Data Protection and Information Security Policy Statement

Prepared by;

Katie Connor
Governance Team Leader
01922 658632
katie.connor@maintel.co.uk

Contents

1. Policy Statement

Maintel is a leading communications services company and this policy applies to all Maintel employees and any other party or individual who processes data and personal data on Mantel's behalf and/or the use of www.maintel.co.uk ("Our Site"), the Maintel Integrated Management System (IMS) and all of the company locations and applicable work sites.

Maintel consider Information Security aspects 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 necessarily control and process information about data subjects, i.e., 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 all current regulations and relevant contractual obligations. The relevant regulation for this policy is The UK General Data Protection Regulation "GDPR". Accordingly, Maintel commits to ensuring all information is handled in a secure manner whilst maintaining the Integrated Management System to meet regulatory requirements and elected certifications and accreditations.

Our Site may contain links to other websites, and wherever that occurs, it is important to note that Maintel will have no control over how your data is collected, stored, or used by such websites. Maintel advise you to check the privacy policies of any such websites before providing data to them.

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.

Please read this Data Protection and Information Security Policy statement carefully and ensure that you understand it. Your acceptance of this policy is deemed to occur upon first use of Our Site, entering pre-contract negotiations and contracted procurement of products and/or services.

- Protect information is set out in terms of.
    - **Confidentiality**: ensuring only persons who are authorised have access to information.
    - **Integrity**: ensuring the purity, accuracy, and completeness of information.
    - **Availability**: ensuring information, associated assets, and systems can be accessed when required by authorised persons.
    - **Regulator**y: regarding regulations, laws, and codes of practice in each country where it operates as a minimum standard in its Information security management standard.

Maintel will:

- Ensure that Maintel management, employees and any other individuals acting on behalf of Maintel will comply with the requirements of the Data Protection and Information Security Policy and that confidentiality of information will be maintained to protect both Maintel and its Customers physical and electronic information assets from all threats, both internal and external, deliberate or accidental, including those related to data subjects personal data and card holder data throughout the organisation.

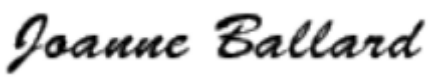
- Minimise the risk of damage to company assets, information, reputation, hardware, software, or data.

- Ensure that Maintel people and computer systems do not infringe any copyright, licensing, or laws.
- Set out clearly the company's policies relating to all aspects of the management of information, personal data, hardware, firmware, software and prevention and detection of malware.
- Define a systematic approach to risk assessment by identifying a method that is suited to the Maintel Integrated Management System (IMS), the identified business information security, legal and regulatory requirements and 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
- Commit to continual improvement of the information security management system

Responsibilities:

- The IT Director has direct responsibility for maintaining the Security Policy and providing advice and guidance on its implementation.
- All managers are directly responsible for implementing the Data Protection and Information Security Policy within their business areas, and for adherence by their staff.
- It is the responsibility of each member of staff to adhere to the Data Protection and Information Security Policy.
- 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 Information Security at all levels throughout Maintel.

This statement represents our general position on data Protection and Information Security issues, and the policies and practices we will apply in conducting our business.



Joanne Ballard

ESG Strategy and Compliance Director

2. Business Continuity

The purpose of Business Continuity/Disaster Recovery is to ensure that all critical Company business activities can be kept at normal or near-normal performance following an incident that has the potential to disrupt business operations. All Maintel offices are included within the scope of this policy.

The following areas are covered within the BCP.

- Building Inaccessibility
- Civil Unrest
- Cyber Attack
- Fire Event
- Flood or Water Event
- IT Infrastructure and 3rd part 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

Areas covered by the BCP are reviewed, at a minimum, annually and at the time of an event and adjusted, as necessary.

It is our Policy to ensure that:

- Provision of products and services is maintained as near to normal as possible
- We identify through appropriate risk assessment, the events that may cause an event and mitigate those risks as far as possible
- An incident timeline is minimised during any disaster event and operations return to as near normal as possible in the shortest time frame.
- All teams are aware of how to identify, report and safely work during a disaster event
- Regulatory and legislative requirements are met
- Appropriate communication and training will be provided for all employees
- Our BC/DR is maintained by a schedule of tests and Internal audits

Each department is responsible for preparing and maintaining current and comprehensive business continuity plans (BCP) for its operations. Certain departments, such as Systems/IT, are also responsible for disaster recovery plans (DRP) to ensure that any damage or disruptions to critical assets can be quickly minimised and that these assets can be restored to normal or near-normal operation in a minimum time frame.

When a plan is completed, approved, and implemented, each plan will include procedures and support arrangements which ensure on-time availability and delivery of customer products and services. The BC/DR plans are certified annually through external audit.

