Cyber Security Policy

Introduction

1.1 Cyber security has been identified as a major risk for DeepForest (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 John Doe, IT Manager if you have any questions about cyber security.

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

Credit

2.1 This document was created using a template from SEQ Legal (https://seqlegal.com).

You must retain the above credit. Use of this document without the credit is an infringement of copyright. However, you can purchase from us an equivalent document that does not include the credit.

Cyber Security Requirements

3.1 You must:

(a) choose strong passwords (the company's IT team advises that a strong password contains list of types of characters, password length etc. as permitted by your IT systems);

(b) keep passwords secret;

(c) never reuse a password; and

(d) never allow any other person to access the company's systems using your login details.

additional list items

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 John Doe, IT Manager by contact method within number minutes of the discovery or occurrence.

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

company owns. You may only connect personal devices to the public Wi-Fi provided in the office.

3.5 You must not install software onto your company computer or phone. All software requests should be made to Jane Smith, IT Administrator.

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

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 number 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.

Declaration

I, John Smith, agree to use company IT systems only in the way this policy describes.

Signed by John Smith

Free Cyber Security Policy: Drafting Notes

This free cyber security policy has been created by Emma Osborn of OCSRC to help small (especially new) businesses to create their first internal policy in relation to cyber security.

This policy is identical to our basic policy, except that it includes a Docular credit, and accordingly it covers only the basics. If you need more detail, you should look at the standard and premium versions of the document.

Issues covered in the policy include: (i) the legal nature of the policy; (ii) the consequences of a breach of the policy; (iii) specific rules of behaviour relating to passwords, technical security measures, breach reporting, personal devices and software installation.

This policy is restrictive rather than permissive.