GSS - Information and Data Security Policy

1. Introduction

Information is a vital asset to any organisation and this is especially so in a knowledge-driven organisation such as Global Solution Services UK Ltd (GSS UK Ltd) , where information will relate to the delivery of Information, advice, guidance learning, teaching administration and management. This policy is concerned with the management and security of GSS's information assets (an information asset is defined to be an item or body of information, an information storage system or an information processing system which is of value to GSS) and the use made of these assets by its members and others who may legitimately process this information on behalf of our customers, clients, staff and others who have an interest in our organisation and its business.

This overarching policy document provides an overview of information security alongside our GDPR and Confidentiality policy documents which taken together constitute the Information Security Policy for GSS.

2. Purpose

An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets. In this world of computerised technology it is necessary to ensure that all GSS's computing facilities, programs, data, network and equipment are adequately protected against loss, misuse or abuse, and that adverse effects of failures in confidentiality, integrity, availability, cyber-attack and compliance are minimised and eliminated and that this protection is as cost-effective as possible.

It is also important to ensure that all users are aware of and fully comply with this policy statement and all associated policies, and are aware of and work in accordance with the relevant procedures and codes of practice;

It will always be our responsibility to ensure that all users are aware of and fully comply with the relevant UK and European Union legislation and that this is upheld and monitored regularly for changes which may affect our business and working patterns.

3. Scope

This document and other related documents in the GDPR Policy apply to all information assets which are owned by GSS and used by its staff, customers, clients and contractors for the business purposes which are connected to any networks managed by GSS and our Main contractors.

The sub documents in the Information Security Policy (namely GDPR, confidentiality, IT Monitoring and Equipment use policies) apply to all information which GSS processes, irrespective of ownership or form.

All documents in the Information Security Policy sub documents apply to all members of our staff (including Associates, agency staff, temporary or contract) working on behalf of the organisation and any others who may process information on behalf of the GSS.

4. Structure

The Information and Data Security Policy is structured in accordance with the recommendations based on the control guidelines set out in the industry standard ISO 27001.

This overall document has a set of other sub-policy documents which together constitute the Information Security Policy of GSS UK Ltd. All of these documents are of equal standing and can be taken in conjunction with or alongside this policy.

Any personal data which we collect, record or use in any way whether it is held on paper, on computer, or other media will have appropriate safeguards applied to it to ensure that we comply with the General Data Protection regulations 2018). We fully endorse and adhere to the eight principles of Data Protection as set out in the 2018 Act. These principles state that personal data must be:-

· Fairly and lawfully processed
· Processed for specified and lawful purposes and not in any other way which would be incompatible with those purposes
· Adequate, relevant and not excessive
· Accurate and kept up to date
· Not kept for longer than is necessary
· Not passed, given or discussed with any party outside of that of GSS or relevant parties in line with the processing of the customers details
· Processed in line with the data subject's rights and kept secure
· Not transferred to a country which does not have adequate data protection laws.

5. Information Security Principles

For the avoidance of doubt GSS adopts the following which continue to underpin this policy:

1. Information will be protected in line with all relevant GSS's policies and legislation, notably those relating to data protection, human rights and freedom of information.

2. Each information asset will have a nominated owner who will be assigned responsibility for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect the asset

3. Information will be made available solely to those who have a legitimate need for access.

4. All information will be classified according to an appropriate level of security.

5. The integrity of information will be maintained at all times.

6. It is the responsibility of all individuals who have been granted access to information to handle it appropriately in accordance with its classification.

7. Information will be protected against unauthorised access and only individuals who have been appropriately assessed, vetted and security checked will have access to sensitive data

8. We must always ensure that paper records are kept securely and managed effectively and are kept in a secure place with lockable cabinets, cupboards etc and accessed by those with authority only.

9. Customer data, confidential information and any client information must be transported using the guidance laid out in GSS's Transportation of Data.

