TGC COMPUTERS LTD
INFORMATION SECURITY POLICY

1 INTRODUCTION

TGC Computers Ltd *(hereinafter referred to as the **"Company"**)* has an extensive and robust Information Security Program that consists of a vast array of policies, procedures, controls and measures. This Information Security Policy is the foundation of this program and ties together all other policies as they relate to information security and data protection.

The Company Information Security Policy covers all aspects of how we identify, secure, manage, use and dispose of information and physical assets as well as acceptable use protocols, remote access, password and encryptions. To ensure that the importance of each information security area is not missed or vague, we use separate policies and procedures for each information security area and where applicable, reference these external policies in this document.

All information security policies and procedures should be read and referred to in conjunction with each other, as their meaning, controls and measures often overlap. The policies and documents that form part of the Company ***Information Security Program are: -***

- Information Security Policy
- Risk Assessment Policy & Procedures
- Business Continuity Plan
- Remote Access & Bring Your Own Device (BYOD) Policy
- Access Control & Password Policy
- Clear Desk & Screen Policy
- Third Party/Outsourcing Policy & Procedure
- Supplier Due Diligence Policy & Questionnaire

- Data Retention & Erasure Policy
- Data Protection Policy & Procedure
- Asset Management Policy

2 POLICY STATEMENT

Information and physical security is the protection of the information and data that the Company creates, handles and processes in terms of its confidentiality, integrity and availability from an ever-growing number and wider variety of threats, internally and externally. Information security is extremely important as an enabling mechanism for information sharing between other parties.

The Company are committed to preserving Information Security of all physical, electronic and intangible information assets across the business, including, but not limited to all operations and activities.

We aim to provide information and physical security to: -

- Protect customer, 3rd party and client data
- Preserve the integrity of The Company and our reputation
- Comply with legal, statutory, regulatory and contractual compliance
- Ensure business continuity and minimum disruption
- Minimise and mitigate against business risk

3 PURPOSE

The purpose of this document is to provide the Company's statement of intent on how it provides information security and to reassure all parties involved with the Company that their information is protected and secure from risk at all times.

The information the Company manages will be appropriately secured to protect against the consequences of breaches of confidentiality, failures of integrity, or interruptions to the availability of that information.

4 SCOPE

This policy applies to all staff within the Company *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the UK or overseas)*. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

5 OBJECTIVES

The Company have adopted the below set of principles and objectives to outline and underpin this policy and any associated information security procedures: -

- Information will be protected in line with all our data protection and security policies and the associated regulations and legislation, notably those relating to data protection, human rights and the Freedom of Information Act
- All information assets will be documented on an Information Asset Register (IAR) by the IT Manager and will be assigned a nominated owner who will be responsible for defining the appropriate uses of the asset and ensuring that appropriate security measures are in place to protect it
- All information will be classified according to an appropriate level of security and will only be made available solely to those who have a legitimate need for access and who are authorised to do so
- It is the responsibility of all individuals who have been granted access to any personal or confidential information, to handle it appropriately in accordance with its classification and the data protection principles
- Information will be protected against unauthorised access and we will use encryption methods as set out in the above objectives in this policy
- Compliance with this Information Security and associated policies will be enforced and failure to follow either this policy or its associated procedures will result in disciplinary action

The IT Manager has the overall responsibility for the governance and maintenance of this document and its associated procedures and will review this policy at least annually to ensure this it is still fit for purpose and compliant with all legal, statutory and regulatory requirements and rules. It is the sole responsibility of the IT Manager to ensure that these reviews take place and to ensure that the policy set is and remains internally consistent.

6 PROCEDURES & GUIDELINES

6.1 SECURITY CLASSIFICATION

Each information asset will be assigned a security classification by the asset owner or Information Security Officer, which will reflect the sensitivity of the asset. Classifications will be listed on the Information Asset Register.

6.2 ACCESS TO INFORMATION

Staff at The Company will only be granted access to the information that they need to fulfil their role within the organisation. Staff who have been granted access must not pass on information to others

unless they have also been granted access through appropriate authorisation. ***Refer to the Company's Access Management Policy for protocols and more information.***

6.3 Secure Disposal of Information

Care needs to be taken to ensure that information assets are disposed of safety and securely and confidential paper waste must be disposed of in accordance with relevant procedures on secure waste disposal. Where an external shredding service provider is employed, secure paper disposal bins are in each office and used in all instances of confidential paper disposal.

