EXCELLENT FORTUNE DEVELOPMENT GROUP

Data Security Policy

1. Overview

The protection of data is a critical business requirement. The company must protect restricted, confidential or sensitive data from loss to avoid reputation damage and to avoid adversely impacting our operations.

2. Purpose

The purpose of this policy is to outline the requirements on data security to prevent any data leakages.

3. Scope

This policy applies to employees, contractors, consultants and all other workers in the company and its subsidiaries, including all personnel affiliated with third parties.

4. Policy

4.1 You need to have a secure password on all systems containing company's data in accordance to the company's Password Policy. These credentials must be unique and must not be used on other external systems or services.

4.2 You must adhere to the company's Clean Desk Policy. To maintain information security, you need to ensure that printed data is not left unattended at your workstation.

4.3 You must not reference the subject or content of any sensitive or confidential data publicly.

4.4 Any sensitive or confidential information being transferred on a portable device (e.g. USB stick, laptop) must be password protected or encrypted.

4.5 You must ensure that assets holding company's data are not left unduly exposed, for example visible in the back seat of your car.

4.6 You must immediately notify your superior if a device containing company's data is lost (e.g. mobiles, laptops etc).

4.7 If you identify an unknown, un-escorted or otherwise unauthorized individual in the company's premises or work sites, you need to notify your superior immediately.

4.8 Visitors to the company's premises or work sites must always be escorted by an authorized employee. If you are responsible for escorting the visitors, you must restrict them to only the appropriate areas.

4.9 If you have been assigned the ability to work remotely, you must take extra precaution to ensure that company's data is appropriately handled.

4.10 If you find a system or process which you suspect is not compliant with this policy or the objective of information security, you have a duty to inform the policy owner so that appropriate actions can be taken.

4.11 Terminated employees will be required to return all records, in any format, containing the company's and personal information.

5. Policy Compliance

5.1 Compliance Measurement

The company will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the policy owner in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.