ROBOTECH
CADSolutions

Cyber security policy

1. Introduction

1.1 Cyber security has been identified as a major risk for Robotech CAD Solutions, Inc. (the "company") and every employee and contractor needs to contribute for us to remain secure.

1.2 The company has invested in technical cyber security measures, but we also need our employees and contractors to be vigilant and act to protect the company IT systems.

1.3 This policy provides information about your role in keeping the company secure.

1.4 Please contact Alberto Freire, CIO if you have any questions about cyber security.

3. Cyber security requirements

3.1 You must:

(a) choose strong passwords;

(b) never reuse a password;

(c) never allow any other person to access the company's systems using your login details; and

(d) keep passwords secret.

3.2 You must not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on your computer, phone or network or the company IT systems.

3.3 You must report any security breach, suspicious activity, or mistake you make that may cause a cyber security breach, to Alberto Freire, CIO by email within 60 minutes of the discovery or occurrence.

3.4 You must only access work systems using computers or phones that the company owns.

3.5 You must not install software onto your company computer or phone. All software requests should be made to Alberto Freire, CIO.

3.6 You should avoid clicking on links to unknown websites, downloading large files, or accessing inappropriate content using company equipment or networks.

4. Consequences of system misuse

4.1 The company considers the following actions to be a misuse of its IT systems or resources:

(a) any malicious or illegal action carried out against the company or using the company's systems;

(b) accessing inappropriate, adult or illegal content within company premises or using company equipment;

(c) excessive personal use of company IT systems during core working hours;

(d) removing data or equipment from company premises or systems without permission, or in circumstances prohibited by this policy;

(e) using company equipment in a way prohibited by this policy;

(f) circumventing technical cyber security measures implemented by the company's IT team; and

(g) failing to report a mistake or cyber security breach within 60 minutes of its occurrence or discovery.

4.2 If you are an employee, misuse of the IT system will be referred to the human resources team and may be considered misconduct or gross misconduct; if you are a contractor and are found to be misusing the company IT systems, your contract may be terminated.