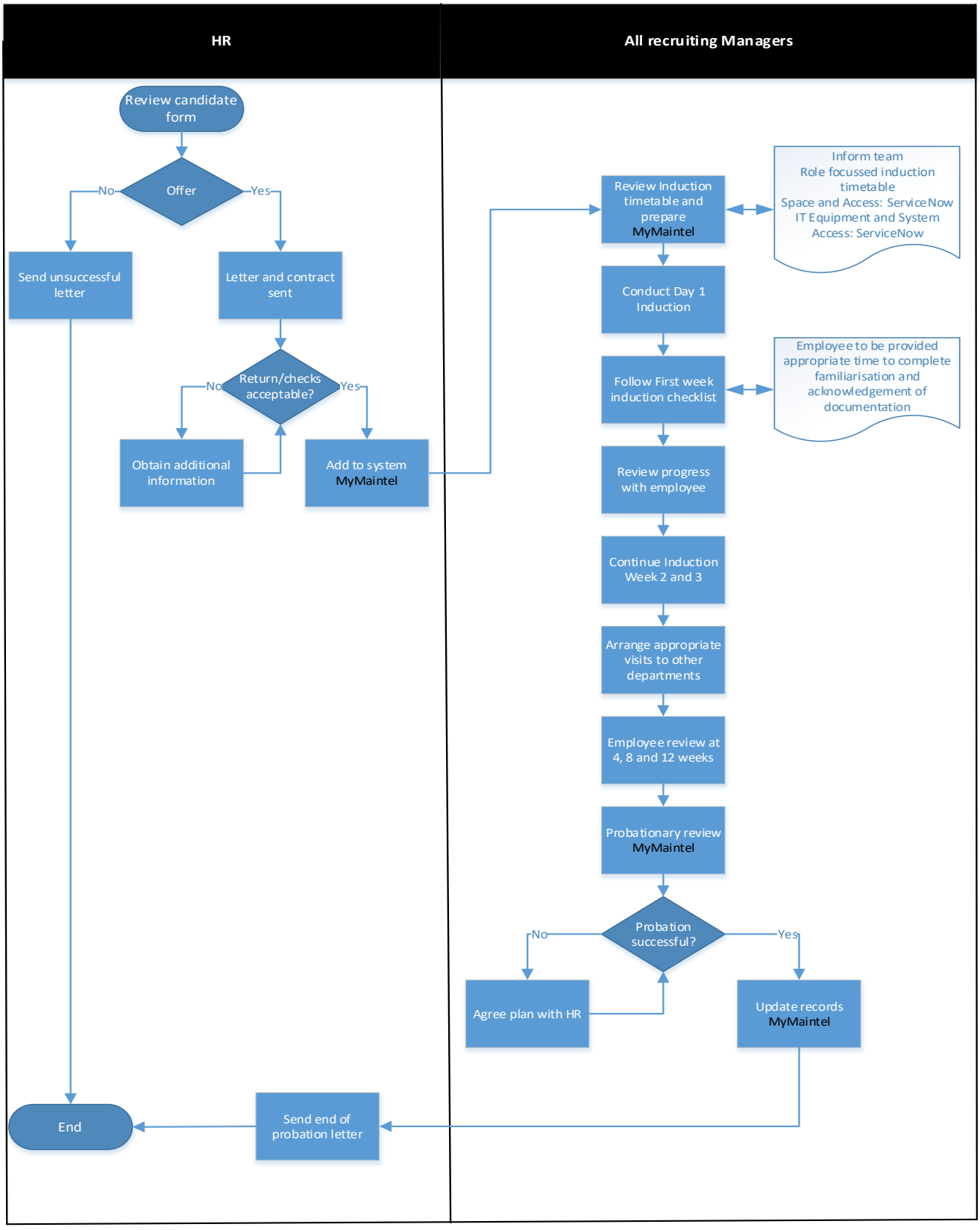
- Check the interaction of systems documentation, which details the connections between systems that use the administrator access for connectivity in the background.
- The super-user (administrator) password for critical applications shall be reset as soon as possible (maximum of 2 weeks) after the member of staff leaves the organisation.
- All systems will be checked for continued functionality.
- All default passwords used will be immediately updated.

