Electronic Assembly Services Ltd +pcb design +pcb manufacture +pcb assembly

EASL CYBER SECURITY POLICY

The risk of data leak, scams and security breaches can have a detrimental effect on EASL's systems, technology infrastructure and reputation. Subsequently, EASL has created this policy to protect EASL sensitive & confidential data and help outline the security measures put in place to ensure information remains secure and protected. All personnel have a responsibility to be cyber security aware in the activities they perform for EASL and to follow the requirements.

Scope:

This policy applies to all EASL's permanent and part-time employees, suppliers, interns and/or any individuals with access to the company's electronic systems information, software and/or hardware.

Transferring Data:

EASL recognises the security risks of transferring confidential data internally and/or externally. To minimise the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over EASL's networks.
- Obtain the necessary authorisation from senior management.
- Adhere to EASL confidentially agreement rules.
- Immediately alert the IT department regarding any breaches, malicious software and scams.

Email Security:

Protecting email systems is a high priority as emails can lead to data theft, scams and carry malicious software. Hence, EASL requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments and clicking on links.
- Contact the IT department regarding any suspicious emails.

Protect Personal and Company Devices

Employees are to keep both their personal and company-provided computer, tablet and mobile phone secure. To keep these devices secure:

- Keep all devices password protected and do not share the password with others.
- Login to company accounts and systems through secure and private networks only.
- Avoid accessing internal systems and accounts from other people's devices or lending your own devices to others.

Disciplinary Action:

Unintentional violations of this policy can warrant a verbal warning, frequent violations of the same nature can lead to a written warning and intentional violations can lead to suspension and/or termination.

Andy Birch
Managing Director