**Physical Control Policy**

**Overview**

Physical Control Policy is placed to secure the physical environment access at HiQuSystems for employees and visitors. The policy ensures the safety of the company hardware, computers, laptops, printers, server rooms, networks, printed materials, company’s financial files and other relevant material deemed necessary for smooth operations of the company.

The policy ensure that each employee is well equipped with required hardware and access to resources required to perform his/her daily tasks effectively and efficiently.

The policy is devised to control theft, loss of company’s intellectual property and financial records at all time. Yet it enables to employees to perform their duties.

**Policy**

**Server room**

The server room is out of bound for all resources except for Network administrator(NA)/GM Development/GM. The server room must be locked all time. The NA will require to visit server room to remove fault on need basis. Such visit is logged in Server Room Access register with date, time, reason, resolution and duration of visit.

Any faulty hardware must be replaced immediately for which NA will raise a request and new hardware will be purchase as per Purchase Policy.

**Access to office**

Access to office is limited to only HiQuSystems employees using biometric access control situated at the main door. Each employee is provided with office key incase biometric system is out of order or management decided to not to use the biometric system in situation like COVID-19.

Its responsibility of the last person to make sure office lights are properly switched off, all windows are closed and office main door is properly locked.

All visitors must follow the Visitor Log Policy to enter HiQuSystems premises.

**New resource joining**

Upon arrival of new resources, he/she is been issue with HiQuSystesm access card bearing employees picture with name, employment date, and company address with in two working days. This card must be present all the time with an employee and can be checked at the building entrance.

The resource is assigned a work station with all the essentials to perform daily task. The laptop/desktop is assigned to user and Asset Possession form is filed and signed by employee. Then it is employees is responsibility to make sure to keep the hardware in working condition and refrain for physical abuse. The login id/password is created for local network by Network Administrator which is shared with resource and GM.

The resource is required to follow the Clean Desk Policy for security and control.

The laptop is provided to resource for office work and in situation like COVID-19 to work from home. Work from home is allowed in any other situation with prior approval of manager/GM for which an email must be sent to concerned staff.

Any other hardware required to work from home is conditional and resource must take the responsibility of safety and return of the hardware intact. The Asset Possession form is required to be signed by manager/GM.

**Fire extinguisher**

The proper fire extinguishers must be placed at location which is easily accessible in case of fire. The fire extinguishers must conform to the required standards for wood, foam, and computer/laptop materials.

**Power circuit breaker**

Power circuit breaker is located at a place which is easily accessible and all staff must be made aware to switch of main circuit breaker in case of fire or other emergencies.