



INFORMATION AND DATA SECURITY POLICY STATEMENT

Introduction and purpose

IOMA has an Information and Data Security Policy as a means of protecting the information and IT systems of our company from unauthorised access, use, crime, disclosure, disruption, destruction or loss.

The aim is to protect IOMA and our uniform and work wear supplies for the public and commercial sectors as well as our customers from the adverse impact on our operations, our clients and our professional standing of any IT related failure, breach of security and disclosure of confidential and restricted information.

These procedures are in addition to our data protection obligations under the Data Protection Act 1998, which are detailed separately in complementary policies, including our Business Continuity Policy. The Senior Responsible Director for the implementation, monitoring and reporting on all matters relating to information and data security is the Sales Director:-

Statement of Policy

The IOMA Information and Data Security Policy operate within the following Framework:-

- **Confidentiality:** ensuring that information can only be accessed by authorised persons;
- **Integrity:** ensuring the information is current & correct without error or modification;
- **Availability:** ensuring that accessibility of information and data;
- **Security:** ensuring the secure collection, processing, and storage of information on IOMA computer systems and the secure transmission across networks to other IT systems, especially when using remote and hand-held devices.

The Information and Data Security Policy Statement is applicable to all staff and sub-contractors working for or on behalf of IOMA and is contained in our ISO9001 Quality Management systems and Manual. The Company is registered with the Office of the Information Commissioner.

Roles and responsibilities within the Company

The implementation of the Policy is the responsibility of our Sales Director to report routinely to our Board. He is also responsible for ensuring compliance with all industry guidance, legislation and good practice relating to data protection and information security as well as the contract terms and condition of our customers.



Implementing effective IT security systems and practices

IOMA has a service level agreement with 5 Star Computing consultancy to ensure our systems and software operates efficiently and effectively and have the required protective systems. Also, we have the technical support and back up capability to ensure we can resume operational effectiveness with the minimum of delay or impact on our service delivery. This IT consultancy support ensures that the procedures and practices of IOMA and/or the staff include:-

- Maintaining an inventory of all computer equipment and software;
- Registering all proprietary software and ensures compliance with licence conditions;
- Locating File Servers that hold or process critical, and/or sensitive data in secure areas with controlled access;
- Storing business critical information on the network and regularly and routinely “backed up” that data;
- Minimising the risks of computer viruses through training and anti-virus software;
- Reporting suspected computer viruses immediately to the 5 Star IT Consultant;
- Prohibiting the use of unlicensed software on IOMA computing equipment;
- Forbidding the use of personal no-work related software onto IOMA computers;
- Providing archive of key data securely stored off-site accessible in the event of a major incident or business disruption;
- Exiting and log off or lock PCs when leaving them unattended;
- Securing portable computing devices (laptops/tablets) and removable data storage at all times on or off IOMA premises.

The Company recognises that access to the Internet and e-mail access carries with it a security, business threats and virus related risks and therefore all staff are notified of these risks and dangers at their induction, Terms and Conditions and in the Staff Handbook.

As such, our Code of Conduct and Induction specifically refers to a prohibition of accessing inappropriate websites for personal and non-work purposes. Accessing such unauthorised websites or accessing confidential information may result in disciplinary action leading to dismissal. IOMA has comprehensive arrangements for complying with data protection, security duties for all customer information, especially police personnel data.

Our quality assurance systems and organisational structures ensure personal and confidential data for customers will be secure at all times and safely destroyed by:-

- Assigning the Operations Director as the Data Controller who oversees our management information, compliance and the integrity of data;
- Communicating our access control procedures to the secure IT Room and Server facility at Induction and during any Business Continuity Planning exercise;
- Adhering to our Non Police Personnel Vetting Civilian Level 1-3 to ensure the DBS clearance for all our workforce Undertaking Employee and Workforce Vetting to ensure the integrity of our staff through enhanced DBS and pre-employment checks;

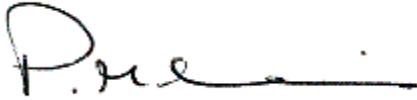


- Issuing this policy, confidentiality and access control arrangement to data and secure facilities as Terms and Conditions of Employment to the Directors, all employees and designated individuals responsible for accounting and administration;
- Providing IT security training to the workforce as part of our commitment to CPD training and business continuity related protection and knowledge;
- Ensuring only authorised members of the workforce have access to our Management Information which is password protected and in special cases encrypted, if required;
- Having robust retention, storage and destruction arrangements procedures for digital, portable and paper copies of customer information as well as highly secure premises with lockable storage cabinets and procedures for the safe destruction of all sensitive and restricted customer information for police forces, using a specialist confidential waste contractor.

The Data Control procedure ensures that our confidential information is retained in accordance with the contract terms. All data, customer information and confidential material will be destroyed by Russell Richardson a British Security Industry Association (BSIA) Accredited (BS8470) and licensed contractor and a Certificate of Destruction is obtained from the contractor as proof that the destruction process has been completed.

Monitoring and reporting obligations

The Managing Director in consultation with the Operation Director and Sales Director along with the IT consultant will report quarterly to the Board of Directors. These reports will address the level of compliance, the outcome of regular and ad hoc inspection of these procedures to protect the confidentiality, integrity and security of our IT systems.

Signed: 

Name: **Paul Levinson**

Title: DIRECTOR

Date: 10 February 2020

Author: Adrian Thomas Sales Director and Matthew Dale IT Consultant 5 Star

Next Review Date: February 2024