Cybersecurity Policies

This will outline clear expectations, rules, and approach that our organization will use to maintain the confidentiality, integrity, and availability of sensitive information obtained.

Protecting confidential data such as:

- Unreleased and classified information
- Customer, supplier, and shareholder information
- Patents and business processes
- New technology and software
- Employees' passwords, tasks, and personal information
- Contracts and legal records for the organization

Organization's use on device security:

- Keep all passwords and issued devices protected
- Secure company devices before leaving work area
- Obtain authorization from manager/supervisor before removing devices from organization premise
- **Regularly** update devices with the latest patches and security software

Organization on transferring data:

- Employees should not transfer classified information to outside parties
- Only transfer classified data over the organization's networks
- Any authorization needed must be obtained by manager/supervisor
- Verify the recipient of the information always, and ensure that the security measures are in place
- Immediately alert the IT department if any breaches or malicious software are found

Cybersecurity Training for employees

- Training helps minimize the risks that could potentially stem from user error. An organization can have all the technology in the world, but no technology solution will help stop all cyber-attacks if the end user is not prepared to help prevent it.

Cybersecurity response plan

Preparing for an incident, identifying incident and reporting it, containing it, eradication, recovery, and learning from the incident:

- Preparation: prepare users for a potential attack/incident
- Identifying: attempting to identify all details of the attack , and figure out why/how it occurred and what it has impacted
- Containment: containing the attack that occurred to make sure it does not affect other parts of the network and/or losing evidence of the attack.
- Eradication: eradicate the malware and patching any vulnerabilities

- Recovery: bringing the systems and networks back up and running – making sure it is all running smoothly again.
- Learning from Incident: Think about how the attack was contained and handled, and attempting to fix the gaps that caused the attack in the first place.

Legal Compliance

- HIPAA compliant: Compliance with the U.S. Health Insurance Portability and Accountability Act that requires companies and organizations that worth with protected health information (PHI) to implement and follow physical and network security measures.
- Export Administration Regulation: regulates the export, reexport and transfer of military items, commercial items, and purely commercial items without obvious military use.
- PCI Security Standards: The global data security standard that is primarily adopted and used by payment card brands that stores or transmits cardholder data and/or sensitive data.

Consistently test run cybersecurity policy and IT security policy

- By consistently test running policies, it will inform the organization of the cyber risk exposure and encourage them to address the identified issues to be able to improve their security.