POLICY ON CYBER SECURITY & CYBER RESILIENCE

2nd Floor, Thottathil Towers, Market Road, Cochin - 682 018.

Reviewed By:

Mr. George Mampilly, Executive Director & CFO

On 01-11-2019

POLICY NO. 15

CYBER SECURITY AND CYBER RESILIENCE POLICIES

INTRODUCTION

This Cyber Security Policy is a formal set of rules by which those people who are given access to company technology and information assets must abide. The Cyber Security Policy serves several purposes. The main purpose is to inform company users: employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the company. The Cyber Security Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets. The Cyber Security Policy also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy answers these questions, describes user limitations and informs users there will be penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of the company computer systems and network.

WHAT ARE WE PROTECTING

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: used by the various departments within the Company. This includes 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.

CLASSIFICATION OF INFORMATION

User information found in computer system files and databases shall be classified as either confidential or non-confidential. The Company shall classify the information controlled by them. Senior manager is required to review and approve the classification of the information and determine the appropriate level of security to best protect it.

CLASSIFICATION OF COMPUTER SYSTEMS

Security Level	Description	Example
RED	This system contains confidential information – information that cannot be revealed to personnel outside of the Company. Even within the Company, access to this information is provided on a "need to know" basis. The system provides mission- critical services vital to the operation of the business. Failure of this system may have life threatening consequences and/or an adverse financial impact on the business of the Company.	Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information.
GREEN	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access Server and application(s). Management workstations used by systems and network administrators.

WHITE	This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	A test system used by system designers and programmers to develop new computer systems.
BLACK	This system is externally accessible. It is isolated from RED or GREEN systems by a firewall. While it performs important services, it does not contain confidential information.	A public Web server with non- sensitive information.

LOCAL AREA NETWORK (LAN) CLASSIFICATIONS

A LAN will be classified by the systems directly connected to it. For example, if a LAN contains just one RED system and all network users will be subject to the same restrictions as RED systems users. A LAN will assume the Security Classification of the highest-level systems attached to it.

DEFINITIONS

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.Thesystemmusthaveatleastonelevelоffirewallprotectionbetweenitsnetworkand 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.

Chief Information Officer. The Senior employee of Information Technology (IT) shall serve as the Chief Information Officer.

Security Administrator. An employee of IT shall be designated as the Security Administrator for the Company.

THREATS TO SECURITY

EMPLOYEES

One of the biggest security threats is employees. They may do damage to your systems either through incompetence or on purpose. You must layer your security to compensate for that as well. You mitigate this by doing the following.

- ✓ Only give out appropriate rights to systems. Limit access to only business hours.
- ✓ Don't share accounts to access systems. Never share your login information with co- workers.
- ✓ When employees are separated or disciplined, you remove or limit access to systems.
- ✓ Advanced – Keep detailed system logs on all computer activity.
- ✓ Physically secure computer assets, so that only staff with appropriate need can access.

AMATEUR HACKERS AND VANDALS.

These people are the most common type of attackers on the internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. There are usually crimes of opportunity. These amateur hackers are scanning the internet and looking for well known security holes that has not been plugged. Web servers and electronic mail are their favorite targets. Once they find a weakness they will exploit it to plant viruses, Trojan horses, or use the resources of your system for their own means. if they do not find an obvious weakness they are likely to move on to an easier target.

CRIMINAL HACKERS AND SABOTEURS.

The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

USER RESPONSIBILITIES

This section establishes usage policy for the computer systems, networks and information resources of the office. It 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.

ACCEPTABLE USE

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. Furthermore, they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside 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 and/or the Company IT designee.

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.

USER CLASSIFICATION

All users are expected to have knowledge of these security policies and are required to report violations to the Security Administrator. Furthermore, all users must conform to the Acceptable Use Policy defined in this document. The Company has established the following user groups and defined the access privileges and responsibilities:

User Category	**Privileges & Responsibilities**
Department Users (Employees)	Access to application and databases as required for job function. (RED and/or GREEN cleared)
System Administrators	Access to computer systems, routers, hubs, and other infrastructure technology required for job function. Access to confidential information on a "need to know" basis only.

Security Administrator	Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function.
Systems Analyst/Programmer	Access to applications and databases as required for specific job function. Not authorized to access routers, firewalls, or other network devices.
Contractors/Consultants	Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function. Knowledge of security policies. Access to Company information and systems must be approved in writing by the Company director/CEO.
Other Agencies and Business Partners	Access allowed to selected applications only when contract or inter-agency access agreement is in place or required by applicable laws.
General Public	Access is limited to applications running on public Web servers. The public will not be allowed to access confidential information.

CONNECTING TO THIRD-PARTY NETWORKS

This policy is established to ensure a secure method of connectivity provided between the Company and all third-part companies and other entities required to electronically exchange information with Company.

“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.

This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

All requests for third-party connections must be made by submitting a written request and be approved by the Company.

CONNECTING DEVICES TO THE NETWORK

Only authorized devices may be connected to the Company network(s). Authorized devices includePCsandworkstationsownedbycompanythatcomplywiththeconfigurationguidelinesof 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.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. thumb drives and writable CD's.

REMOTE ACCESS

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.

UNAUTHORIZED REMOTE ACCESS

The attachment to a user's PC or workstation that is connected to the Company LAN is not allowed without permission IT department. Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

PENALTY FOR SECURITY VIOLATION

The company takes the issue of security seriously. Those people who use the technology and information resources of Company must be aware that they can be disciplined if they violate this policy. **Upon violation of this policy, an employee of company may be subject to discipline up to and including discharge.** The specific discipline imposed will be determined by a case-by- case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information. Discipline which may be taken against an employee shall be administrated in accordance with any appropriate rules or policies and the Company Policy Manual.

In a case where the accused person is not an employee of Company the matter shall be submitted to the CAO. The CAO may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

SECURITY INCIDENT HANDLING PROCEDURES

This section provides some policy guidelines and procedures for handling security incidents. 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 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 manager 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.