10. Information pertaining to GSS's business including customer data, databases, emails and confidential information will NOT be stored on any external personal devices at any time under any circumstances

11. Compliance with the Information Security policy will be enforced.

12. Before any new systems are introduced, a risk assessment process will be carried out which will include an assessment of the legal obligations that may arise from the use of the system. These legal obligations will be documented and a named system controller, with responsibility for updating that information, will be identified.

6. Third Party Access

All third parties who are given access to the organisation's information systems, whether suppliers, customers, contractors or otherwise, must agree to follow the organisation's information handling, retention and security policies. A copy of the information security policies and the third party's role in ensuring compliance will be provided to any such third party, prior to their being granted access.

The organisation will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the information being disclosed or made accessible, GSS may require external suppliers of services to sign a confidentiality agreement to protect its information assets which may form party of any contractual agreements between GSS and the third party

Persons responsible for agreeing maintenance and supporting contracts will ensure that the contracts being signed are in accord with the content and spirit of GSS's security policies.

All contracts with external suppliers for the supply of services to GSS must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier/organisation or individual.

7. Backup and system

GSS will ensure that appropriate backup and system recovery procedures are in place. Backup of GSS's data and the ability to recover this is an important priority. GSS's Management is responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the needs of the business and is conducted diligently to ensure compliance with our internal and external Contracts.
Systems are backed up automatically to a cloud based system

8. Physical Access to information

Areas and offices where Confidential or Restricted information is processed shall be given an appropriate level of physical security and access control. GSS's Head office is located within a secure building with key fob entry to all areas. Staffs with authorisation to enter such areas are provided with information on the potential security risks in the area and the measures used to control them.

All GSS's staff who have access to data must have signed and agree to the protection of that data and understand and abide by the codes of conduct in the sub documents supplied.

Data used for the purpose of delivering GSS's business must be accessed from GSS supplied or any other device authorised in writing by Richard Wood.

When sending out information on behalf of GSS or it partner organisations to customers whether in a single email or multiple adherence to GSS Confidentiality policy must be adhered to including the use of bcc emails where customer details are contained.

Under no circumstances will information pertaining to GSS, customers, clients, or business information be stored on any devices other than those supplied by GSS.

Information pertaining to GSS's business must not be downloaded, stored or saved on any personal device at any time and for any purpose.

Where sensitive or protected data is accessed from any non GSS supplied device any such device is subject to the same security procedures as GSS supplied devices. Written authorisation must be obtained from Richard Wood to access any data held on private networks, cloud based storage, cloud based databases, remote email access or any other similar electronic data repository.

9. Cryptography

The policy on cryptographic controls includes procedures to provide appropriate levels of protection to Confidential or Restricted information whilst ensuring compliance with statutory, regulatory and contractual requirements.

Confidential or Restricted information shall only be imported to or taken for use away from the organisation in an encrypted form. All information pertaining to external customers, clients and potential sensitive information must be encrypted in line with GSS Encryption codes.

Authorised staff shall be able to gain access, when needed, to any relevant information held in encrypted form, but must adhere to confidentiality and Data protection policies at all times.

The confidentiality of information being imported or transferred on portable media or across networks must be protected by use of appropriate encryption techniques. (see GSS's encryption documents) Encryption shall be used whenever appropriate on all remote access connections to the organisation's network and resources.

Encryption codes are regularly monitored, assed and changed to ensure they are constantly able to maintain the highest levels of security and protection of our information.

GSS uses a randomly selected password generator for all passwords which must under no circumstances be shared with ANYONE at ANYTME.

10.Governance

Responsibility for the production, maintenance and communication of this policy document and all sub-policy documents will be the responsibility of the IT Security Manager alongside GSS Directors.

All documents constituting to and or related to the Information Security Policy will be reviewed annually. It is the responsibility of the IT Security Manager and GSS Directors to ensure that these reviews take place. It is also the responsibility of GSS's Directors to ensure that the policy set is and remains internally consistent.

Any substantive changes made to any of the documents in the set will be communicated to all relevant personnel. This policy is also in conjunction with GSS Cyber Essential Plus certification

Signed
Sonia Benjamin-Leach (Director)
November 2021