Electronic information must be securely erased or otherwise rendered inaccessible prior to leaving the possession of the Company, unless the disposal is undertaken under contract by an approved disposal contractor.

In cases where a storage system *(for example a computer disc)* is required to be returned to a supplier it should be securely erased before being returned unless contractual arrangements are in place with the supplier which guarantee the secure handling of the returned equipment. ***Refer to the Company's Retention Policy for protocols and more information.***

6.4 Information on Desks, Screens and Printers

Members of staff who handle confidential paper documents should take the appropriate measures to protect against unauthorised disclosure, particularly when they are away from their desks. Confidential documents should be locked away overnight, at weekends and at other unattended times.

Care should also be taken when printing confidential documents to prevent unauthorised disclosure. Computer screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons and all computers should be locked while unattended. ***Refer to our Clear Desk Policy for protocols and more information.***

6.5 Data Encryption

Encryption methods are always used to protect confidential and personal information within the Company and when transmitted across data networks. We also use encryption methods when accessing The Company network services, which requires authentication of valid credentials *(usernames and passwords)*.

Where confidential data is stored on or accessed from mobile devices *(for example, laptops, tablets, smartphones, external hard drives, USB sticks, digital recorders)* the devices themselves are to be encrypted irrespective of ownership. Where strictly confidential data is stored in public, cloud based storage facilities the data must be encrypted prior to storing to ensure that it is not possible for the cloud service provider to decrypt the data.

Where data is subject to an agreement with an external organisation, the data should be handled *(stored, transmitted or processed)* in accordance with the organisation's specified encryption requirements.

Where there is a requirement to remove or transfer personal information outside of The Company, it is always kept in an encrypted format. Encryption is used whenever appropriate on all remote access connections to the organisation's network and resources. The Company also has documented protocols for the management and use of electronic keys, with a view to controlling both the encryption and decryption of confidential and sensitive information.

All confidential and restricted information transmitted via email is encrypted. Where a secret key is provided to decrypt, this is done so in a separate format to the original email.

6.5.1 ENCRYPTION KEYS

Definitions

Encryption: This is the process of locking up (*encrypting*) information using cryptography. Such information appears illegible if access, unless a corresponding key is used to decrypt the data.

Decryption: The process of unlocking the encrypted information via a key.

The Company utilise both asymmetric and symmetric key encryption algorithms, dependant on the systems, purpose and information. The type of encryption is decided by the IT Manager after assessing the requirements of the information and transfer.

Asymmetric Key Encryption Algorithms: A type of encryption algorithm whereby two different keys are used. One key is for encrypting the information and the other for decrypting. This type is also known as public-key encryption.

Symmetric Algorithms: These are also referred to as *"secret key encryption"* and use the same key for both encryption and decryption.

6.5.2 APPROVED ENCRYPTION ALGORITHMS AND PROTOCOLS

The Company use a variety of encryption methods dependant on the nature of the information being stored or transferred, its location and its use. Below are the standard and acceptable forms of encryption used by The Company.

Symmetric Key Encryption Algorithms

- Triple Data Encryption Standard (3DES)- Minimum encryption key length of 168 bits
- Advanced Encryption Standard (AES)- Minimum encryption key length of 256 bits

Asymmetric Key Encryption Algorithms

- Digital Signature Standard (DSS)
- Elliptic Curve Digital Signature Algorithm (ECDSA)

Encryption Protocols

- IPSec *(IP Security)*
- SSL (*Secure Socket Layer)*
- SSH (*Secure Shell)*
- TLS (*Transport Layer Security) – Minimum Version TLS1.2*
- S/MIME (*Secure Multipurpose Internet Extension)*

6.5.3 KEY USE & PROTOCOLS

Encryption key management is fully automated and all private keys are kept secure, restricted and confidential. Whilst keys are in transit and/or storage, they are always encrypted.

