Information Security Policy

1. Purpose

Information security policy creates the roadmap for implementing security measures to protect Gilgamesh Financial Services and/or GFX Securities and/or the Company's most valuable assets. A strong security policy should set the security tone for the whole Gilgamesh Financial Services and/or GFX Securities and/or the Company, and let personnel know what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

---

2. Scope

This policy is applicable to all personnel with GFX INVESTMENT GROUP LIMITED, including full-time and part-time employees, temporary employees, contractors, and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

Responsibility

- Network Administrator
- System Administrator
- Process Owner
- IT Development Team
- IT Infrastructure Team

---

3. Policy Statement

GFX INVESTMENT GROUP LIMITED must follow the given policy:

- Information and IT assets must be protected against unauthorized access.
- Information is available on a strict need-to-know basis only.
- Information is not disclosed to unauthorized persons through deliberate or careless action.
- Confidentiality of information is ensured in accordance with Gilgamesh Financial Services and/or GFX Securities and/or the Company agreements and best practices.
- Information is protected from unauthorized modification.
- Applicable regulatory and legislative requirements are met.

- Disaster recovery plans for IT assets are developed, maintained, and tested as far as practicable.
- Executive has the direct responsibility for maintaining the policy and providing guidance on its implementation.
- Gilgamesh Financial Services and/or GFX Securities and/or the Company must ensure that the security policy and procedures clearly define information security responsibilities for all personnel. Assign to an individual or team the following information security management responsibilities:
    - Establish, document, and distribute security policies and procedures.
    - Monitor and analyze security alerts and information, and distribute to appropriate personnel.
    - Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
    - Administer user accounts, including additions, deletions, and modifications.
    - Monitor and control all access to data.
    - Information security training is imparted to all users upon each hiring and on an annual basis.
    - All breaches of information security, actual or suspected, are reported and investigated.
    - All Department Heads/Team Leaders are directly responsible for implementing the policy within their business areas/departments, and for adherence by their staff.
    - A culture of compliance towards information security is advocated and promoted.
    - Violations of policies are dealt with through disciplinary action.
    - Information security policy needs to be reviewed annually and is updated based on business objectives or risk environment.
    - Gilgamesh Financial Services and/or GFX Securities and/or the Company should screen all potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)

Secure Data Transmission

1. The Gilgamesh Financial Services and/or GFX Securities and/or the Company must use strong cryptography and security protocols to all locations where sensitive card data is transmitted or received over open, public networks, including the following:
    - Only trusted keys and certificates are accepted.
    - The protocol in use only supports secure versions or configurations.
    - The encryption strength is appropriate for the encryption methodology in use.
2. The Gilgamesh Financial Services and/or GFX Securities and/or the Company should ensure that all the wireless networks transmitting cardholder data, sensitive data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission. WEP must not be used for security control.
3. For TLS implementations, Gilgamesh Financial Services and/or GFX Securities and/or the Company must verify the use of TLS is enabled whenever cardholder data and sensitive data is transmitted or received.

4. The Gilgamesh Financial Services and/or GFX Securities and/or the Company should never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).
5. The Gilgamesh Financial Services and/or GFX Securities and/or the Company should ensure that security policies and operational procedures for encrypting transmissions of cardholder data and sensitive data are documented, in use, and known to all affected parties.
6. Where the covered device is reachable via web interface, web traffic must be transmitted over Secure Sockets Layer (SSL), using only strong security protocols, such as Transport Layer Security (TLS).
7. Covered data transmitted over email must be secured using cryptographically strong email encryption tools such as PGP or S/MIME.
8. Non-web transmission of covered data should be encrypted via application level encryption i.e. where the application database resides outside of the application server, the connection between the database and application should also be encrypted.
9. Where application level encryption is not available for non-web covered data traffic, implement network level encryption such as IPsec or SSH tunneling.

Following is the list of insecure services along with their alternative secure services:

Instead of…	Use…
Web Access	HTTP
File Transfer	FTP, RCP
Remote Shell	TELNET
Remote Desktop	VNC

Data Protection - Confidentiality of Data

The Company adopts measures in line with Data Protection Act in order to implement and maintain systems and procedures that are adequate to safeguard the security, integrity and confidentiality of information. The Company established security mechanisms in order to guarantee the security and authentication of the means of transfer of information, minimize the risk of data corruption and unauthorized access and to prevent information leakage, in order to maintain the confidentiality of the data at all times.

All material non-public information provided by the clients to the Company is held in confidence and is not made known to any other except as follows:

- With the express consent of the client providing such information;
- To FSC if the Company is requested or legally required to do so by the FSC;
- Pursuant to a lawful discovery requested;
- To a counterparty providing clearing services of which such client is a member or in connection with the clearing of securities;
- Subject to appropriate confidentiality requirements, to any person providing services to the Company;

- Subject to appropriate confidentiality requirements, to the Company employees, the board, board committees, attorneys, auditors and agents, independent contractors or other persons that have been engaged by the Company, in each case, who require such information in connection with the discharge of their duties to the Company; and
- All information and data obtained or received by the Company from inspections of accounting and other records will be treated as confidential by the Company.

Network Security Policy & Procedure

Overall responsibility for Network Management activity shall be assigned to the Network operations team. Responsibilities for key tasks will be assigned to one or more individuals. It shall be ensured that the use of network services is consistent with the user access management policy and the requirements of the business applications.

