



Since technology is constantly evolving, we at Graphite India Limited recognize the importance of cyber security and data privacy in delivering seamless information services to enable business operations, enhance productivity, customer satisfaction and stakeholder value along with adequate protection of information assets.

Graphite India Limited (GIL) will ensure that the risks associated with Information gathering, processing and preservation are assessed and managed to an acceptable level and have implemented an adequate security policies, processes, and controls to protect confidentiality, maintain integrity, and ensure availability of all information assets. The Purpose and Objective of this policy is to address the risks by defining, developing, and implementing adequate controls.

To achieve this, it's important to follow basic Data security Practices and Stay Proactive.

- ✓ Regularly Backup Your Data
- ✓ Keep All Systems and Software Updated
- ✓ Ensuring Antivirus Software is Installed and Regularly Updated
- ✓ Email Protection:
  - a) Don't open emails from unknown senders.
  - b) Keep email client apps updated.
- ✓ **DO NOT** leave sensitive information lying around the office.
- ✓ **DO NOT** leave printouts or portable media containing private information on your desk. Lock them in a drawer to reduce the risk of unauthorized disclosure.
- ✓ **DO NOT** use free, unsecured Wi-Fi for shopping or banking on the Internet and even for logging into your social media profiles.
- ✓ **DO NOT** click on links or download attachments from unwanted, unexpected emails, even if such emails look like they are from a known source.
- ✓ **DO NOT** be tricked into giving away confidential information. It's easy for an unauthorized person to call and pretend to be an employee or business partner.
- ✓ **DO NOT** respond to phone calls or emails requesting confidential data.
- ✓ **DO NOT** install unauthorized programs on your work computer. Malicious applications often pose as legitimate software. Contact your IT support staff to verify if an application may be installed.
- ✓ **DO NOT** respond to pop-up ads that may come up on your screen. Close such pop-ups from the task manager.
- ✓ **DO NOT** reply to e-mail(s) requesting financial or personal information. Please check the Email Address from where the mail has come before replying.

This policy shall be made available to employees and other concerned parties. The content and implementation of this policy shall be reviewed and updated periodically, synchronized to changing IT landscape.

|                            |                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------|
| Controlled Document        |  |
| Prepared & Issued by VP-IT | Page   1                                                                             |