The IS Managers will assign a new member of 3rd Line support (preferably a manager or someone with the technical knowledge not to cause harm) to hold and maintain the Administrator password

Vetting Process



New Staff Process



Appendix A – Right to Work documentation

Documents that show an ongoing right to work within the UK – List A

- A passport showing that the holder, or a person named in the passport as the child of the holder, is a British citizen or a citizen of the United Kingdom and Colonies having the right of abode in the United Kingdom.
- A passport or national identity card showing that the holder, or a person named in the passport as the child of the holder, is a national of the European Economic Area or Switzerland.
- A residence permit, registration certificate or document certifying or indicating permanent residence issued by the Home Office, the Border and Immigration Agency or the UK Border Agency to a national of a European Economic Area country or Switzerland.
- A permanent residence card issued by the Home Office, the Border and Immigration Agency or the UK Border Agency to the family member of a national of a European Economic Area country or Switzerland.
- A Biometric Residence Permit issued by the UK Border Agency to the holder which indicates that the person named in it is allowed to stay indefinitely in the United Kingdom or has no time limit on their stay in the United Kingdom.
- A passport or other travel document endorsed to show that the holder is exempt from immigration control, is allowed to stay indefinitely in the United Kingdom, has the right of abode in the United Kingdom, or has no time limit on their stay in the United Kingdom.
- An Immigration Status Document issued by the Home Office, the Border and Immigration Agency or the UK Border Agency to the holder with an endorsement indicating that the person named in it is allowed to stay indefinitely in the United Kingdom or has no time limit on their stay in the United Kingdom, when produced in combination with an official document giving the person's National Insurance Number and their name issued by a Government agency or a previous employer.
- A full birth certificate issued in the United Kingdom which includes the name(s) of at least one of the holder's parents, when produced in combination with an official document giving the person's National Insurance Number and their name issued by a government agency or a previous employer.
- A full adoption certificate issued in the United Kingdom which includes the name(s) of at least one of the holder's adoptive parents when produced in combination with an official document giving the person's National Insurance Number and their name issued by a government agency or a previous employer.
- A birth certificate issued in the Channel Islands, the Isle of Man or Ireland, when produced in combination with an official document giving the person's National Insurance Number and their name issued by a government agency or a previous employer.
- An adoption certificate issued in the Channel Islands, the Isle of Man or Ireland, when produced in combination with an official document giving the person's National Insurance Number and their name issued by a government agency or a previous employer.
- A certificate of registration or naturalisation as a British citizen, when produced in combination with an official document giving the person's National Insurance Number and their name issued by a government agency or a previous employer.
- A letter issued by the Home Office, the Border and Immigration Agency or the UK Border Agency to the holder which indicates that the person named in it is allowed to stay indefinitely in the United Kingdom when produced in combination with an official document giving the person's National Insurance Number and their name issued by a government agency or a previous employer.

Documents that confirm a right to work within the UK for up to 12 months

- A passport or travel document endorsed to show that the holder is allowed to stay in the United Kingdom and is allowed to do the type of work in question if it does not require the issue of a work permit.
- A Biometric Residence Permit issued by the UK Border Agency to the holder which indicates that the person named in it can stay in the United Kingdom and is allowed to do the work in question.

