JENDAMARK INDIA PRIVATE LIMITED

Cybersecurity Policy

Purpose:
The purpose of this policy is to protect the organization's assets and data from cyber-attacks and threats.

Scope:
This policy applies to all employees, contractors, and other individuals who have access to the organization's computer systems and networks.

Roles and Responsibilities:
Cybersecurity Team
Mr. Pranit Laxman Bhagwat (Senior Executive – IT)
Mr. Ashish Sanjay Relekar' (Jr. Executive – IT)

Employee Responsibilities:
- Use strong passwords and change them regularly. A strong password is at least 12 characters long and includes a mix of upper and lowercase letters, numbers, and symbols. Employees should change their passwords every 90 days or less, or more often if required by the organization.
- Be careful about what links you click on and what attachments you open. Phishing emails are a common way for cybercriminals to gain access to sensitive data. Employees should be careful about clicking on links in emails or opening attachments from unknown senders.
- Keep software and operating systems up to date. Software updates often include security patches that can help protect against known vulnerabilities. Employees should install software updates as soon as they are available.
- Be aware of the organization's cybersecurity policies and procedures. Employees should take the time to read and understand the organization's cybersecurity policy. They should also be aware of any specific cybersecurity procedures that apply to their job role.
- Report suspicious activity immediately. If an employee sees something suspicious, such as an unusual email or a strange login attempt, they should report it to their supervisor or the IT department immediately.

Employees are required to follow all of the security procedures outlined in this policy. These procedures include, but are not limited to:
- Using strong passwords and changing them regularly
- Encrypting sensitive data
- Reporting suspicious activity immediately

Enforcement:
Violations of this policy may result in disciplinary action, up to and including termination of employment.
In addition to the sections listed above, a cybersecurity policy may also include other sections, such as:
- Incident response plan: This section should describe the steps that the organization will take in the event of a cyber-attack.
- Risk assessment policy: This section should describe the process that the organization will use to assess its cybersecurity risks.
- Business continuity plan: This section should describe the steps that the organization will take to maintain operations in the event of a cyber-attack or other disaster

Policy Review:
On annual frequency policy will reviews and updates

Additional Sections:
Incident response plan, Risk assessment policy, Business continuity plan

Communication:
Jendamark India communicate this policy to all employees, contractors, and visitors through various means, including signage, employee handbooks, and Notice Board

Rev. No.: 00

Date: 01.08.2022

Mr. Himanshu Jadhav

CEO