IT Security Policy

everest

At Everest Industries limited, we acknowledge the importance of safeguarding our information assets, maintaining the integrity of the systems, and ensuring the continuous operation of our business. As such, we are pledged to establishing and enforcing robust IT security measures to protect against any and every unauthorized access, data breaches, and other cyber threats.

1. We adhere to all relevant laws and regulations of land related to IT assets and their security.
2. We aim to foster a culture of security by integrating best security practices into all business processes and practices. This includes regular training and awareness programs for all employees to ensure they understand their roles and responsibilities in maintaining security.
3. We are dedicated to nurturing skills and embracing behaviours that facilitate a safe digital environment. This includes providing ongoing education and training to our employees and promoting a culture of vigilance and responsibility.
4. We strictly use authorized software and adhere to anti-piracy norms. Unauthorized installation and use of software are strictly prohibited. We believe in respecting intellectual property rights and encourage our employees to do the same.
5. We are committed to protecting the privacy of all data related to our employees, customers, and vendors. We have implemented stringent measures to ensure the confidentiality, integrity, and availability of this data.
6. We adopt best practises and cutting-edge technology to manage the evolving threat landscape. This includes regular reviews and updates of our security measures to ensure they remain effective against new and emerging threats.
7. We aim to foster a culture of security by integrating best security practices into all business processes and practices. This includes regular training and awareness programs for all employees to ensure they understand their roles and responsibilities in maintaining security. We also provide specific training related to IT security norms.
8. In the event of a security incident, we have a comprehensive incident response plan in place to ensure swift and effective action. This includes identifying, containing, eradicating, and recovering from incidents, as well as learning from these incidents to improve our security measures.
9. We conduct regular assessments of our IT systems and practices to identify any potential vulnerabilities or areas for improvement. These are carried out by independent third parties to ensure objectivity.
10. We believe in continuous improvement and will regularly review and update this policy to reflect changes in our business, technology, and the wider threat landscape.

Date – 1st March 2024