- A work permit or other approval to take employment issued by the Home Office, the Border and Immigration Agency or the UK Border Agency when produced in combination with either a passport or another travel document endorsed to show the holder is allowed to stay in the United Kingdom and is allowed to do the work in question, or a letter issued by the Home Office, Border and Immigration Agency or UK Border Agency to the holder or the employer or prospective employer confirming the same.
- A Certificate of Application issued by the Home Office, the Border and Immigration Agency or the UK Border Agency to or for a family member of a national of a European Economic Area country or Switzerland stating that the holder is permitted to take employment which is less than 6 months old when produced in combination with a positive confirmation letter from our Employer Checking Service.
- A residence card or document issued by the Home Office, the Border and Immigration Agency or the UK Border Agency to a family member of a national of a European Economic Area country or Switzerland.
- An Application Registration Card issued by the Home Office, the Border and Immigration Agency or the UK Border Agency stating that the holder is permitted to take employment, when produced in combination with a positive confirmation letter from our Employer Checking Service.
- An Immigration Status Document issued by the Home Office, the Border and Immigration Agency or the UK Border Agency to the holder with an endorsement indicating that the person named in it can stay in the United Kingdom, and is allowed to do the type of work in question, when produced in combination with an official document giving the person's National Insurance Number and their name issued by a Government agency or a previous employer.
- A letter issued by the Home Office, Border and Immigration Agency or UK Border Agency to the holder or the employer or prospective employer, which indicates that the person named in it can stay in the United Kingdom and is allowed to do the work in question when produced in combination with an official document giving the person's National Insurance Number and their name issued by a Government agency or a previous employer.

Documents that are not acceptable for proving the right to work within the UK

- a Home Office Standard Acknowledgement Letter or Immigration Service Letter (IS96W) which states that an asylum seeker can work in the UK. Where we are presented with this document, we advise the applicant to call the Immigration Service on 0151 237 6375 for information about how they can apply for an Application Registration Card.
- a National Insurance number on its own in any format.
- a driving licence issued by the Driver and Vehicle Licensing Agency.
- a bill issued by a financial institution or a utility company.
- a passport describing the holder as a British Dependent Territories Citizen which states that the holder has a connection with Gibraltar.
- a short (abbreviated) birth certificate issued in the UK which does not have details of at least one of the holder's parents.
- a licence provided by the Security Industry Authority.
- a document check by the Criminal Records Bureau.
- a card or certificate issued by the Inland Revenue under the Construction Industry Scheme.

3.19 Sustainable Procurement and Supplier Management Policy

The purpose of this policy is to set out in detail the area of Supplier Control and Sustainable Procurement including:

- the control of externally provided processes, products, and services.
- integrity of suppliers Information Security, Health and Safety, Environmental and Data Protection controls.
  Maintel consideration of the impacts of procurement decisions on local communities, the environment and society as a whole

All Maintel employees shall adhere to this policy and consider sustainability as a factor in their purchasing decisions.

Applicable Legislation

Including but not limited to:

- Climate Change and Sustainable Energy Act 2006
- The Environment Act 1995
- The Environmental Protection Act 1990
- Control of Substances Hazardous to Health (COSHH) Regulations 2002

Approach

Maintel have determined and apply criteria for the evaluation, selection, monitoring of performance and re-evaluation of external providers and contractors which is based on their ability to provide products and services in accordance with requirements and the assessment and elimination of hazards to reduce risks when:

- Products and Services from external providers are intended for incorporation into Maintel's own products and Services.
- Products and Services are provided directly to customers by external providers on behalf of Maintel.
- A process or part of a process is provided by an external supplier in agreement with Maintel.

Suppliers are managed via the Product Team and Procurement Team.

Other responsibilities include Legal, Commercial, Governance, Product and Operations.

Maintel introduced additional control in the form of annual Supplier Questionnaire (from December 2021) to broaden the Environmental, Social and Governance (ESG) information collected.

All essential, business critical and new suppliers are expected to complete the survey within 90 days from date of receipt, the survey contains the following:

- Supplier Survey
- Environmental Output: Scope 1, 2 and 3 emissions
- Emissions Strategy: What the supplier is doing to reduce environmental impact, including ambition targets
- Sustainability Report

Upon receipt of the completed survey, we carry out the following:

- Update our critical supplier risk assessment based on overall response scores
- Share the results with the supplier
- Work with the supplier on any identified improvement areas
- Use environmental data in Maintel Scope 3 calculations and reporting

Following the completion of the risk assessment suppliers are monitored and surveyed on a regular basis to encourage lowering of identified risks and continual improvement:

- Red: Bi-monthly
- Amber: Quarterly
- Green: Yearly

Sustainable procurement requires the full consideration of environmental, economic, and social impacts, as well as the financial and performance implications of procurement. This means considering the impacts of procurement decisions on local communities, the environment and society.

