AdvancedMaintenanceUKLtd
Units 2-4 Chiltern Enterprise Centre, Station Road, Theale, Berkshire RG7 4AA
T: 01189303 738 ● W: www.advancedmaintenance.co.uk ● E: info@advancedmaintenance.co.uk

Information Security Management System Policy

The General Data Protection Regulations (GDPR) comes into force on 25th May 2018 superseding the UK's Data Protection Act 1998. The UK is currently passing its own Data Protection Bill through Parliament which will go over and above the GDPR requirements.

It is a legal requirement for the Advanced Maintenance UK Ltd to comply with the GDPR. It is also AMUK's policy to ensure any personal data held by us in whatever form be treated with sensitivity and privacy, as befits such information.

Advanced Maintenance UK Ltd is registered with the Information Commissioners Office (ICO) - Registration Reference Z2474095.

AMUK needs to keep certain information about its employees, customers, and suppliers for financial and commercial reasons and to enable us to monitor performance, to ensure legal compliance and for health and safety purposes.

This policy sets out how we seek to protect personal data and ensure that staff understands the rules governing their use of personal data to which they have access in the course of their work.

In particular, this policy requires staff to ensure that the Data Protection Officer and/or the GDPR Support Team be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Data Protection Officer

To ensure the implementation of this policy AMUK has designated Hazel Lightowler as the Data Protection Officer. All enquiries relating to the holding of personal data should be referred to her in the first instance.

Sensitive Personal Data

In most cases where AMUK processes sensitive personal data they will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work).

Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and Relevance

AMUK will ensure that any personal data they process is done lawfully, fairly and transparently.

The data collected on a subject should be adequate, relevant and limited to what is necessary in relation to the purposes for which it is being collected.

Personal data shall be accurate, where necessary kept up to date, and kept only for the period of time required to complete the processing task for which it is obtained.

Individuals may ask that AMUK correct inaccurate personal data relating to them. If you believe that information held is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Data Protection Officer in writing.

Access to Personal Data

Access to all personal data is restricted to limited staff. Employment checks are carried out on personnel as applicable to their role and / or the service they are delivering. Employees will obtain Disclosure Barring Service checks and complete relevant security clearances as required.

Right to be Forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Data Audit and Register

Regular data audits to manage and mitigate risks will inform AMUK's data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

I.T Security

Personal data stored electronically will be protected by AMUK's security policies and processes. AMUK operates an Acceptable Use Policy, a Password Policy and a Breach of Data Policy.

Accesses to all systems are restricted to limited employees as required for the application of their job role.

Only AMUK issued USB drives must be used by AMUK's employees. All third-party USB drives must be checked by the IT department before they are used in our AMUK systems.

Our business continuity arrangements identify how we will protect and recover the personal information we hold.

Transferring Data Internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the EEA without first consulting the Data Protection Officer.

Reporting Breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary.
- Individuals may ask that AMUK correct inaccurate personal data relating to them.

If you believe that information held is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Data Protection Officer in writing.

Access to Personal Data

Access to all personal data is restricted to limited staff. Employment checks are carried out on personnel as applicable to their role and / or the service they are delivering. Employees will obtain Disclosure Barring Service checks and complete relevant security clearances as required.

Right to be Forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Data Audit and Register

Regular data audits to manage and mitigate risks will inform AMUK's data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

I.T Security

Personal data stored electronically will be protected by AMUK's security policies and processes. AMUK operates an Acceptable Use Policy, a Password Policy and a Breach of Data Policy.

Accesses to all systems are restricted to limited employees as required for the application of their job role.

Only AMUK issued USB drives must be used by AMUK's employees. All third-party USB drives must be checked by the IT department before they are used in our AMUK systems.

Our business continuity arrangements identify how we will protect and recover the personal information we hold.

Transferring Data Internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the EEA without first consulting the Data Protection Officer.

Reporting Breaches

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Any breach of the Data Protection Policy, either deliberate or through negligence, may lead to disciplinary action being taken and could in some cases result in a criminal prosecution.

Third Party Access to Advanced Maintenance UK Ltd.'s ICT Systems

With the exception of our primary IT support partner access to AMUK systems is restricted and can only be accessed as agreed with the System Administrator.

All third-party providers are bound by confidentiality and security clauses within the service level agreements agreed.

Subject Access Requests

You are entitled to know what personal information AMUK holds about you, why it is being held and who AMUK discloses your information to.

- All Subject Access Requests must be referred to the HR Manager in the first instance.
- All Subject Access Requests will be dealt with in accordance with the current ICO Code of Practice on Subject Access.

Storage of Data

Hard copy personal data, whether related to our employees; suppliers or our customers are held in secure cabinets with access restricted to limited staff. This personal data is not routinely carried in transit however where it is required to be transported it will be held in secure containers.

Electronic personal information held locally will be held with restricted access to limited staff. This will be password controlled via the Network Login. This personal data is not routinely carried in transit however where it is required to be transported it will be held on encrypted USB drives.

Obsolete and unused IT equipment is stored for a short period to ensure all information required has been removed, and then destroyed by our IT Company to a military grade level.

Retention of Records and Data

For some records and data there are statutory retention periods with statutory authorities. For other records there is no statutory retention periods however there are either recommended retention periods or retention periods required by third party organisations.

AMUK will retain records in accordance with the relevant authorities' recommendations and guidelines.

Disposal of Data

All hard copy personal data and IT equipment including hard drives are disposed of in a secure manner by an approved waste disposal contractor and relevant waste transfer notes obtained.

All hard copy personal data is either securely shredded on-site or disposed of offsite via secured facilities. Hard drives are shredded at an off-site facility.

Electronic data is removed from our systems either through deletion or if required, archiving. All archived records are secured stored with limited access.

Marketing

Clients may be contacted for marketing purposes. No marketing materials may be e-mailed to any other individuals or companies without prior permission of the recipient.

Managers should check our compliance with legal obligations such as copyright or licensing requirements when downloading or copying information, and when publishing documents.

The Information Security Management System Manual is subject to continuous review and improvement.

SIGNED BY DIRECTORS:

Mr Ricky Gale	Mr David Jones
Operations Director	**Technical Director**

Signed copy held by Data Protection Officer