GATHERACT SECURITY POLICY

Information is a critical company asset. Information is comparable with other assets in that there is a cost in obtaining it and a value in using it. However, unlike many other assets, the value of reliable and accurate information appreciates over time as opposed to depreciating. Shared information is a powerful tool and loss, or misuse can be costly, if not illegal. The intent of this Security policy is to protect the information assets of the organization.

In addition, in this policy, the main objective followed by **GATHERACT**, is to establish and maintain adequate and effective security measures for users, to ensure that the confidentiality, integrity and operational availability of information is not compromised.

Sensitive information must therefore be protected from unauthorized disclosure, modification, access, use, destruction or delay in service.

Each user has a duty and responsibility to comply with the information protection policies and procedures described in this document.

1. **PURPOSE**

The purpose of this policy is to safeguard information belonging to **GATHERACT** within a secure environment.

This policy informs **GATHERACT** staff and other persons authorized to use **GATHERACT** facilities of the principles governing the retention, use and disposal of information.

2. **SCOPE**

This policy applies to all employees of **GATHERACT** who use computer systems or work with documents or information that concerns customers, suppliers or any other partner for whom the organization has collected information in the normal course of its business.

3. **GOALS AND OBJECTIVES FOLLOWED**

The goals and objectives followed of this policy are:

- Protect information from unauthorized access or misuse;
- Ensure the confidentiality of information;
- Maintain the integrity of information;
- Maintain the availability of information systems and information for service delivery;
- Comply with regulatory, contractual and legal requirements;
- Maintain physical, logical, environmental and communications security;
- Dispose of information in an appropriate and secure manner when it is no longer in use;

4. **AUTHORIZED USERS OF INFORMATION SYSTEMS**

All users of **GATHERACT**'s information systems must be formally authorized by the company's IT department. Authorized users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person.

Authorized users shall take all necessary precautions to protect the **GATHERACT** information in their personal possession. Confidential, personal or private information must not be copied or transported without consideration of:

- the permission of the owner of the information;
- the risks associated with loss or falling into the wrong hands;
- how the information will be secured during transport to its destination.

5. **ACCEPTABLE USE OF INFORMATION SYSTEMS**

User accounts on the company's computer systems must only be used for the company's business and must not be used for personal activities during working hours.

During breaks or mealtimes, limited personal use is permitted, but use must be legal, honest and decent while considering the rights and sensitivities of others.

- Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to company systems for which they do not have authorization.
- Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the employees' manager and/or the company IT designee. Users shall not download unauthorized software from the Internet onto their PCs or workstations.

Unauthorized use of the system may constitute a violation of the law, theft and may be punishable by law. Therefore, unauthorized use of the company's computer system and facilities may constitute grounds for civil or criminal prosecution.

6. **ACCESS CONTROL**

The fundamental element of this security policy is the control of access to critical information resources that require protection against unauthorized disclosure or modification.

Access control refers to the permissions assigned to persons or systems that are authorized to access specific resources. Access controls exist at different layers of the system, including the network. Access control is implemented by username and password. At the application and database level, other access control methods can be implemented to further restrict access.

Finally, application and database systems can limit the number of applications and databases available to users based on their job requirements.

7. **NORMAL USER IDENTIFICATION**

All users must have a unique username and password to access the systems. The user's password must remain confidential and under no circumstances should it be shared with management and supervisory staff and/or any other employees. Also, all users must comply with the following rules regarding password creation and maintenance:

- Password must not be found in any English or foreign dictionary. This means, do not use a common noun, noun, verb, adverb or adjective. These can be easily cracked using standard "hacking tools";

- Passwords should not be displayed on or near computer terminals or be easily accessible in the terminal area;

- User accounts will be frozen after 3 failed logon attempts;

- Logon IDs and passwords will be suspended after 31 of days without use.

Below, you will find some additional important points to remember:

- Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

- Users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account.

- Employee Logon IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the company office.

- Employees who forget their password must call the IT department to get a new password assigned to their account. The employee must identify himself/herself by (e.g. employee number) to the IT department.

- Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee’s password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

8. **CONFIDENTIALITY OF INFORMATION**

Any information or documents that are not to be made public are designated as "Confidential Information". This information is invaluable to the company and therefore, all employees who, in the course of their duties, handle this type of information are expected to behave as follows:

- All confidential documents should be stored in locked file cabinets or rooms accessible only to those who have a business “need-to-know.”

- All electronic confidential information should be protected via firewalls, encryption and passwords.

- Employees should clear their desks of any confidential information before going home at the end of the day.

- Employees should refrain from leaving confidential information visible on their computer monitors when they leave their workstations.

- All confidential information, whether contained on written documents or electronically, should be marked as “confidential.”

- All confidential information should be disposed of properly (e.g., employees should not print out a confidential document and then throw it away without shredding it first.)

- Employees should refrain from discussing confidential information in public places.

- Employees should avoid using e-mail to transmit certain sensitive or controversial information.
- Limit the acquisition of confidential client data (e.g., social security numbers, bank accounts, or driver’s license numbers) unless it is integral to the business transaction and restrict access on a “need-to-know’ basis.
- Before disposing of an old computer, use software programs to wipe out the data contained on the computer or have the hard drive destroyed.

9. SECURITY OF INFORMATION

Information stored on computer systems must be regularly backed-up so that it can be restored if or when necessary.

All care and responsibility must be taken in the destruction of sensitive information. Electronic information relating to customers, administrative and commercial information must be disposed of in a secure manner.

Sensitive or confidential paper documents must be placed in the shredding bins or destroyed in the manner indicated to you by your department head.

10. USER RESPONSIBILITIES

Any security system relies on the users of the system to follow the procedures necessary for upholding security policies. Users are required to report any weaknesses in the company computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

Employees are therefore expected to:

- Complies with security procedures and policies;
- Protects their user ID and passwords;
- Inform the IT department of any security questions, issues, problems or concerns;
- Assists the IT department in solving security problems;
- Ensures that all IT systems supporting tasks are backed up in a manner that mitigates both the risk of loss and the costs of recovery;
- Be aware of the vulnerabilities of remote access and their obligation to report intrusions, misuse or abuse to the IT department;
- Be aware of their obligations in the event that they store, secure, transmit and dispose of vital information concerning the activities or operations of the company, customers, partners or strategic information on the company's products and services

11. MONITORING OF THE COMPUTER SYSTEM

The company has the right and capability to monitor electronic information created and/or communicated by persons using company computer systems and networks, including e-mail messages and usage of the Internet. It is not the company policy or intent to continuously monitor all computer usage by employees or other users of the company computer systems and network.

However, users of the systems should be aware that the company may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with company policy.

12. **SYSTEM ADMINISTRATOR**

System administrators, network administrators and security administrators will have access to the host systems, routers, hubs and firewalls necessary to perform their tasks.

All system administrator passwords will be deleted immediately after an employee who has access to these passwords has been terminated, dismissed or otherwise left the company's employment.

13. **MANAGERS DUTY**

Supervisors / Managers shall immediately and directly contact the company IT Manager to report change in employee status that requires terminating or modifying employee logon access privileges.

14. **EMPLOYEE AGREEMENT ON SECURITY POLICY**

I acknowledge that I have received a copy of the **GATHERACT** Security policy. I have read and understand the policy. I understand that, if I violate the policy, I may be subject to disciplinary action, including termination. I further understand that I will contact my supervisor if I have any questions about any aspect of the policy.

Dated: ____________________________

EMPLOYEE COMPANY

____ _________________
____

Authorized Signature Authorized Signature

____ __________________________________

Print Name and Title Print Name and Title