

## INFORMATION SECURITY MANAGEMENT SYSTEM

As industry leaders in providing security services inclusive of manned guarding, key holding and alarm response we have an obligation to our customers, employees, legislative and regulatory requirements as well as business values to ensure that the information that we hold and process for operational purposes is processed fairly, lawfully and securely. In order for us to do this, we have determined a range of security controls, policies and procedures in line with the requirements of ISO 27001:2013 Information Technology – Security Techniques.

- This policy's goal is to protect our informational assets against all internal, external, deliberate or accidental threats.
- Top management have approved the information security policy & shall strive to continually improve the Information Security Management System (ISMS).
- The Information security policy and associated objectives ensures that:
  - **Information will be protected** against unauthorized access;
  - **Confidentiality** of information will be assured;
  - **Integrity** of information will be maintained;
  - **Availability** of information for business processes will be maintained;
  - **Legislative and regulatory** requirements will be met;
  - **Business continuity plans** will be developed, maintained and tested;
  - **Information security training** will be available to all employees;
  - **All actual or suspected information security incidents** will be reported to the CEO (Managing Director) and will be thoroughly investigated.
- Procedures exist to support the policy, including virus control measures, passwords, continuity plans and effective risk management.
- Business requirements for availability of information systems will be met.
- The CEO (Managing Director) is responsible for maintaining the policy and providing support and advice during its implementation.
- All managers are directly responsible for implementing the policy and ensuring staff compliance in the respective departments.
- Compliance with contractual security obligations.
- Compliance with the Information Security Policy is mandatory.

## DATA PROTECTION

Our data protection policy sets out our commitment to protecting personal data and how we implement that commitment with regards to the collection and use of personal data.

We are committed to:

- ensuring that we comply with the eight data protection principles held within the Act
- meeting our legal obligations as laid down by the GDPR
- ensuring that data is collected and used fairly and lawfully
- processing personal data only in order to meet our operational needs or to fulfill legal requirements

- taking steps to ensure that personal data is up to date and accurate
- establishing appropriate retention periods for personal data
- ensuring that data subjects' rights can be appropriately exercised
- providing adequate security measures to protect personal data
- ensuring that a nominated officer is responsible for data protection compliance and provides a point of contact for all data protection issues
- ensuring that all staff are made aware of good practice in data protection
- providing adequate training for all staff responsible for personal data
- ensuring that everyone handling personal data knows where to find further guidance
- ensuring that queries about data protection, internal and external to the organization, are dealt with effectively and promptly
- Regularly reviewing data protection procedures and guidelines within the organization.

After the introduction of The General Data Protection Regulation on 25<sup>th</sup> May 2018, we ensure that all of our operational policies and procedures are compliant to the GDPR and to the Data Protection Act 2018.

## PRIVACY

We collect certain information or data about you when you use our website ([www.ssgukltd.com](http://www.ssgukltd.com)).

This includes:

- questions, queries or feedback you leave, including your email address if you send an email and telephone number if you complete our enquiry form
- your IP address, and details of which version of web browser you used
- information on how you use our site, using cookies and page tagging techniques to help us improve the website

This helps us to:

- improve the site by monitoring how you use it
- respond to any enquiries you send us, if you've asked us to
- provide you with information on our products and services

We can't personally identify you using your data.

### Where your data is stored

We store your data on our cloud storage in the UK.

By submitting your personal data, you agree to this.

### Keeping your data secure

Transmitting information over the internet is generally not completely secure, and we can't guarantee the security of your data.

### Any data you transmit is at your own risk.

We have procedures and security features in place to try and keep your data secure once we receive it.

# Information Security Management System Policy



ISO 27001:2013 Ref; Clause 5.2

---

We won't share your information with any other organizations for marketing, market research or commercial purposes, and we don't pass on your details to other websites.

## **Disclosing your information**

We may pass on your personal information if we have a legal obligation to do so.

## **Your rights**

You can find out what information we hold about you, and ask us not to use any of the information we collect.

Approved by

A handwritten signature in black ink, appearing to read 'Ahmad'.

Ahmad Rafique (C.E.O.)

1<sup>st</sup> September 2021

This policy shall be reviewed annually as a minimum and available to external parties upon request