Due to their nature, when the Company use symmetric encryption key algorithms, there is a requirement to share the secret key with the recipient. Protecting and securing the key for sharing is paramount to protecting the information the key encrypts, and so encrypting the key itself is a mandatory requirement. During distribution and transfer, the symmetric encryption keys are always encrypted using a stronger algorithm with a key of the longest key length for that algorithm.

The Company's aim when encrypting secret keys is to afford them a higher, more stringent level of protection than the encryption used to protect the data. When keys are at rest, they are again secured with encryption methods, equal to or higher than the existing encryption level.

Where asymmetric algorithms are used, the public key is passed to the certificate authority to be included in the digital certificate that will be issued to the end user. Once the digital certificate is issued, it is then made available to all relevant parties. The corresponding private key is only made available to the end user who is in receipt of the corresponding digital certificate.

6.6 REMOTE ACCESS

It is the responsibility of all the Company employees with remote access privileges to the company network, to ensure that their remote access connection is given the same consideration as the user's on-site connection to The Company. ***Refer to our Remote Access & BYOD Policy for protocols and more information.***

- Secure remote access must be strictly controlled
- Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases

- At no time, should any the Company employee provide their login or email password to anyone else
- The Company employees with remote access privileges must ensure that their The Company owned or personal computer or workstation, which is remotely connected the company network, is not connected to any other network at the same time, except for personal networks that are under the complete control of the user.
- All hosts that are connected to The Company internal networks via remote access must use the most up-to-date anti-virus software

6.7 Firewalls & Malware

The Company understands that adequate and effective firewalls, malware and protected gateways are one of the main and first lines of defence against breaches via the internet and our networks.

We utilise configured firewalls and have daily anti-virus applications running on all computers, networks and servers. The IT manager is responsible for checking the log of all scans and for keeping these applications updated and compliant.

Systems are regularly scanned and assessed for unused and outdated software with the aim of reducing potential vulnerabilities and we routinely remove such software and services from our devices where applicable.

The IT manager also has full responsibility for ensuring that the latest application and software updates and/or patches are downloaded and installed, keeping our security tools current and effective. Security software is reviewed and updated monthly, or sooner where updates or patches have been released.

7 Security Breach Management

7.1 Introduction

The Company's definition of a breach for the purposes of this and related documents, is a divergence from any standard operating procedure (SOP), which causes a failure to meet the required compliance standards as laid out by our own compliance program objectives and/or those of any regulatory body.

Compliance in this document means any area of business that is subject to rules, laws or guidelines set out by a third party which are to be followed and which, when breached, could cause emotional, reputational or financial damage to a third party.

7.2 BREACH MANAGEMENT APPROACH

The Company has robust objectives and controls in place for preventing security breaches and for managing them if they do occur. Due to the nature of our business, the Company processes and stores a vast amount of personal information and confidential client data and as such, require a structured and documented breach incident program to mitigate the impact of any breaches. Whilst we take every care with our systems, security and information, risks still exist when using technology and being reliant on human intervention, necessitating defined measures and protocols for handling any breaches.

We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary, however should there be any compliance breaches, we are fully prepared to identify, investigate manage and mitigate with immediate effect and to reduce risks and impact.

The Company have the below objectives with regards to Breach Management: -

- To maintain a robust set of compliance procedures which aim to mitigate against any risk and provide a compliant environment for trading and business activities
- To develop and implement strict compliance breach and risk assessment procedures that all staff are aware of and can follow
- To ensure that any compliance breaches are reported to the correct regulatory bodies within the timeframes as set out in their code of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Compliance Breach Incident Form for all breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To comply with regulating bodies and laws on compliance breach methods, procedures and controls
- To protect consumers, clients and staff – including their data, information and identity

Please refer to our Data Breach Policy & Procedures for further details.

8 PCI DSS COMPLIANCE

As the Company take, use or store cardholder data, we choose to comply with the industry leading Payment Card Industry Security Standards Councils regulations and guidance and take full responsibility for managing the security standards and our approach to compliance in this area. We

understand the payment card brands directly (*Visa, MasterCard etc*.) enforce compliance with the PCI Data Security Standards (PCI DSS) and remain updated with any regulations and codes of conduct as they apply to us.

