UKFAST®
YOUR FUTURE IS OUR BUSINESS

INFORMATION SECURITY POLICY

Classification: Public

Document Owner: Head of Security & Compliance

Date: 06/05/2020

VERSION CONTROL

Version	Name	Description	Open Comment	Date
3.0	Stephen Crow	Head of Security & Compliance	Reformatted document	06/05/2020

Policy Statement

UKFast.net ltd and its subsidiary companies 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, contractual, compliance and commercial image.

Purpose

The purpose of this document it to set out UKFast's and its subsidiary companies aims and a framework for setting objectives for the management of information security through the organization. Clear Information and information security requirements will continue to be aligned with UKFast objectives and ISMS.

Scope

The Information security policy applies to all information assets owned by UKFast or which are on any networks managed by UKFast. The guidelines in the Information Security Policy, apply to all information which UKFast processes, irrespective of ownership or form. 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.

Framework

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 the ISMS. The risk assessment, Statement of Applicability and risk treatment plan identify how information-related risks are controlled. The Compliance team is responsible for the management and maintenance of the risk treatment plan and the responsibility of creating and distributing security policies and procedures.

Data Protection

The issue of data protection is at the forefront of UKFast's objectives for the future, especially in relation to GDPR. For this reason, UKFast has enhanced its ISMS to comply with ISO 27018 (Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) to help satisfy the legal requirement of abiding by the regulation.

Control objectives for each of these areas are supported by specific, documented policies and procedures. Where cloud platforms are provisioned to clients and UKFast is acting as data processor, contractual agreements will clearly define the responsibilities between UKFast and the client.

If clients have any issues concerning the protection of PII data, please contact DPO@ukfast.co.uk

Objectives

This policy sets out the foundation of the information security objectives for the year ahead, the objectives listed in a separate document titled "ISMS Objectives". Within this document are the objectives for the year, derived from the internal & external issues and requirements of the board. Each objective is consistent with this policy in terms of achieving or maintaining the triad of information security (Confidentiality, Integrity, and Availability), measurable where possible, have owners or updaters, and be based on the risk assessment results of the organisation.

Security Working Group

UKFast has established a Security Working Group (SWG) chaired by the Head of Defensive Securities & Compliance 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: information.security@ukfast.co.uk.

UKFast is committed to maintaining its ISMS and continually improving the system. A full, up to date list of UKFast's certifications can be found here. UKFast also maintain 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.

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*

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.

Confidentiality:

"Property that information is not made available or disclosed to unauthorized individuals, entities, or processes."

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:

"Property of accuracy and completeness"

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.

Availability:

"Property of being accessible and usable on demand by an authorized entity"

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.

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.).

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. If you think you have caused a security breach, or detected one. Please send all details to information.security@ukfast.co.uk

ClearCloud Information Security

ClearCloud uses AWS for their information security, this includes the ability to protect information, systems and assets.

This security possess the following features:

- Strong identity foundation: Enforces separation of duties with appropriate authorization for each interaction with AWS resources. Offers privilege management and reduce reliance of long term credentials.
- Enables Traceability: Monitor, alert and audit actions and changes within the ClearCloud environment. Integration of logs with systems to automatically respond and take action.
- Applies security to all layers: Security is applied to all layers (e.g., edge network, VPC, subnet, load balancer, every instance, operating system, and application).
- Automates security: Automated software improves the ability to securely scale more rapidly and cost effectively.
- Protects data at transit and at rest: ClearCloud data is classified into sensitivity levels and use mechanisms, for example encryption, tokenization and access control where appropriate.
- Protects data: AWS creates mechanisms and tools to reduce or eliminate the need for direct access of manual processing of data. This reduces the risk of loss or modification and human error when ClearCloud handle sensitive data.
- Prepares for security events: Allows ClearCloud to prepare for an incident by having an incident management process that aligns to ClearClouds requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.