

Wildanet

High Level Statement



1. Document Control

Title	High Level Statement		
Owner	Justin Clark		
Author	Nathan Sussex		
Version	1.0		
Approved By:	Justin Clark		
Approval date	15/08/2021		
Audience	COO & ISF		

2. Document History

Version	Date	Comment	Updated by
1.0	01/08/21		Nathan Sussex

Information Security: High Level Statement

- A. The purpose of the Information Security Management System (ISMS) is to protect the Wildanet information assets from all threats, whether internal or external, deliberate or accidental.
- B. The Leadership Team has required that the ISMS be established and has approved the Information Security Policy (ISP) and has mandated that these will apply to Wildanet Systems.
- C. The Leadership Team has required that the ISMS is operated under a regime of continuous improvement through feedback from staff, interested parties and the audit regime.
- D. The Information Security Forum has responsibility for maintaining the policy, as well as related security policies, and providing advice and guidance on its implementation.
- E. The policy will be reviewed at least on an annual basis as well as upon significant changes in the business.

It is the policy of Wildanet to ensure that:

- a. Information will be protected against unauthorised access.
 - b. Confidentiality of information will be assured.
 - c. Integrity of information will be maintained.
 - d. Availability of information is ensured as required by the business processes. Regulatory and legislative requirements will be met.
 - e. It will implement relevant industry best practice in its endeavour to GDPR and DPA regulations.
 - f. Business continuity plans will be produced, maintained and tested.
 - g. Employees will undertake information security training at least on an annual basis.
 - h. All breaches of information security, actual or suspected, will be reported to, and investigated by the Information Security Forum.
 - i. Business requirements for the availability of information and information systems will be met.
- F. All managers are responsible for implementing the policy within their business areas and each member of staff will adhere to the policy.
- G. All staff (employees and contractors) are required to read and acknowledge the Information Security Policy. Non-compliance with the Security Policy will result in disciplinary action and in cases of serious breaches may result in dismissal.
- H. Supplier Partners shall adhere to Wildanet Information Security Policy in relation to Wildanet data where relevant.
- I. It is the desire of the Leadership Team that the company follows a cycle of continuous improvement with regards to the maturity of information security within the business, the ISMS and the wider organisation.

31 August 2021

Wildanet COO
Justin Clark