IT SECURITY POLICY

This IT Security Policy outlines behaviors expected of employees when dealing with IT. This IT policy, is to establish and maintain adequate and effective IT security measures for our Customer's Data, to ensure that the confidentiality, integrity and operational availability of information is not compromised.

This Policy is to ensure that organizational IT systems are not open to abuse, the Company reserves the right to monitor individual staff usage but only where authorized by senior HR staff and where, in the circumstances, it is fair and appropriate to do so. A range of monitoring activities needs to be established to ensure that the IT systems are operating efficiently and effectively. This includes the monitoring of information entering, leaving, or stored on organizational IT systems. Such monitoring is not, in general, person-specific, but the employee's personal data may be accessed as part of this policy.

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

Each agent/employee/member has a duty and responsibility to comply with the information protection policies and procedures described in this document as well as treat the Customer Data with the utmost integrity at all times.

1. PURPOSE

The purpose of this policy is to safeguard Customer Data and Information, within a secure environment.

This policy informs staff and other persons authorized to use facilities of the principles governing the retention, use and disposal of a Customer's Data and Information.

2. SCOPE

This policy applies to all Agents/employees who use computer systems toaccess a Client's Data environment or work with data, documents or information that concerns Clients in any shape or form. Computing resources include all Company owned, licensed, or managed hardware and software, and use of the Company network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network

3. GOALS AND OBJECTIVES FOLLOWED

The goals and objectives followed of this policy are:

- Protect information from unauthorized access or misuse; only Agents directly overseeing a project or a client's environment may hold the passwords to such environments. Passwords or any other entry-gate to a Clients environment may not be shared amongst other agents; the transfer of any passwords or entry-gate information to a Client's environment must be approved and signed off by the Company before such changes can be made; sharing of passwords or any entry—gate information to a Client's environment to a 3rd party is by no means allowed.

- Ensure the confidentiality of information; Sharing of any Client Data to a 3rd party or outside of the organization, is by no means allowed, unless;

- The client has advised, in writing that the information in question may be sharedas part of a project or agreement in order to reach a common goal.

- Ensures that only authorized users can access objects on the system.

- Authentication assurance or verification that the resource (human or machine) at the other end of the session really is what it claims to be. Solid authentication defends a system against the security risk of impersonation, in which a sender or receiver uses a false identity to access a system.

- Ensuring stronger authentication methods than traditional user name and password logon procedures provide. Authenticated users might have different types of permissions based on their authorization levels

- Authorization assurance that the person or computer at the other end of the session has permission to carry out the request. Authorization is the process of determining who or what can access system resources or perform certain activities on a system. Typically, authorization is performed in context of authentication.

- Integrity assurance that arriving information is the same as what was sent out. Confidentiality

- Comply with regulatory, contractual and legal requirements;

4. ACCEPTABLE USE OF INFORMATION SYSTEMS

User accounts on the company's computer systems must only be used for the company's business and to render the service to a Customer which is agreed upon. This includes any work been administered for a Customer which falls in the after-hours category.

- Employees may use only the computers, computer accounts, and computer files for which they have authorization.
- Employees may not use another individual's account, or attempt to capture or guess other users' passwords.
- Employees are individually responsible for appropriate use of all resources assigned to them, including the computer, the network address or port, software and hardware. Therefore, employees are accountable to the Company for all use of such resources.
- You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access. You must configure hardware and software in a way that reasonably prevents unauthorized users from accessing the Companys network and computing resources.
- Employees must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator
- Unauthorized use of the system which poses a threat to a Clients Data and / or Environment,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.

5. UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee authorized to engage in any activity that is illegal while utilizing Company owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

- System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Company.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Company or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting the Company business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a Company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any Company account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

12. Circumventing user authentication or security of any host, network or account.

13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

15. Providing information about, or lists of, Company employees to parties outside the Company

- Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. ACCESS CONTROL

The fundamental element of this IT 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 and level of skill which can potentially negatively impact a Customer’s Environment.

7. NORMAL USER IDENTIFICATION

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

- Passwords must not be found in any English or foreign dictionary. This means, do not use a common noun, verb, adverb or adjective. These can be easily deciphered using standard "hacking tools";
- Passwords should not be displayed on or near computer terminals or be easily accessible in the terminal area;
- passwords must be protected from unauthorized disclosure and modification when stored and transmitted;
- The Company will enforces password minimum and maximum lifetime restrictions

Some Rules when choosing a password

- Use both uppercase and lowercase letters if the computer system considers an uppercase letter to be different from a lowercase letter when the password is entered.
- Include digits and punctuation characters as well as letters. • Choose something easily remembered so it doesn't have to be written down.
- Use at least eight characters with a combination of numeric, alpha and special characters.
- It should be easy to type quickly so someone watching the keyboard cannot follow what is typed.
- Use two short words and combine them with a special character or a number, like robot4me or eye-con2.
- Put together an acronym that has special meaning to you. • End of one word is the beginning of another word.

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

- Users are not allowed to access password files on any network infrastructure components and where this level of access is not needed. 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

ofaccess to production systems must request a Special Access account.

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

- Employees will be responsible for all transactions occurring during Logon sessions initiatedby use of the Employee's password and ID. Agents 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 Customer Data and Information or Documents are not to be made public and are deemed anddesignated as "Confidential Information". This information is invaluable and therefore, all Agents who, in the course of their duties, handle this type of information areexpected to behave as follows:

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

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

- Employees should refrain from leaving confidential information visible on their computermonitors.

- 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.,Employee 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 forum, including their place of residence.

- 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;

Any Data or Hardware that is been disposed of; the Company must have writtenconsent from the Customer as well as provide proof the destruction to the Customer in good faith.

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 data security system relies on the users of the system to follow the procedures necessary for upholding data 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.

Agents are therefore expected to:

- Comply with data security procedures and policies;
- Protect their user ID and passwords;
- Inform the Head of ICT department of any data security questions, issues, problems or concerns;

- Ensures that all IT systems supporting tasks are backed up in a manner that mitigates boththe 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 Company;

- Be aware of their obligations if 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 Agents 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 dayaccess), and Agents' electronic files and messages to the extent necessary to ensure that theInternet and other electronic communications are being used in compliance with the law and withcompany policy.

Systems shall be monitored to ensure all information security events are recorded. The organization shall comply with all relevant legal requirements applicable to the monitoring and logging activities. System monitoring shall be used as a means to check the effectiveness of controls adopted and also to verify the conformance to the organizational access control and acceptable use policies. System monitoring shall consider the following aspects:

- compliance with regulatory and statutory obligations;
- effective maintenance of IT systems;
- prevention or detection of unauthorized use of, or other threats to the organizational IT systems, or criminal activities;
- compliance with organizational policies and procedures; and
- review of usage and staff training.

12. SYSTEM ADMINISTRATOR

System administrators, network administrators and data 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.