CYBERSECURITY

Doc. Type:	**Program**	Effective Date:	**12/1/2020**
Section:	**70**	Revision	**01**
Status:	**Issued**	Last Revised:	**12/1/2020**

1. BACKGROUND

a. H2 Enterprises is committed to providing computing, telecommunications, networking infrastructure and audio-visual support across the organization.

b. H2 Enterprises reserves the right, without prior notice, to monitor, modify, block and/or remove an employee's or contract worker's access to the Company's Information Technology Systems

2. PURPOSE

a. This purpose of CYBERSECURITY POLICY is to

i. Maintain a secure company information technology environment insuring the confidentiality, integrity and availability of critical information and systems.

ii. Ensure the availability of systems through Disaster Recovery/Business Continuity planning, testing and execution.

iii. Enforce secure and effective access to technology resources through use of authentication and identity management technologies.

iv. Monitor and protect the network from threats posed by malicious entities located inside and outside the companies

3. PROCEDURE

a. Employees may be issued specific job-related technology (i.e. cellular phone, laptop computer, tablet, etc.). It is the employee's responsibility to properly care for, check in, check out, and maintain all issued technology

b. Employees will be required to notify IT of any problems, incidents or issues regarding issued technology equipment. The information we create, collect and use as part of our work is not only valuable but may also need special handling to avoid the potential for loss, misuse or harm to our reputation.

c. Company Information is to be used for company business purposes only. You should never:
   i. View it for a non-business reason
   ii. Access or transfer it for personal gain, advantage or any other personal reason
   iii. Give access to or transfer it without first obtaining appropriate approvals •
   iv. Download, upload, create or save it on a personally owned computing or storage device
   v. Access from a public computer

d. Employees are responsible for properly managing company information.

e. Intellectual property is confidential and includes, but is not limited to, copyrights, trademarks, patents, trade secrets, and contractual obligations.

f. All entries on the company's books and records must reflect fairly, accurately, and in reasonable detail, the business transactions and other activities of the company. Information created and contained within or transmitted via the company's technology is the property of the company. You should have no expectation of privacy regarding non-business, personal information created, communicated, transmitted and/or stored in information technology systems.

g. Access use and retention of information technology systems and company information must be as permitted by and in accordance with applicable laws, rules, regulations and company policies.

h. Employees must manage and protect all company information against loss and unauthorized access, especially secured information

i. You must report actual or suspected data security breaches involving unauthorized access to information to Management, Human Resources/or the IT department. Employee Handbook {JK01264784.1 17597 006 }

j. Company Information stored electronically should be maintained on Company-controlled and indexed systems with search capabilities

k. The use of an External Storage Device requires prior approval. Secured Information may have additional security requirements. The company is responsible for backing-up electronic Company Information stored on the company systems. The company is committed to ensuring that Company Information is not misused, altered, lost, disclosed or destroyed before its scheduled destruction

l. All Company Information must be kept secure and must be available when needed

m. Employees are required to change their network passwords every 90 days. Sharing your password with others is strictly prohibited. Email notifications will be emailed 10 days prior to the expiration of a password. Complex passwords are required, which means all passwords must contain as lease 8 characters and include the following: Passwords must be at least 8 characters long and include the following

    i. 1 Capital letter

    ii. 1 Lowercase letter

    iii. 1 Number

    iv. 1 Special Character

4. ROLES AND RESPONSIBILITIES

a. All employees should understand they are responsible to eliminate all cybersecurity threats.

b. All employees are responsible for protecting intellectual property owned by the company.

c. Supervisors are responsible for monitoring and provide feedback relating potential threats, abuse and neglect of technological equipment, tools and use.

d. The information technology (IT) department will implement cost effective solutions that enhances the company's ability to provide top quality services to our clients and customers to protect from Cybersecurity threats

5. TRAINING AND DOCUMENTATION

a. Employees are to review and acknowledge the Cybersecurity Policy at time of Hire/Onboarding and receive ongoing annual training reviews.

b. Employee training and acknowledgment documentation will be stored in employee training file