cosco capital
incorporated

DATA PRIVACY AND CYBERSECURITY POLICY

The privacy and security of personal data collected from all our stakeholders - our customers, suppliers and service providers, shareholders and public investors, employees, in the course of conducting the group’s business activities are all important and critical to Cosco. The officers and employees of Cosco adhere to the principles of the Data Privacy Act (RA 10173) and comply with the best data privacy practices sanctioned in its Implementing Rules and Regulations and Memorandum Circulars issued by the National Privacy Commission.

SCOPE

This policy applies to Cosco and its subsidiaries’ employees, suppliers/vendors, customers, contractors, and anyone else who may have access to Cosco's systems, websites, software, and hardware.

OUR COMMITMENT

Cosco is committed to protecting and securing the data collected from our employees, customers, suppliers, contractors, and other service providers, whether in the form of a physical or a digital copy.

Protecting Privacy

Cosco commits to protecting the confidentiality as well as privacy of the information, records, and data collected from all our stakeholders in the course of conducting its normal business activities.

Cybersecurity and Information Security

Cosco commits to securing information, records, and data from our stakeholders through the application of multiple-layer cybersecurity measures to minimize or eliminate the risk of cyberattacks.

DATA PRIVACY PRACTICES

Collection of Personal Data

Cosco may gather personal information of all covered stakeholders such as name, address, phone number, gender, marital status, age, religious affiliation, health, or education in the normal course of business.

Use of Personal Data

Cosco uses these data to facilitate processing of transactions with all stakeholders, administer your account with us, and most especially, to be more efficient in providing you with our services.

Non-Disclosure of Personal Data

Cosco will not disclose your personal information without your consent or in any circumstance not authorized by law or any valid order of a court or government agencies.

Security of Personal Data

Cosco applies multiple-layer security measures and modern technologies to make sure your personal data are kept confidential and secured with us. Our employees are trained to handle your personal data with the utmost confidentiality and we have adequate internal control processes and systems in place to avoid security breaches or violations.

Use of Cookies

Our websites use “cookies” to allow us to help you navigate efficiently, obtain the information and services you need, and enhance user experience. Users' web browser places cookies on their hard drive for record-keeping purposes and sometimes to track information about them to help personalize the content presented to the user based on history. However, a cookie gives us no access to your computer or any information about you other than the data you choose to share with us.

You can choose to accept or decline cookies. By continuing to visit or use our website, you are agreeing to use cookies and similar technologies for the purpose described in this policy.

Data Privacy Rights

You may inquire or request information about processing your personal data, including the data privacy and security policies implemented by Cosco to protect your personal data.

You may also request for an updating, rectification, or amendment of your personal data or file a complaint in case of any breach or violation of your privacy.

You may send your inquiry or request to the following:

Email: dataprivacy@coscocapital.com
Letter: Office of the Data Protection Officer
3/F New Tabacalera Building, 900 Romualdez St., Paco
Manila, 1007 Philippines
Call: +632- 8257-0851

CYBERSECURITY PRACTICES

Device Security

Cosco's data may be in danger if employees log in to their company's accounts using their personal smartphones, tablets, or computers. Cosco does not advise its employees to use personal devices to access company data. If unavoidable, employees must keep their gadgets in a secure location away from the reach of others.

We advise our employees to adhere to the following best practices:

1. Keep the passwords for all electronic devices safe and secure.
2. Use only secure networks when logging into workplace accounts.
3. Regularly install security updates.
4. Update antivirus programs frequently.
5. Never leave your gadgets exposed and vulnerable.
6. When you leave your workplace, lock your computers.

Email Security

Emails may carry scams and malware (e.g. worms, bugs, etc.). Our policy is to constantly alert personnel to the following in order to prevent virus infection or data theft:

1. Avoid opening or clicking suspicious files and links.
2. Always double-check email sender names and addresses.
3. Look for inconsistencies in email addresses, links, and domain names. Also, check for grammatical errors and spelling mistakes.
4. Be wary of click-bait headlines (for example offering prizes, advice, etc.)

Employees may always get in touch with our IT department if they have any questions about whether the email or any other sort of data received is secure.

Data Transfer

Data transmission is one of the most popular methods of cybercrime. The company encourages to follow these recommended practices:

1. Avoid sending personal data such as customer and employee private information.
2. Observe data privacy protocols.
3. Data can only be exchanged over the company's network.