The Company confirms that we are PCI compliant and have a valid certification which covers our payment system. Our staff are fully trained on the requirement under the PCI DSS and have prompt reminders on screen or in hard copy format when taking payments. Any call recordings are automatically switched off during the relay of card and/or payment information and our card processing activities and associated systems and technologies comply with the PCI-DSS standard.

8.1 DEFINITIONS

Credit Card Data - Full magnetic strip or the PAN (Primary Account Number) plus any of the following:

- Cardholder name
- Expiration date
- Service Code (CVS)

PCI-DSS - Payment Card Industry Data Security Standard

PCI Security Standards Council - The security standards council defines credentials and qualifications for assessors and vendors as well as maintaining the PCI-DSS.

Self-Assessment - The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI DSS.

PAN - Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. It is also called Account Number.

8.2 PCI DSS APPROACH & PROTOCOLS

The Company takes PCI compliance very seriously and understands our obligations to protect cardholder data. The Company aims to meet the below policy objectives, which have been created in accordance with the actual PCI standards as set out for vendors.

- Create PA-DSS compliant Payment Applications that facilitate and do not prevent our customers PCI DSS compliance
- Follow the best practices of the PCI DSS Requirements whenever we process or transmits cardholder
- Educate staff, customers, integrators, and resellers on how to install and configure the Payment Applications in a PCI DSS-compliant manner

- Ensure that our Payment Applications meet PA-DSS Requirements by successfully passing a PADSS
- Assessment as specified in PCI PA-DSS Requirements and Security Assessment Procedures
- Comply with the Vendor Release Agreement (ROV) including the adoption and implementation of Vulnerability Handling Policies consistent with industry best practices
- Create a PA-DSS Implementation Guide, specific to each application, in accordance with the requirements in the PA-DSS
- Adhere to our own defined software versioning methodology as validated and documented in the ROV1.
- Install and maintain a firewall configuration to protect data and never use vendor-supplied defaults for system passwords and other security parameters
- Protect stored data by using encryption methods, restricted access and login authentication
- Encrypt transmission of cardholder data and sensitive information across public networks
- Use and regularly update anti-virus software and develop and maintain secure systems and applications
- Restrict access to data by business need-to-know and assign a unique ID to each person with computer access
- Track and monitor all access to network resources and cardholder data and regularly test security systems and processes
- Ensure that all payments transactions are compliant and that any stored personal or card details are done so in accordance with the PCI-DSS
- Ensure that all staff are fully trained on the PCI requirements and using any PCI compliant payment software and/or systems
- Ensure that staff have regular training on PCI compliance to ensure adherence to the standards and our own business objectives
- Ensure that all customers are informed of any rights that they have under the PCI compliance standards

8.3 CARD STORAGE & DISPOSAL

The Company complies with all PCI-DSS requirements when it comes to the storage and disposal of any personal and/or card information. We ensure that each of the below objectives are achieved through our PCI, compliance, secure waste disposal, retention and information security procedures: -

- Credit card information is not entered onto or stored on any of the Company's network servers, workstations, or laptops
- Credit card information is never transmitted via email and we advise all customers and clients to adhere to this rule as well
- Web payments are always processed using a PCI-compliant service provider and credit/debit card numbers are not entered into a web page of a server hosted on our own personal network
- Electronic storage of credit/debit card data is prohibited by this policy and our Compliance Officer carries our regular and routine checks and audits to ensure that these policy objectives is not being violated
- All hard-copy, paper documents containing credit/debit card information are limited to instances specifically required by the transactions and if there is a need to retain such information, it is kept in a secure and safe location, only accessible by authorised staff.
- Where hard-copy card details have been retained, the Company follows it secure waste disposal policy and procedures for destroying the documents via approved methods once business needs no longer require retention

9 RESPONSIBILITIES

All information users within the Company are responsible for protecting and ensuring the security of the information to which they have access. Managers and staff are responsible for ensuring that all information in their direct work area is managed in conformance with this policy and any subsequent procedures or documents. Staff who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures.

The Company will ensure that staff do not attempt to gain access to information that is not necessary to hold, know or process and that restrictions and/or encryptions are in place for specific roles within the organisation relating to personal and/or sensitive information.