CLOUD HOSTING WITHIN REACH

Information security policy

CLOUD HOSTING WITHIN REACH

Contents

1 Introduction

In the business context of VM Host's (VMH) operations it is recognised that infrastructure and customer information are vital for its success.
The company recognises confidentiality, integrity and availability of information and information systems as critical factors ensuring continuous operations.
The company shall establish, maintain and review information security management system (ISMS) in accordance with the international standard ISO/IEC 27001.

2 Purpose

The purpose of this policy is to:

- Provide principles for defining and regulating the management of information systems and other information assets,
- Ensure relevant and accurate information is available to staff members and customers,
- Ensure VMH's compliance with relevant regulatory and contractual obligations in protecting confidentiality, integrity and availability,
- Provide a secure and safe working environment for authorised staff members, contractors and interns,
- Protect its assets from all relevant threats, internal or external, deliberate or accidental,
- Ascertain that all staff members, contractors, interns and any other third party understand their responsibility in protecting confidentiality, integrity and availability,
- Appropriate information security objectives are defined and, where practicable, measured,
- Appropriate Business Continuity arrangements are in place to counteract interruptions to business activities and these take account of information security;
- Appropriate Information security education, awareness and training is available to staff and relevant others working on behalf of the company;
- Breaches of information security, actual or suspected, are reported and investigated through appropriate processes
- Appropriate access control is maintained and information is protected against unauthorized access.
- Continual improvement of the information security management system is made as and when appropriate.

3 Information security principles

4.1. All information shall be adequately classified in accordance with relevant regulatory and/or contractual obligation
4.2. Information shall be protected from unauthorised access and processing,
4.3. All authorised users are held responsible for information management and handling,
4.4. Information shall be provided with the cost effective protection according to its classification level,
4.5. Security events and incidents shall be reported in accordance with the company's policy.

4 Compliance, awareness and disciplinary procedure

5.1. Any security event or incident must be reported immediately,

5.2. All staff members, contractors, interns shall be informed about the policy and shall acknowledge they had understood the contents of the same