Information Security Policy

Classification: PUBLIC Reference: *ISO 5.1.1*

Contents

Information Security Policy

Classification: PUBLIC Reference: *ISO 5.1.1*

Policy Statement

The Board and management of UKFast, the head office of which is located at Manchester, which provides dedicated managed hosting, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout UKFast in order to preserve competitive edge, cash-flow, profitability, legal, regulatory and contractual compliance and commercial image.

Information and information security requirements will continue to be aligned with UKFast goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, for e-commerce and for reducing information-related risks to acceptable levels.

UKFast's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and the maintenance of ISMS. The risk assessment, Statement of Applicability and risk treatment plan identify how information-related risks are controlled. The IMS Manager is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

In particular, business continuity and contingency plans, data back-up procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are supported by specific, documented policies and procedures.

All employees of UKFast and certain external parties identified in the ISMS are expected to comply with this policy and with the ISMS that implements this policy. All staff, and certain external parties, will receive and/or be required to provide appropriate training.
The ISMS is subject to continuous, systematic review and improvement.

UKFast has established a Security Working Group (SWG) chaired by the Compliance Manager who will invite attendees from around the business to feedback on the information security programme of UKFast, its overall effectiveness and any suggestions for improvement.

For more details on how to participate in the SWG email compliance team. Opinions are welcomed from around the business.

UKFast is committed to maintaining certification of its ISMS to ISO27001:2013 as well as maintaining a secure cardholder data environment on its service delivery network along with robust physical security controls for the UKFast Campus sites and the Data Centres. In addition, UKFast will be committed to maintain similar levels of security at other sites such as satellite offices in Glasgow and London.

This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan, annually, as a minimum.

In this policy, "information security" is defined as: *preserving*

Information Security Policy

Classification: PUBLIC Reference: *ISO 5.1.1*

This means that management, all full time or part time staff, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches and to act in accordance with the requirements of the ISMS. The consequences of security policy violations are described in UKFast's disciplinary policy. All staff will receive information security awareness training and more specialized staff will receive appropriately specialized information security training.

The *availability*:

This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The UKFast network must be resilient and UKFast must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity and resilience plans.

Confidentiality:

This involves ensuring that information is only accessible to those authorised to access it and therefore preventing both deliberate and accidental unauthorised access to UKFast's information and proprietary knowledge and its systems including its network, websites and e-commerce systems.

Integrity:

This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency including for network, e-commerce systems, web sites, and data back-up plans, and security incident reporting. UKFast must comply with all relevant data-related legislation in those jurisdictions within which it operates.

Of the *physical (assets):*

The physical assets of UKFast including but not limited to premises, computer hardware, data cabling, telephone systems, filing systems and physical data files.

And *information assets:*

The information assets include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, web site(s), intranet(s), PCs, laptops, mobile phones and PDAs as well as on CD ROMs, USB sticks, back-up drives and any other digital or magnetic media, and information transmitted electronically by any means. In this context "data" also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.).

Information Security Policy

Classification: PUBLIC Reference: *ISO 5.1.1*

Of *UKFast:*

UKFast and such partners that are part of our integrated network and have signed up to our security policy and have accepted our ISMS.

A SECURITY BREACH is any incident or activity that causes or may cause a break down in the availability, confidentiality or integrity of the physical or electronic information assets of UKFast.

References

The Compliance Manager is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff via shared compliance management system.

This was approved by The Board and is issued on a version controlled basis under the signature of The Board. This document is reviewed annually.