## Cyber – Information Security

1. **Purpose**

The purpose of the Cyber – Information Security policy is to inform company users, supervisors, employees, contractors, and other authorized users of their obligatory requirements for protecting the technology and information assets of the company. The Cyber - Information Security Policy describes the technology and information assets that shall be protected and identifies many of the threats to those assets.

1. **Responsibilities**

It is the obligation of all users of the company systems to protect the technology and information assets of the company. This information must be protected from unauthorized access, theft, and destruction. The technology and information assets of the company are made up of the following components:

* Computer hardware, CPU, disc, email, web, application servers, PC systems, application software, system software, etc.
* System software including operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
* Application software: This may include custom written software applications, and commercial off the shelf software packages.
* Communications network hardware and software including routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

1. **Employee Threats to Cyber Security**

To mitigate threats to information security

* Only give out appropriate rights to systems. Limit access to only business hours.
* Do not share accounts or to access systems.
* Never share your login information with anyone.
* When employees are separated or disciplined, they shall have their access to systems and websites removed
* Keep detailed system logs on all computer activity.
* Physically secure computer assets, so that only staff with appropriate need can access.

1. **Usage Policy**

The usage policy for the computer systems, networks and information resources pertains to all employees and contractors who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for the business purposes of the company.

* User accounts on company computer systems are to be used only for business of the company and not to be used for personal activities. Unauthorized use of the system may be in violation of the law, constitutes theft and can be punishable by law. Therefore, unauthorized use of the company computing system and facilities may constitute grounds for either civil or criminal prosecution.
* Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Users are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of the company.
* 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.
* Users shall not download unauthorized software from the Internet onto their PCs or workstations.
* 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.

1. **Use of the Internet**

* The company will provide internet access to employees and contractors who are connected to the internal network and who has a business need for this access.
  + Employees and contractors must obtain permission from their supervisor and file a request with the Security Administrator.
* The internet is a business tool for the company. The internet is to be used for business-related purposes such as: communicating via electronic mail with suppliers and business partners, obtaining useful business information and relevant technical and business topics.
* The internet service may not be used for transmitting, retrieving, or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature for “chain letters” or any other purpose which is illegal or for personal gain.

1. **User System and Network Access – User Identification**

All users are expected to have knowledge of these security policies and are required to report violations to the Security Administrator.

All users will be required to have a unique logon ID and password for access to systems. The user’s password should be kept confidential and MUST NOT be shared with management and supervisory personnel and/or any other employee whatsoever. More complex passwords make it more difficult for a password to be guessed or forced. All users shall comply with the following rules regarding the creation and maintenance of passwords:

* Password must not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective.
* Passwords shall include at least one capitalized letter, a number or punctuation mark, and be at least 8 characters in length.
* Passwords shall not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
* Password must be changed every (180 of days).
* User accounts will be frozen after (30 of days) failed logon attempts.
* Logon IDs and passwords will be suspended after (60 of days) days without use.

Standard Users:

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 as outlined elsewhere in this document.

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.

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.

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.

System Administrator Access Users:

System Administrators, network administrators, and security administrators will have (type of access) access to host systems, routers, hubs, and firewalls as required to fulfill the duties of their job.

All system administrator passwords will be DELETED immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of the company.

Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by the company and require the permission of the user’s company IT Manager. Monitoring of the special access accounts is done by entering the users into a specific area and periodically generating reports to management. The reports will show who currently has a special access account, for what reason, and when it will expire. Special accounts will expire in 30 days and will not be automatically renewed without written permission.

Third Party Users:

“Third-party” refers to vendors, consultants and business partners doing business with company, and other partners that have a need to exchange information with the company. Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of the company. The third-party company will ensure that only authorized users will be allowed to access information on the company network. The third-party will not allow Internet traffic or other private network traffic to flow into the network. A third-party network connection is defined as one of the following connectivity options:

A network connection will terminate on a to-be-specified-date and the third-party will be subject to standard company authentication rules.

All requests for third-party connections must be made by submitting a written request and be approved by the company. Only authorized devices may be connected to the company network(s). Authorized devices include PCs and workstations owned by company that comply with the configuration guidelines of the company. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach to the network: non-company computers that are not authorized, owned and/or controlled by company.

Only authorized persons may remotely access the company network. Remote access is provided to those employees, contractors and business partners of the company that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to company network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.

1. **Types of Access to Computer Systems**

A fundamental component of our Cyber - Information Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

* Externally accessible to public. The system may be accessed via the Internet by persons outside of the company without a logon id or password. The system may be accessed via dial-up connection without providing a logon id or password. It is possible to “ping” the system from the Internet. The system may or may not be behind a firewall. A public Web Server is an example of this type of system.
* Non-Public, Externally accessible. Users of the system must have a valid logon id and password. The system must have at least one level of firewall protection between its network and the Internet. The system may be accessed via the Internet or the private Intranet. A private FTP server used to exchange files with business partners is an example of this type of system.
* Internally accessible only. Users of the system must have a valid logon id and password. The system must have at least two levels of firewall protection between its network and the Internet. The system is not visible to Internet users. It may have a private Internet (non-translated) address and it does not respond to a “ping” from the Internet. A private intranet Web Server is an example of this type of system.

1. **Training**

Employees who have even remote access to any company computers shall be trained in Cyber - Information Security as part as initial training, and then refresher training annually thereafter. Training shall be on types of access, types of threats, user responsibilities, acceptable use, user system, and network access, incident notification and management.

In addition, the following areas must be covered in the training program:

* Phishing attacks
* Removable media
* Passwords and Authentication
* Physical security
* Mobile Device Security
* Working Remotely
* Public Wi-Fi
* Cloud Security
* Social Media Use
* Internet and Email Use
* Social Engineering
* Security at Home

1. **Monitoring Use of Computer Systems**

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.

1. **Security Incident Handling Procedures**

The term “security incident” is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the company network. Some examples of security incidents are:

* Illegal access of a company computer system. For example, a hacker logs onto a production server and copies the password file.
* Damage to a company computer system or network caused by illegal access. Releasing a virus or worm would be an example.
* Denial of service attack against a company web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
* Malicious use of system resources to launch an attack against other computer outside of the company network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their supervisor immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem. The Company will investigate with the IT employee(s) or third party IT contractor for lesson learned to prevent future incidents.