GS IT Security policy

GUEBSON SYSTEM LTD is responsible to ensure that all legal obligations to maintain security and confidentiality including the GDPR Regulations, and others Acts linked such: Data Protection, Human Rights, Copyright, Designs and Patents, and Computer Misuse Act are met.

The safe and effective use of End User Equipments, Information Communication Technologies (ICTs) Network connection, videoconferencing, social networking, and other media applications and services.

It is of utmost importance ensuring the security and maintenance of GUEBON SYSTEM LTD's technology platforms, including the appointments booking platform, is crucial for both internal and external operations.

GUEBSON SYSTEM LTD aims to safeguard and protect the whole Tech systems from misuse and to minimise the service disruptions by development a Security Policy and procedures to manage and enforce it,

Key purpose of the Security Policy is to ensure that:

- Proper evaluation of End User Equipment's is conducted, leading to the implementation of a robust security framework.
- Security incident detection and resolution protocols have been implemented.
- The confidentiality, integrity and availability of GUEBSON SYSTEM LTD systems are maintained
- Staff members have a clear understanding of their duties, positions, and the level of responsibility they hold while utilizing the GUEBSON SYSTEM LTD’s Platform

TECH DEPARTMENT / TEAM ROLES & RESPONSIBILITIES

It is the responsibility of the GUEBSON SYSTEM LTD IT department to ensure that all legal obligations to maintain security and confidentiality including the GDPR Regulations, and others Acts linked such: Data Protection, Human Rights, Copyright, Designs and Patents, and Computer Misuse Act are met.

Ensure all staff are instructed in their security responsibilities.

All staff, Customers and users of GS Platforms must undergo comprehensive training.

Ensure no unauthorised staff are allowed to access any GUEBSON SYSTEM LTD Platforms and End User Equipments systems.

Determine which individuals are to be given access to each level of system data based upon on a job function, role and need and independent of status.

Ensure the relevant Line managers are advised immediately about staff changes affecting computer, Shareholder, or mobile phone access what the user account may be withdrawn or deleted.

Ensure that GUEBSON SYSTEM LTD staff know how to report any Tech issues, security, incidents, malfunctions and suspected system weaknesses or threats by raising a ticket through our ITSM Tool

Be proactive in monitoring and identifying any actual or potential information security issues.

Establish protocols to reduce the risk of fraud, theft, and system disruptions. Implement, oversee, record, and disseminate information security policies and instructions.

Report to the Management Team as part of Management Review Meetings on the effectiveness of GUEBSON SYSTEM LTD IT and Security policies and procedures, key risks and mitigation.

Provide guidance on current or possible violations of confidentiality and suggest corrective measures.

Ensure GUEBSON SYSTEM LTD meets its legal responsibility under the Freedom of Information Act, advising staff on their legal responsibilities under the act and ensure a proper process exists for responding to requests of information in a timely manner.

Development and implementation of Information sharing security protocols

Ensure GUEBSON SYSTEM LTD equipment is sited or protected to reduce risks from environmental threats and hazards, and unauthorised access.

Ensure GUEBSON SYSTEM LTD equipment purchases are security labelled, appropriate licensed software loaded, and suitably configured for use prior to addition to the GUEBSON SYSTEM LTD assets list.

Allocate and configure individual user accounts and associated user authentication for each authorised user and any relevant network operating systems.

Authorise End User Equipment's disposal, delete it from the GUEBSON SYSTEM LTD asset list and ensure data storage devices are purged of sensitive data prior to secure disposal.

MEMBER / USER RESPONSIBILITIES

Each member or Staff (this includes all permanently employed, contracted, Freelancers, Customers and voluntary staff members) and any other authorised users share a responsibility to maintain the security of GUEBSON SYSTEM LTD information and systems and these are listed below;

It is the responsibility of every user to make sure that their actions do not lead to any breaches in IT security.

- It is imperative to adhere to the applicable security and confidentiality policies and procedures set forth by GUEBSON SYSTEM LTD.
- Please be aware that violations of policy will be thoroughly investigated through a formal disciplinary process, which could result in termination of employment and/or legal action.
- Is personally responsible for the accuracy and currency of the data they record on the platforms or systems.
- Must not disclose their passwords or allow anyone else to use their password or allow another user to work under their log on.
- Any potential conflicts of interest must be disclosed.
- Must report any software or system malfunctions that it is believed could lead to a security incident to the IT department immediately.
- Must report suspected security weaknesses or threats to the IT department.
- All staff members, freelancers and relevant third-party users are required to undergo suitable training and receive periodic updates on the policies and procedures.
- Authorised users of GUEBSON SYSTEM LTD shall receive appropriate system and platform training or guidance before authorisation is granted.
- Violations of this policy and associated procedures shall be dealt with through a formal disciplinary process and / or legal action.

ACCESS AND PRIVILEGES

Formal procedures will be used to control access to systems.

The IT department will approve, assign equipment, software or application for access and access privileges will be modified or removed, as appropriate, when an individual changes job or leaves.

Access to systems will be based upon the staff member’s job role and relevant task requirements.

No individual will be given access to a live system unless properly trained and made aware of his or her security responsibilities.

Passwords are required which should be at least eight characters long and a mix of alphanumeric characters with sufficient complexity of structure to reflect the confidentiality of data held on GUEBSON SYSTEM LTD.

Users must keep their passwords secret, never disclose them to colleagues, and if requested to do so report that incident to their Line Manager.

Passwords should be changed at least every 90 days.

