cyber security policy

Introduction

Cyber security has been identified as a major risk for Armada Training Solutions Ltd (Armada). This policy outlines employees' and sub-contractors' responsibilities relating to Armada's IT systems, and every employee and sub-contractor must adhere to this for us to remain secure.

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

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

Please contact Steven Smith, Managing Director, if you have any questions about cyber security.

If you are an employee, this policy forms part of your employment contract. If you are a sub-contractor, this policy forms a part of your contract of engagement. Any breach of this policy shall constitute a breach of contract.

Employees' and sub-contractors' cyber security responsibilities and requirements

You must:

- Choose strong passwords. Passwords represent the biggest risk of unauthorized access to Armada's IT systems. Armada advises that a strong password contains different types of characters such as upper- and lower-case letters, numbers and punctuation characters;
- keep passwords secret;
- never reuse a password; and
- never allow any other person to access the company's systems using your login details.

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

You must report any security breach, suspicious activity, or mistake you make that may cause a cyber security breach, to *Steven Smith, Managing Director* immediately upon discovery or occurrence.

You must only access work systems using computers or phones that the company owns. You may only connect personal devices to the Armada's Wi-Fi available in all locations and training facilities.

You must not install software onto your company computer or phone without prior permission. All software requests should be made to Steven Smith, Managing Director.

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

Consequences of system misuse

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

- any malicious or illegal action carried out against the company or using the company's systems;
- accessing inappropriate, adult or illegal content within company premises or using company equipment;
- excessive personal use of company IT systems during core working hours;
- removing data or equipment from company premises or systems without permission, or in circumstances prohibited by this policy;
- using company equipment in a way prohibited by this policy;
- circumventing technical cyber security measures implemented by the company's IT team; and
- failing to report a mistake or cyber security breach.

If you are an employee, misuse of the IT system will be referred to Steven Smith, Managing Director, and may be considered gross misconduct; if you are a contractor and are found to be misusing the company IT systems, your contract may be terminated.

Reviewing

This policy is in effect, and should be reviewed every year.

Signed:

Policy version:	1.0
Original policy publish date:	1 October 2023
Last review date:	N/A
Reviewed by:	Steven Smith, Managing Director
Next review due:	30 September 2024