Where Maintel deliver their services through third parties we are not directly responsible for procurement in these instances, however, we will work with our delivery partners to ensure that where possible similar standards are used in their own procurement activities by providing them with guidance on good sustainable practices.

- **Environmental** – using recycled and recyclable products, natural resource consumption, 'greener' sources of energy, energy efficiency, management of waste, and considering the impact of transportation in order to reduce our environmental impact and ecological footprint.

- **Economic** – embedding Sustainable Procurement within the Maintel procurement processes that take our environmental, economic, and social responsibilities into account when determining the specification of goods and services and procuring the most sustainable option where it can be shown to offer best value for money. Sustainability will also be embedded throughout the Maintel supply chain by identifying supplier capability and where possible encouraging suppliers to consider the impact of their products and services, and to offer more sustainable alternatives. We also recognise the benefits of having a diverse supplier base which does not unreasonably exclude small and medium enterprises, local businesses, social enterprises and the third and voluntary sectors.

- **Social** – enabling employment, training opportunities and community benefits by including, where applicable, social and community clauses within our contracts, adopting ethical sourcing practices, encouraging, and promoting good health and ensuring that suppliers and contractors do not contravene equality and diversity legislation.

Our Policy

It is our policy that:

- Supplier evaluations are based on the following criteria.

    - Availability and ability to provide products and services to Maintel requirements.
    - Where appropriate, evidence of compliance to International Standards, PCI-DSS Attestation, Certifications and Accreditations is provided and maintained throughout the contracted period.
    - Satisfactory records and actions relating to equality, environmental and Health & Safety issues.
    - Financial stability
    - Insurance arrangements
    - Business continuity capacity appropriate for the contract in place

- The internal risk scoring of the level of service provided.
- Efficiency of service
- Sustainability of provision; environmental, economic, and social responsibilities

- Suppliers identified as business critical to Maintel business, including Technology Partners, Carriers and Hosting Partners, Mobile Partners, Operational Support Partners and those Maintel have nominated to be watched are identified within IMS Risk.

- Critical services provided by third parties are identified and assessed as services or assets within IMS Risk

- All suppliers are informed of the details of and the requirement to adhere to Maintel Policies including but not limited to:

  - **Data Protection and Information Security**: Access to Maintel information and the customer data held on our servers is subject to the Data Protection Policies in place.
  - **Health and Safety**: Minimum legal and regulatory compliance with international standard achievement being preferred
  - **Environmental**: Minimum legal and regulatory compliance with international standard achievement being preferred

- The SLA's with business-critical suppliers are reviewed on an annual basis.

- Were practical an audit report will be sought for critical suppliers to the effectiveness of their standards and certifications:

  - ISO27001 Information Security Management System
  - PCI-DSS attestation
  - Cyber Essentials or Cyber Essentials Plus
  - ISO 45001 Health and Safety
  - ISO22301 Business Continuity
  - ISO14001 Environmental (or equivalent)
  - Required qualifications for individuals.

- Purchases cannot be carried out without a valid Purchase Order number being provided to the supplier through adherence to the Purchasing Control process.

- When information or data is to be transferred between Maintel and a supplier this is conducted as per the Exchange of Information Policy.

- Where possible, a written contract shall exist between all parties involved. The contract will include:

  - The scope of the services to be delivered
  - Dependencies between services, processes, and the parties
  - Requirements to be fulfilled by the supplier
  - Service targets
  - Interfaces between service management processes operated by the supplier and other parties
  - Workload characteristics
  - Exceptions
  - Authorities and responsibilities of Maintel and the supplier including adherence to Maintel Policies and Procedures
  - Reporting and communication to be provided by the supplier
  - Basis for charging
  - Activities and responsibilities for the expected or early termination of the contract and the transfer of services to a different party