END USER EQUIPMENT PROTECTION

GUEBSON SYSTEM LTD equipment will always be installed and sited in accordance with the manufacturer’s specification and with due consideration of Health and Safety legislation.

Equipment will be strategically placed to mitigate the potential hazards posed by environmental factors and unauthorized entry. In instances where the equipment needs to be located in public spaces, it will be positioned in a manner that minimizes the risk of unauthorized access or inadvertent viewing.

Measures will be implemented to safeguard essential equipment through environmental controls.

Such controls will trigger alarms if environmental problems occur, In such cases only authorised entry will be permitted.

Proper maintenance agreements or arrangements will cover all central processing equipment, such as DB’s or file servers.

Records of all faults/suspected faults will be maintained by the IT department supported by the administration support team.

Any supplier requiring remote access to resolve system issues will be required to provide a written commitment to maintain confidentiality of data and information and only use qualified representatives.

Each request for share folders or remote access will be authorised by the IT department.

DATA SECURITY OFF PREMISES

It is important to be aware that hard drives in any device and removable storage devices used for data backup could potentially store sensitive or confidential information. Taking these disks or storage media off site poses a risk to the security of this data.

Other than to transport it for a legitimate purpose, equipment and data will not be taken off site without approval of the appropriate line manager and IT department, Portable computing devices must be provided with encryption and should not be left unattended.

To preserve the integrity of data, frequent synchronisations should be made with system server computers.

They should be maintained regularly, batteries kept charged to preserve their availability, and anti-virus software updated appropriately

HARDWARE AND EQUIPMENT DISPOSAL

End User Equipments or other company devices disposal can only be authorised by the GUEBSON SYSTEM LTD IT department who will ensure that data storage devices are irreversibly purged of sensitive data before disposal, or they are securely destroyed.

The procedures for disposal will be documented, Unusable devices must also be securely destroyed.

APPLICATION / SOFTWARE LICENSE

GUEBSON SYSTEM LTD only permit approved software to be installed on its devices.

- Users must not download or upload unauthorised software.
- No removal storage devices, from whatever source are to be loaded unless they have been virus checked and approved by the IT department.
- Users should report any viruses detected/suspected on their machines immediately to the IT department.
- It is a criminal offence to make or use unauthorised copies of commercial software and offenders are liable to disciplinary action and civil or criminal prosecution.

DATA BACKUP / RECOVERY

Daily backup routines are implemented for all central systems.

- The backups are stored in a secure location that is physically separate from the system's premises, ensuring protection against any potential loss of the building.
- The viability of central systems backups is tested when used in contingency tests.
- All users must use the internal networks or VPN for any project documentation to ensure that back up of all key documents is maintained.

NETWORK & INTERNET USAGE

Internet usage during working hours is permitted solely for conducting official business of the Company, however it is important to acknowledge that utilizing the Internet carries the risk of compromising the security of sensitive Company data and exposing our system to potential viruses or spyware.

Such vulnerabilities may grant unauthorized individuals external to the Company access to confidential information.

Removing such programs from the Company network requires investment of time and resources that is better devoted to progress.

For this reason, and to assure the use of work time appropriately for work, we ask staff members to limit Internet only for business use.

Additionally, it is strictly prohibited to utilize Company computers or any other equipment to access, view, or visit any pornographic or inappropriate websites, as well as any sites that are unethical, immoral, or unrelated to business activities. Violation of this policy may result in disciplinary measures, including possible termination of employment.

Limited, responsible use of Internet access during non-working hours such as a lunch break is acceptable however the use of social networking sites such as Facebook which may introduce unsafe access to the GEBSON SYSTEM LTD End user Equipements and network will constitute a serious breach of internet policy and will not be tolerated at any time.

EMAIL & COMMUNICATION

Email Usage is strictly limited to Company business purposes.

Company data and information must not be shared outside of the Company without authorisation at any time.

Viewing pornography or sending pornographic jokes or stories via email constitutes sexual harassment and will be treated as a disciplinary offence, as will any emails that discriminate against employees based on any protected classification, such as race, gender, nationality, religion, and others.

You are also not permitted to conduct personal business using the Company computer or email. Please keep this in mind as you consider forwarding non-business emails to colleagues, family, and friends.

Non-business-related emails waste company time and attention.

Sending or forwarding non-business emails could result in disciplinary action that may lead to employment termination.

E-mail and Internet usage assigned to an employee's computer are solely for the purpose of conducting Company business use.

Keep in mind that the Company owns any communication or information sent via email or that is stored on company equipment.

IT Team & Management and other authorized staff have the right to access any material in your email or on your computer at any time. Please do not consider your electronic communication, storage or access to be private if it is created or stored at work.

SECURITY INCIDENTS MANAGEMENT

A security incident is an event that can result in:

- Degraded system integrity.
- Loss of service platform availability.
- Disclosure/loss or corruption of confidential information.
- Disruption of activity.
- Financial loss.
- Legal action.
- Unauthorised access to Platform, and applications.
- Misuse of software or access privileges

All security incidents must be reported to the IT Department immediately who will decide the most appropriate action to resolve or minimise impact on data or systems. The incident will be further reported to the Senior Management Team who will take advice from the IT manager as to any further actions.

Any security incidents will be formally logged via our ITSM Tool, categorised by severity and the resultant actions recorded.

Any major security incident will be immediately referred to the Senior Management Team for investigation.

- The management and implementation of all IT and Security systems are subject to periodic review by both internal and external auditors as part of our Quality Management System.

This policy will be brought to the attention of all users and monitored in line with normal assurance processes.

This policy will be reviewed each 6-month / year to ensure its continued suitability