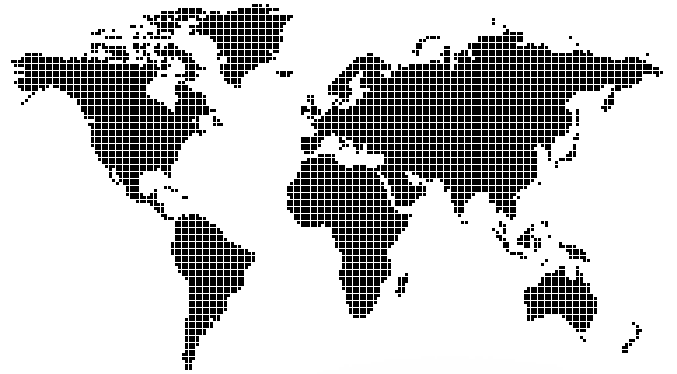


BUSINESSPOLICY

營業方針



THE DATA PROTECTION POLICY

Since 1998, we have successfully launched over 986 new product projects in our factories without a single case of copyright infringement or leakage of confidential information.

The Data Protection Policy is a mark of guarantee that 3CEMS will protect the intellectual property of our clients to the highest degree. This policy defines the measures, duties and roles every individual in the corporation takes to safeguard confidential information entering our factories.

All information relating to designs, product build and structure, on both hard and soft copies, will be labeled as "Secret".

Managing Media Storage

- The Media Management regulations affect all computers in the production departments, including, but not limited to, IE/ME/TE and QE divisions.
- There will be no access to any removable media, drives and ports. This includes, but is not limited to the following: diskette drives, CD-ROM/RW drives, USB ports or external access ports for the delivery of any data larger than 16 kilobytes.
- If in the situation that there should there be a need for the download of information to removable media (i.e. for mechanical, engineering, production, testing or quality control), the requestor, regardless of position, shall request for an approved, secured, USB drive. The drive shall only be released to the requester after the required release forms are attained and the signatories of the following management are received:
 - The Department Manager of the staff.
 - The Product Manager of the customer's information.
 - The Director of the factory.

The duration the drive is needed must be declared. Upon expiry, the drive must be returned for data verification. Any delay in performing this process may lead to severe disciplinary measures, which also includes the termination of employment.

- Email accounts will have restricted file size delivery. Installation of other file transfer software, or communications software that include file transfer features, like internet messengers, drop-boxes and file transfer protocols are disabled. Web access is limited in order to prevent access to web based file transfer services.

Paperwork Management

- The Paperwork Management regulations will affect all employees, regardless of position.
- Should copies of any information, classified as "Secret" be requested, the requestor shall complete the required release forms and acquire the signatories:
 - The Department Manager of the staff requesting the copies.
 - The Product Manager of the customer's information being requested for copies.
 - The Director of the factory where the copies are being requested.

Factory Security

- A list of materials, known as the Data Protection List, is posted at each department manager's office for the easy identification of secret data.
- Every individual is screened by both electronic and visual means upon entering and exiting the plant. Anyone who is in the possession of media or materials listed in the Data Protection List will be liable for disciplinary actions, including the termination of employment.

Pre Employment Scanning

- Every new hire may be subjected to intensive screening for previous criminal convictions.
- New hires into top level management are required to present at least two guarantors, one of which must be backed by a legitimate business entity. This will serve to guarantee the integrity and financial background of our managers and directors.

Non-Disclosure Agreement

- Non-Disclosure Agreements can be arranged by either the client or by us. This will serve as a material form of protection of intellectual property.