The network and security components used for communication and network security shall be appropriately configured, maintained and secured.

The Gilgamesh Financial Services and/or GFX Securities and/or the Company must use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.

Servers supporting critical applications shall be logically separated from other servers. The network design shall have network segregation such that, but not limited to Servers supporting critical applications shall be logically separated from other servers. All connections to the critical application servers shall route through the firewall.

The entry points to the Gilgamesh Financial Services and/or GFX Securities and/or the Company network shall be restricted and ensure that the firewalls are used to secure these entry points.

The network and security components used for communication and network security will be appropriately configured, maintained and secured.

Network components will be supported by accurate, up-to-date documentation, to ensure that the network is configured accurately and securely.

Current configuration information about network infrastructure and critical network devices like firewall and system components shall be stored locally and backed up securely at an alternate location.

IT shall be responsible to create and maintain network services agreements with external parties. Such agreements shall include but may not be limited to:

- A clear description of security features
- Service Levels
- Management requirements of all network services used
- Terms of non-disclosure of GFX INVESTMENT GROUP LIMITED information
- Adequate measures shall be taken to ensure security in all remote connections.

Data Back-Up and Recovery (Hard Copy and Electronic)

Gilgamesh Financial Services and/or GFX Securities and/or the Company maintains its electronic records on cloud service providers and trading system providers. These records consist of the firm's internal accounting records, subscription agreements, trading records, etc. If our primary site is inoperable, we will continue operations from the back-up site or an alternative location by using new devices and plugging into our online accounts with the cloud service providers.

Technology, Data and Cybersecurity

The Company will maintain certain personally identifiable information regarding clients in its electronic databases to facilitate the processing of transactions on behalf of its clients to comply with rules, regulations, and laws. The personally identifiable information stored on GFX INVESTMENT GROUP LIMITED network is protected from unauthorized access, treated as confidential, and handled according to the terms of the Gilgamesh Financial Services and/or GFX Securities and/or the Company privacy policy.

We attest that personally identifiable information and customer information stored on our systems will be protected as follows:

- Gilgamesh Financial Services and/or GFX Securities and/or the Company Internet-facing servers will be protected from access through firewalls and/or other security devices.
- The firm's critical servers will reside on isolated networks that will have no direct Internet access.
- Gilgamesh Financial Services and/or GFX Securities and/or the Company internal systems that store customer personally identifiable information will lock people out of internal systems after a few unsuccessful login attempts.
- Access to shared drives will be restricted to active employees and pre-authorized individuals on a "need to know" basis within Gilgamesh Financial Services and/or GFX Securities and/or the Company through password-protected logins to the network.

- Encryption technology will be employed for data transmissions across public networks and on portable media devices.
- System backups will reside either in secure facilities at Gilgamesh Financial Services and/or GFX Securities and/or the Company or in secure storage provided by a third party specializing in secure information management.
- All end-station computers will use state-of-the-art antivirus software that is regularly updated.
- Operating System security patches will be applied to all systems on a regular basis.
- Employees will be trained on the requirements to protect personal information.
- Systems are reasonably designed to protect personally identifiable information.

Gilgamesh Financial Services and/or GFX Securities and/or the Company further attests that should a breach occur, management will promptly take action to secure information, mitigate the breach, and notify, on a timely basis, any customers whose personally identifiable information could have been compromised.

IT Function

The relevant Department will manage IT functions in-house, whereas the Company will enter into collaboration agreements with providers to ensure the Security and Integrity of:

- The network used by the Company
- The trading platform used by the Company's personnel and clients
- The servers and personal computers of Company's personnel

In addition, the Department with necessary external support shall be responsible for ensuring that procedures are in place regarding the following issues:

- Information Technology Security
- Information Technology Backup

Continuity of IT Systems

The IT Department has established procedures to ensure that in situations of an interruption to the Company's systems (trading, telephones, etc.), the following are met:

- Preservation of essential data and functions.
- Maintenance of providing its investment services and activities.
- At least the timely recovery of such data and functions and the timely resumption of its investment services and activities.

The Company identifies specific systems that are considered core systems required for ensuring business continuity. These systems ensure: a. The continued and uninterrupted access to the internet. b. The continued and uninterrupted operation of the trading platform. c. The continued and uninterrupted operation of the digital telephone system, which shall be critical to the smooth functioning of the telephone order system. The telephone order placing system shall be an alternative/backup system to the internet-based one.

If, due to system or integration failures, the user of this document is unable to carry out any tasks, then the Company will have to be contacted immediately. If the system issue is not resolved immediately, then the author and/or the approver of this policy should also be informed without undue delay.

To reduce the impact on critical systems caused by underlying failures, the system designs these redundant systems will take into consideration methods and means to support failover to secondary systems.

In order to ensure that systems continue to operate at appropriate levels of performance, system metrics will be collected and monitored by a centralized monitoring solution. Any breach of performance thresholds will be reported to the technical service team for review with upgrades to be planned where appropriate. The Company's systems, where possible, will be hosted on cloud infrastructure allowing for the rapid increase of resources or removal of over-allocated resources to manage costs.

All major systems within the Company's computing infrastructure are backed up on a regular basis. Information Technology Services have a Backup Strategy which details the frequency of backups. It is also strongly advised that all users save their work to their network drive; this drive is backed up, and any loss or damage to files can often be rectified by the restoration of the files from an existing backup.