Towergold Limited - Data Security Policy

Introduction

Towergold Ltd needs to gather and use certain information about individuals and other legal entities. These include customers, suppliers, employees and other people Towergold Ltd has a relationship with or may need to contact, including government agencies.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards - and to comply with the law.

Why this policy exists

This data protection policy ensures that Towergold Ltd:

- Complies with data protection law and follows good practice
- Protects the rights of employees, customers, suppliers and other organisations
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Policy scope

This policy applies to all employees, suppliers, sub-contractors and any other person or institution working on behalf of Towergold Ltd.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR rules. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Vehicles associated with the individuals

As well as any other information relating to individuals.

Data protection risks

This policy helps to protect Towergold Ltd from some data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.

- Reputational damage. For instance, Towergold Ltd could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Towergold Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Users of data must ensure that it is handled and processed in line with this policy and data protection principles.

The board of directors (BOD) is ultimately responsible for ensuring the company meets its legal obligations. As regards data protection, the Company Secretary is required to:

- Inform the BOD about its data protection responsibilities, risks and issues.
- Review all data protection procedures and related policies, in line with an agreed schedule.
- Arrange data protection training and advice for the people covered by this policy.
- Handle data protection questions from staff and anyone else covered by this policy.
- Deal with requests from individuals regarding their rights in relation to their data held by Towergold Ltd.
- Check and approve any contracts or agreements with third parties that may handle personal data held by Towergold Ltd.
- Ensure all systems, services and equipment used for storing data meet acceptable security standards.
- Perform regular checks and scans to ensure security hardware and software is functioning properly.
- Approve any data protection statements attached to marketing communications such as emails and letters
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General employee guidelines

- The only people able to access data covered by this policy should be those who need it for their work and have been given access rights.
- Data should not be shared informally.
- Towergold Ltd will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines outlined below.
- In particular, strong passwords must be used and they should never be shared.

- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- Data should be regularly reviewed and updated. If it is found to be out of date or no longer required, it should be deleted and disposed of.
- Employees should seek assistance from the Company Secretary if they are unsure about any aspect of data protection.

Data Storage and Use

The rules, herewith, describe how and where data should be safely stored. Questions about storing data safely can be directed to the Company Secretary. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason.

- When data is stored on paper, it must be kept in a secure place where unauthorised people cannot see it nor have access to it.
- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer or photocopier.
- Any documents scanned on the networked photocopier should not be saved in the internal memory of the scanning machine.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees. Strong passwords should be made of a series of letters (upper and lower case), numbers, and symbols
- If data is stored on removable media (like a CD / DVD / USB thumb drives), then these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers.
- Servers containing personal data should be sited in a secure location.
- Company wireless networks should be secured using strong passwords, with the said passwords being made available to designated employees only.
- Access to company databases should be apportioned on a restricted basis to prevent the accidental deletion of data.
- Mobile telephones should be protected with a password / pin.
- Email clients on all Computers and Phones should be protected by strong passwords.

- Any internal mails that contain personal data should be encrypted.
- Emails that contain personal data and need to be transmitted externally should have their contents contained inside a Microsoft Word document with a strong password. The said password should be communicated to the recipient via another method, such as text message.
- Access to the company email / database servers should only be made over a secure (SSL) connection from mobile telephones / web.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company’s standard backup procedures.
- Data should never be saved directly to PC’s, laptops or other mobile devices like tablets or smart phones.
- Data should always be accessed and updated centrally.
- All servers and computers containing data should be protected by approved security software and a firewall.
- Logons to servers should be audited to detect any unauthorised access.
- Users should always lock their workstation when away from their desks.