Maintel recognises the importance of an active and fully supported BC/DR program to ensure the safety, health and continued availability of its employees and the production and delivery of services for customers.

To drive continual improvement within the BC/DR, Maintel set objectives on an annual basis as part of the Management Review Process; these objectives ensure the system is appropriately monitored and measured.

All objectives are communicated to staff and include key responsibilities, timescales, and appropriate measures of success.

3. Cookies

3.1. Our use of Cookies

Our Site may place and access certain first party Cookies on your computer or device. First party Cookies are those placed directly by Maintel and are used only by Maintel. We use Cookies to facilitate and improve your experience of Our Site and to provide and improve our products and/or services. We have carefully chosen these Cookies and have taken steps to ensure that your privacy and personal data is always protected and respected.

By using Our Site, you may also receive certain third-party Cookies on your computer or device. Third party Cookies are those placed by websites, services, and/or parties other than us. Third party Cookies are used on Our Site for performance. These Cookies are not integral to the functioning of Our Site and your use and experience of Our Site will not be impaired by refusing consent to them.

All Cookies used by and on Our Site are used in accordance with current and applicable "Cookie Law".

Please refer to Our Site under Cookie Choices, to provide consent where you choose to. By giving your consent to the placing of Cookies you are enabling us to provide the best possible experience and service to you. You may, if you wish, deny consent to the placing of Cookies; however certain features of Our Site may not function in part, fully or as intended.

Certain features of Our Site depend on Cookies to function. Cookie Law deems these Cookies be "strictly necessary". These Cookies are shown below.

Your consent will not be sought to place these Cookies, but it is still important that you are aware of them.

You may still block these Cookies by changing your internet browser's settings, but please be aware that Our Site may not work properly if you do so. We have taken great care to ensure that your privacy is not at risk by allowing them.

The following first party Cookies may be placed on your computer or device:

Name of Cookie	Purpose	Strictly Necessary
eu_necessary_cookie	EU cookie banner	Yes
eu_performance_cookie	EU cookie banner	Yes

Our Site uses analytics services provided by Google Analytics.

Website analytics refers to a set of tools used to collect and analyse anonymous usage information, enabling us to better understand how Our Site is used. This, in turn, enables Maintel to improve Our Site and the products and/or services offered through it.

You do not have to allow Maintel to use these Cookies, however whilst our use of them does not pose any risk to your privacy or your safe use of Our Site, it does enable us to continually improve Our Site, making it a better and more useful experience for you.

The analytics service used by Our Site uses the following Cookies:

Name of Cookie	First / Third Party	Provider	Purpose
_ga	Third	Google analytics	Performance Expires after 2 years
_gat	Third	Google analytics	Performance Expires after 10 minutes
_gid	Third	Google analytics	Performance Expires after 10 minutes
Wp	Third	Act On	Visitor Activity Persistent

3.2. Force 24 Marketing automation platform

We also use Force 24's marketing automation platform. Force24 cookies are first party cookies and are enabled at the point of cookie acceptance on Force 24 site. The cookies are named below:

Name of Cookie	First / Third Party	Provider	Purpose
F24_autoID	First	Force 24	Temporary identifier on a local machine or phone browser that helps us track anonymous information to be later married up with f24_personid. If this is left anonymous it will be deleted after 6 months. Non-essential, first party, 10 years, persistent.
F24_personID	First	Force 24	This is an ID generated per individual contact in the Force24 system to be able to track behaviour and form submissions into the Force24 system from outside sources per user. This is used for personalisation and ability to segment decisions for further communications. Non-essential, first party, 10 years, persistent.

The cookies allow us to understand our audience engagement thus allowing better optimisation of marketing activity.

The information stored by Force24 cookies remains anonymous until:

- Our website is visited via clicking from an email or SMS message, sent via the Force24 platform and cookies are accepted on the website.
- A user of the website completes a form containing email address from either our website or our Force24 landing pages.

The Force24 cookies will remain on a device for 10 years unless they are deleted.

Other Tracking

We also use similar technologies including tracking pixels and link tracking to monitor your viewing activities

Device and browser type and open statistics

All emails have a tracking pixel (a tiny invisible image) with a query string in the URL. Within the URL we have user details to identify who opened an email for statistical purposes.

Link Tracking

All links within emails and SMS messages sent from the Force24 platform contain a *unique tracking* reference, this reference help us identify who clicked an email for statistical purposes.

3.3. Managing Cookies

In addition to the controls that Maintel provide, you can choose to enable or disable Cookies in your internet browser. Most internet browsers also enable you to choose whether you wish to disable all cookies or only third-party Cookies. By default, most internet browsers accept Cookies, but this can be changed. For further details, please consult the help menu in your internet browser or the documentation that came with your device.

