INNODIS LTD IT Policy

Executive Summary – June 2020

Table of Contents

Executive Summary 1

Introduction 2

Acceptable Use Policy 2

Access Control Policy 2

Clean Desk Policy 2

Disaster Recovery Plan 3

Email Policy 3

Ethics Policy 3

Pandemic Response Policy 4

Password Creation Guidelines 4

Password Protection Policy 4

Remote Access Tool Policy 4

Software for IT Users and Normal Users 5

VPN & Remote Access Policy 5

Wireless Policy 5

Non-exhaustive 5

Introduction

The present document is a concise summary of the IT policy of Innodis Ltd and is not exhaustive.

Acceptable Use Policy

The Acceptable Use Policy outlines use which is considered acceptable of any electronic device, computer or network system belonging to Innodis Ltd, the objective of which is to protect employees and the company from inappropriate use which entails risks such as unauthorised access, virus attacks and tampering with network systems and services. The policy outlines what is considered to be acceptable use, and also lists some types of use considered unacceptable and risky.

Acceptable use refers to normal day-to-day use in the course of company duties, and where employees are responsible for exercising good judgement.

The policy also lists some unacceptable uses, such as:

- Circumventing the IT security systems and protocols which the Company has put in place;
- Unauthorized use, or forging, of email addresses and email information;
- Accessing and/or using - or allowing access to and/or use of - devices and/or network systems without authorisation.

Access Control Policy

The Access Control Policy enforces the access rights that the IT team has put in place at Innodis Ltd. Upon request, each user can gain access to the Company's network, namely shared folders, email, and so on. Users are required to fill in the ***IT Access Form*** duly signed and approved by both the user's manager and the IT manager. As for any IT materials/equipment needed, a request needs to be sent by email, and management approval has to be obtained.

Clean Desk Policy

The Clean Desk policy determines the minimum requirements for maintaining a safe workplace to ensure that sensitive information is out of reach and secure. The policy reduces the risks of unauthorized access, loss of - and damage to - information during and outside normal working hours. It ensures that all confidential documentation and information are safely locked away when not in use or when the employee leaves his/her workstation.

Disaster Recovery Plan

This policy serves as a baseline for the requirements in the Disaster Recovery Plan process implemented by the IT Team to recover IT systems, applications, and data from any potential disaster that could cause major disruptions to operations. The Disaster Recovery Plan includes contingency plans and procedures in case a major unforeseen, disruptive event occurs. The contingency plans mentioned are:

- Computer Emergency Response Plan
- Succession Plan
- Critical services list
- Data Backup and Restore Plan
- Equipment Replacement Plan
- Mass Management

Email Policy

The email policy ensures the proper use of the company's email system and awareness about using the email system for the benefit of the company. The policy outlines the minimum requirements for the use of email within the network and provides guidelines for the appropriate use of email systems and services to minimize disruptions to services and activities, as well as to comply with the applicable policies and laws.

The Email Policy includes the following:

- Email Creation
- Monitoring and Confidentiality
- Email deletion

Ethics Policy

The purpose of this policy is to establish a culture of openness and trust, and serves as a guide for proper business behaviour and ethical conduct. The observance of sound ethical principles is a team effort involving the participation and support of every employee. The Ethics Policy outlines the following:

- Executive commitment to Ethics
- Employee commitment to Ethics
- Company awareness
- Formulation of ethical practices
- Unethical Behaviour and reporting

Pandemic Response Policy

This policy is intended to be followed in the case of a pandemic to limit the spread of the disease and outlines a response plan over and above the normal business continuity and disaster recovery planning of the Company. The Pandemic Response Plan includes contingency plans to ensure the continued running of the company's operations. The process plan incorporates the following:

- The Pandemic Response Plan Team
- The Communications Team
- An alert system
- A set of emergency safety polices
- An employee training process
- IT operations

Password creation Guidelines

The Password Creation Guideline provides best practices and requirements for creating secure and strong passwords. The password policy requires the use of secure passwords following the standards below:

- Contains a minimum of eight characters; and
- Contains alphanumeric and special characters (symbol); and
- Contains at least one uppercase and one lowercase character.

Password Protection Policy

The Password Protection Policy establishes a standard for the creation of strong passwords and the protection of those passwords. The policy covers the following points below where the best practices are listed to protect passwords:

- Password Creation
- Password Change
- Password Protection
- Application Development
- Multi-Factor Authentication

Remote Access Tool Policy

The Remote Access Tool Policy defines the requirements for remote access tools used at Innodis Ltd. Remote Access is a valuable tool used to provide support, and it must therefore comply with a set of requirements. For instance, it must be secured, include proper authentication and conform to the Company's security systems and measures.

Software for IT Users and Normal Users

A list of all softwares approved and/or installed for a user is maintained. The list may be amended as and when new softwares are introduced. Users are not allowed to install any software either listed or not listed without the approval of the IT manager. The list of approved softwares is found in the ***Software for IT Users and Normal Users Policy***.

VPN & Remote Access Policy

The VPN & Remote Access Policy defines rules and requirements for connecting to the company's network from any host. These rules and requirements are designed to minimize the potential exposure to Innodis Ltd from damages potentially arising from unauthorized access/use of the company's network and resources. Company prejudice may include the loss of confidential data, intellectual property, reputational damage, damage to critical internal systems, as well as fines or other financial liabilities incurred as a result.

Wireless Policy

The Wireless policy specifies the conditions that wireless infrastructure devices must satisfy to connect to the company's network. Only those wireless infrastructure devices that meet the standards specified in the policy are granted access to the Company's network.

Non-exhaustive

Kindly note that this is not the exhaustive IT Policy and is of limited scope. A full and updated version of the IT Policy is available on request.