Cyber Security Policy

Renaissance Global Ltd. Cyber Security Policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

This policy applies to all our employees who has permanent access to our systems and hardware.

The employees of the company are obliged to protect the company's data and the company has provided our employees guidelines on how to avoid security breaches.

The company also advices its employees to avoid accessing internal systems and accounts from other people's computers or lending their own computers to others.

The company advices its employees to avoid opening attachments and clicking on links when the content is not adequately explained and also of suspicious clickbait titles.

The company has provided adequate guidelines to the employees to have complex passwords as password leaks are dangerous and can compromise our entire infrastructure and have also stated to change them at regular intervals.

The company has devised clear guidelines and has informed employees to avoid transferring sensitive data (e.g. customer information, employee records) to other devices and email accounts unless absolutely necessary. The employees are further advised to share confidential data over the company network/ system and not over public Wi-Fi or private connection.

The company encourages its employees to report perceived attacks, suspicious emails or phishing attempts at the earliest to the IT Team for review.

The company understands the critical attempts at unapproved access to network systems and ensures reporting to the senior management, Internal/external business partners, customers/suppliers and government agencies as the need arises.

The company understands that the complaints to report cybercrimes needs to be uploaded on the government website i.e**. https://cybercrime.gov.in/** whereby feedback is provided by the governmental agencies after investigating the same.

The company also advices its employees to reduce the likelihood of security breaches by turning off their screens and lock their devices when leaving their desks and also report a perceived threat or possible security weakness in company systems.

The company has further laid down guidelines to refrain employees from downloading suspicious, unauthorized or illegal software on their company equipment and to avoid accessing suspicious websites.

The company also has laid down explicit guidelines to comply with our social media and internet usage policy as follows and have installed firewalls, anti-virus software's and has strict parameters set to access authentication systems.

The company endeavors to instill confidence in our customers, stakeholders and employees and ensure cyber security measures are strongly implemented in the company and the only way to gain their trust is to proactively protect our systems and databases to which we can all contribute by being vigilant and keeping cyber security top of mind.