You can choose to delete Cookies on your computer or device at any time, however you may lose any information that enables you to access Our Site more quickly and efficiently including, but not limited to, login and personalisation settings.

It is recommended that you keep your internet browser and operating system up-to-date and that you consult the help and guidance provided by the developer of your internet browser and manufacturer of your computer or device if you are unsure about adjusting your privacy settings.

4. Data Protection

4.1. 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

4.2. Your Rights

As a data subject, you have the following rights under GDPR, 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 (please contact Maintel using the details in section 6).
- The right to be forgotten – i.e., the right to ask Maintel to delete any personal data Maintel hold about you (Maintel only hold your personal data for a limited time, as explained in this policy but if you would like Maintel to delete it sooner, please contact us using the details in section 6).
- The right to restrict (i.e., prevent) the processing of your personal data.
- The right to data portability (obtaining a copy of your personal data to re-use with another service or organisation).
- The right to object to Maintel using your personal data for particular purposes; and
- 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.

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 in section 6 below and we will do our best to solve the problem for you as soon as reasonably possible. If we are unable to help, 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.

4.3. What data do we collect?

Depending upon your interaction with Maintel and use of Our Site, Maintel may collect some or all of the following personal data and non-personal data, please also see the Cookies section on Maintel use of Cookies and similar technologies.

- Name
- Business/Company Name
- Job Title
- 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
- Web browser type and version
- Operating system
- A list of URLs' starting with a referring site, your activity on Our Site, and the page you exit from

4.4. How do we use your Data?

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. For more details on security see section 4.5, below.

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 (e.g., by subscribing to emails) or because it is in our 'legitimate interests' as defined and prescribed in the GDPR. Specifically, Maintel may use your data for the following purposes:

- Providing and managing your Account.
- Providing and managing your access to Our Site.
- Personalising and tailoring your experience on Our Site.
- Supplying products and/or services to you (please note that Maintel require your personal data to enter into a contract with you).
- Personalising and tailoring Maintel products and services for you and your business
- Replying to emails from you.
- Supplying you with emails that you have opted into (you may unsubscribe or opt-out at any time by clicking the unsubscribe link in our emails).
- Analysing your use of Our Site and gathering feedback to enable Maintel to continually improve Our Site and your user experience.

With your permission and/or where otherwise permitted by law, Maintel may also use your data for marketing purposes which may include contacting you by email and/or telephone and/or text message and/or post with information, news and offers on Maintel products and/or services. We will not, however, send you any unsolicited marketing or spam and will take all reasonable steps to ensure that we fully protect your rights and comply with obligations under the current Data Protection regulations and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

Third parties whose content appears on Our Site may use third party Cookies, as detailed in the Cookies section. Please refer to the Cookies section within this document for more information on controlling Cookies. Please note that we do not control the activities of such third parties, nor the data they collect and use and advise you to check the privacy policies of any such third parties.

You have the right to withdraw your consent to Maintel using your personal data at any time, and to request that Maintel delete it.

Maintel do not keep your personal data for any longer than is necessary considering the reason(s) for which it was first collected. Data will therefore be retained for the following periods (or its retention will be determined on the following bases):

- Marketing contact information: Until permission is withdrawn, i.e., Unsubscribe
- In accordance with contractual obligations; full term of agreement plus 7 additional years
- Cardholder data is not retained for any reason

4.5. How and where do we store your Data?

We only keep your personal data for as long as we need to use it as described above in section 4.4, and/or for as long as we have your permission to keep it.

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 European Economic Area ("the EEA") (The EEA consists of all EU member states, plus Norway, Iceland, and Liechtenstein). If Maintel do store data outside the EEA, 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)

4.6. Do we share 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.

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

These may include payment processing, delivery 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 under the law.

We may also compile statistics about the use of Our Site including data on traffic, usage patterns, user numbers and other information. All such data will be anonymised and will not include any personally identifying data, or any anonymised data that can be combined with other data and used to identify you. We may from time to time share such data with third parties such as prospective investors, affiliates, partners, and advertisers. Data will only be shared and used within the bounds of the law.

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

4.8. How can you control your Data?

When you submit personal data via Our Site, you may be given options to restrict our use of 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. Please note, however, that these services will not prevent you from receiving marketing communications that you have consented to receiving.

4.9. Your right to withhold information

You may access Our Site without providing any data at all. However, to use all features and functions available on Our Site you may be required to submit or allow for the collection of certain data.

You may restrict Maintel use of Cookies. For more information, see Cookies section within this document.

4.10. How can you access your Data?

You have the right to ask for a copy of any of your personal data held by Maintel (where such data is held). Under the GDPR, no fee is payable, and we will provide all reasonable information in response to your request free of charge.

