

Information Security

POLICY STATEMENT



Global Switch Information Security Policy Statement

Issue No 4

Owner: Chief Financial Officer
Published on all Global Switch Websites
Displayed on all office notice boards

Introduction

Global Switch is a leading owner, operator and developer of large scale, carrier and cloud neutral, multi-customer data centre facilities in Europe and Asia-Pacific. Global Switch's core offering is technical space with resilient 24x7x365 power and cooling, security and infrastructure and environmental monitoring for its customers to house their computer servers, network equipment and other IT infrastructure.

Global Switch – Security

We are committed to protecting Global Switch and our customers from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, to minimise business damage and to maximise return-on-investment and business opportunities.

Objectives

The purpose of this Information Security Policy Statement is to confirm that Global Switch's Executive Committee and site Managing Directors will:

- Design, implement and maintain an Information Security Management system that conforms to the requirements of ISO 27001:2013 international standard and any relevant local laws, regulations and statutory requirements.
- Protect Global Switch's data from a loss of confidentiality, integrity and availability, including:
 - Information printed or written on paper
 - Information stored electronically
 - Information transmitted by post or using electronic means
 - Information stored on tape, video or disk
 - Information spoken in conversation
- Ensure that regulatory and legislative requirements will be met, such as the Companies Act, the Data

Protection Act, the EU General Data Protection Regulation (GDPR), the Computer Misuse Act and the Copyright, Design and Patents Act.

- Ensure a Business Continuity Plan is in place and will be maintained and tested to ensure that information and vital services are available to users 24x7x365
- Provide information security training to staff as required.
- Ensure that all breaches of information security, actual or suspected, will be reported to, and investigated by, the appointed Information Security Manager at each of Global Switch's data centres.

Guidance and procedures have been produced to support this policy, including:

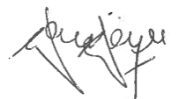
- Incident handling, information back up, system access, virus controls, password and encryption.
- The creation of the role of Information Security Manager (Managing Directors).
- A Policy update will be included on monthly Management Team Meeting Agendas.
- The Information Security Manager will ensure that the Information Security Policy is maintained at all times and is reviewed at a minimum annually.

Responsibilities

All Global Switch staff and contractors are required to comply with the Global Switch Information Security policy.

Responsibility and authority has been delegated to site Managing Directors (Information Security Managers) to meet the requirements of this policy and to ensure that in doing so they manage information security and provide advice and guidance on implementation of the Information Security Policy.

Signed



David Doyle
Chief Financial Officer, Global Switch
Reviewed: March 2019