- The roles of and relationships between lead and sub-contracted suppliers will be documented.
- Regular formal communication is made with suppliers on a frequency dependent upon the amount of business conducted with the supplier and the importance of the goods or services to Maintel
- Any changes to the scope or terms of existing contracts are managed and documented fully via the change management policy
- Risks and Hazards associated with the Supplier processes, products and services are identified, assessed and wherever possible eliminated prior to introduction to the supply chain.
- The performance of critical suppliers will be monitored on a regular basis through regular meetings and a combination of supplier-provided reports verified against the contract requirements, internally produced reports from the Maintel Operational areas and Customer feedback.
- Where Maintel are not directly responsible for procurement in the supply chain we will work with our delivery partners to ensure that where possible similar standards to this policy are used in their own procurement activities by providing them with guidance on good sustainable practices.
- We will seek to achieve best value for money in all our procurement activity.
    - This means considering both the price and quality in procurement decisions and recognising that the cheapest price does not always represent best value.
    - Consideration will be given where possible to environmental criteria by reviewing the whole life cost or whole life value of the purchase (including any decommissioning and/or disposal costs where appropriate) and the level of after sales support and service that may be required.

- We will aim to reduce greenhouse gas emissions by targeting reduction in travel to deliver contracts, explore opportunities for the local sourcing of materials and use energy efficient goods, services, and products.
- We will improve resource efficiency and seek to reduce the consumption of paper, energy, water, and waste by:
    - Maintaining and repairing where possible to extend product lifespan.
    - Encouraging recycling, and the reuse or reallocation of materials.
    - Using recycled goods and materials where possible.
    - Encouraging minimal packaging and where possible subscribe to a take back scheme for packaging/equipment which can be recycled.
    - Buying products only when necessary and reducing the volume of materials consumed.
    - Selecting more durable, environmentally friendly alternatives, and complying with all legislation concerning disposal i.e., WEEE (waste, electrical and electronic equipment) Directive.
    - Buying energy efficient appliances and equipment where applicable, e.g. A-rated appliances.
    - Specifying low VOC (volatile organic compounds) paints.
    - Considering FSC (Forest Stewardship Council) trademarks or equivalent for purchases of timber.
    - Selecting environmentally friendly options for cleaning and pest control adhering to Control of Substances Hazardous to Health (COSHH) Regulations; and
    - Considering fair trade products or similar where appropriate.

Supplier On-Boarding Process

A comprehensive set of internal and external checks exists for each supplier commencing with gathering information through our supplier on-boarding form and a range of internal check to ensure an additional supplier is not being requested when a supplier with an existing Maintel relationship can be utilised. If the supplier passes initial internal checks and all required information has been provided, external checks are completed for Companies House – correct organisation set up, VAT registration, Sanctions, Adverse Media, Insolvency (Credit Check), Anti-Money Laundering and Sustainable business. All supplier passing checks are provided with the Supplier Code of Conduct and Maintel Terms and Conditions – Where it is not possible to use Maintel T's and C's for example a Cloud provider, Maintel ensures negotiations take place prior to signature to meet at least Maintel minimum requirements.

Suppliers are risk assessed and based on risk assessment and criticality to Maintel customer supply, regular supplier review and improvement meetings take place with recorded actions.

For full process please see separate document within the IMS Portal – Processes folder.

4 Document Information

Area	Information
Document Title	Business Continuity Policy
Author	Compliance Team
Process Owner	Director of Information Systems & Head of Infrastructure Services
Date Created	28/06/2021
Current Approval date	31/07/2025
Minor change approval by	Compliance Team
Substantial change approved by	Gold Command
Summary	Maintel handbook containing the Information Security policy information.
Classification	See footer
Reference	ISO22301
Associated Records	IMS Portal, Auto Task

This document is uncontrolled if any pages are printed, or it is downloaded.

Change Record

Latest Change Date	Detail	Re-approval required
31/07/2025	Space for CEO signature	Provided

This document is republished annually

Maintel

Contact us/Thank you

Solid solutions for a dynamic world

Maintel is a communications managed services provider. We empower our clients across the public and private sector to deliver mission critical services and achieve their workplace, service and customer experience goals.

03448711122
info@maintel.co.uk

69 Leadenhall Street
London, EC3A 2BG

maintel.co.uk