Please contact Maintel for more details at subjectaccessrequest@maintel.co.uk, or using the contact details below in section 6.

5. Risk Management

The purpose of this policy is to describe Maintel risk management framework and how risks will be identified, assessed, monitored, and reported within the business at the corporate level.

Risk management is a process which aims to help businesses understand, evaluate, and take action on all their risks with a view to increasing the probability of achieving their 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.

It is our policy to.

- identify risks in relation to the achievement of our objectives
- assess their relative likelihood and impact
- respond to the risks identified, considering our assessment
- 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 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 is regularly reviewed and approved by the Board.

Accountability and Responsibility

The table summarises the responsibility of the various risk management responsibilities:

Body	Roles and responsibilities include:
Board	Set the tone for risk management including risk appetite Have overall responsibility for the risk management arrangements Periodically review the corporate risk register, Receive reporting of any new major risks Horizon scanning and consideration of emerging risks
Audit and Risk Committee	Ensure the approach to risk management is sound and operating as intended Challenge the risk register, the scoring, the risks on the register Monitor actions and processes to ensure compliance Assess the level of assurance on the controls in place Horizon scanning and consideration of emerging risks
Executive directors	Periodically review, update, and amend the entire risk register Challenge the risks, scores, and mitigations of other risk owners Recommend where further mitigating actions may be required
Governance Team Leader	Act as an advocate for risk management across all levels of the business Responsible for the development of the business's risk management procedures subject to approval by the Board Drafting the Risk Management Policy for the Board approval and presenting it for review and approval periodically

Body	Roles and responsibilities include:
	Co-ordinate the risk management activities of the management team and IMS management team and escalating new risks to the appropriate risk register Compile risk information and reports for the Executive team and Board Providing risk management update reports to the Board Monitoring the application of the Risk Management Policy.
IMS Management Team	Responsible for the Security and Health and Safety Risk Assessments and the Environmental Significance Assessment 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 activity/asset Identify precautions and recommend the actions to be taken to protect the 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 sufficient effectiveness to justify the residual/net risk score Identify and report changes in the external or internal environment that can influence the risk profile
All Staff	Understand, accept, and implement risk management processes within their areas of operation 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

Maintel, like any other business, is exposed to potential risks that could disrupt or destroy critical business functions and/or the production and delivery of services to our customers. Our strategy for continuing business in the event of a disaster is to ensure the safety and security of all employees and to continue critical business functions, production, and delivery of services from predefined alternatives.

6. General Information

- **Changes to Maintel Policy**: We may change this Policy from time to time (for example, if the law changes). Any changes will be immediately posted on Our Site, and you will be deemed to have accepted the terms of the updated Policy on your first use of Our Site following the alterations. We recommend that you check regularly to keep up to date.

- **Contacting Maintel**: If you have any questions about this Policy, please contact us by email at gdpr@maintel.co.uk, by telephone on +44(0)344 871 1122, or by post at 160 Blackfriars Road, Southwark, London, SE1 8EZ. Please ensure that your query is clear, particularly if it is a request for information about the data Maintel hold about you.

- **Data Protection Officer**: Maintel is not obligated to allocate the position of Data Protection Officer (DPO) but has chosen to do so. , .

    - Maintel internal contact for Data Protection matters is
        - Email address: legal.enquiries@maintel.co.uk
        - Telephone Number: +44(0)344 871 1122
        - Address: 160 Blackfriars Road, Southwark, London, SE1 8EZ

- **Maintel Europe Ltd**: is a limited company registered in England under company number 023665837, whose registered address is 160 Blackfriars Road, London, England, SE1 8EZ, and whose main trading address is 160 Blackfriars Road, London, England, SE1 8EZ.

- **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. Required breaches shall be reported to the Supervisory Authority within 72 hours and the Data Subject/s as soon as possible.

- **Training**: All Maintel employees receive Data Protection training during the annual refresher, at Induction and during job role changes. Line Managers are responsible for ensuring information and training is provided to all members of their team.

- www.maintel.co.uk: is owned and operated by Maintel Europe Ltd

7. Document Information

Area	Information
Document Title	Data Protection and Information Security Policy Statement
Author	Governance Team Leader
Process Owner	Head of Information Systems
Date Created	27/10/2014
Date Approved	15/05/2023
Approved By	ESG Strategy and Compliance Director
Summary	Overarching policy detailing the commitment to Information Security and Data Protection, including GDPR, Cookies, Business Continuity and Risk Management
Classification	ISO27001, PCI-DSS, HSCN, Cyber Essentials, GDPR
Reference	Public
Associated Records	Atlas - IMS Portal

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

Change Record

Latest change date	Detail	Re-approval
15/05/2023	Amended to DPO details	Provided