Global Switch

Information Security Policy

Contents	Page No

Issue, review and amendment

Owner:	Group Director, Information
Sponsor:	Chief Operating Officer
Review Period:	Annual

Document Reviews				
Date	**Revision**	**Reviewer**	**Approver**	**Document changes**
16 May 2024	1	Arnie Owen		Initial draft document
05 Nov 2024	1	Arnie Owen	David Burton	Reviewed as part of ISMS implementation

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 24 x 7 x 365 power and cooling, security and infrastructure and environmental monitoring for its customers to house their computer servers, network equipment and other IT infrastructure.

Our data centres provide rich, carrier and cloud-neutral ecosystems and offer reliability, security, and flexibility that our customers require to house their IT infrastructure. Global Switch's Data Centres are exclusively positioned in central, network dense locations in Tier 1 markets.

As we operate globally, we recognise that we are subject to multiple pieces of legislation governing the protection of personally identifiable information and other laws governing the use of computing equipment and information processing.

Information Security Policy

The CEO and executive of Global Switch recognise that the effective management of information security risk is critical to protect the confidentiality, integrity, and availability of our information assets and the customer information and services stored and processed in our data centres and has implemented an information security management system (ISMS) to act as a framework for managing the information security arrangements intended to mitigate or manage these risks.

The ISMS establishes standards and rules that apply to all our facilities, services, and information .1systems, and the processes that support them and is subject to regular internal and

external audit to ensure that it remains effective while maintaining conformity to the international standard for information security management, ISO/IEC 27001.

Information Security Objectives

Global Switch has set objectives that the ISMS is intended to achieve which consider our overall business objectives, the needs and expectations of our stakeholders, and the outputs of our risk assessment and treatment activities. The objectives are to:

1. achieve accredited certification of the ISMS to the requirements of ISO 27001 and maintain it thereafter
2. ensure that our ISMS consistently reflects the context of our organisation and the needs and expectations of interested parties
3. ensure that we comply with relevant legislation, regulation and contractual obligations relating to information security
4. ensure that the ISMS, information security risks, and the controls implemented to manage those risks, are dynamic and reflect the changing threat landscape, the company's context, and our risk appetite
5. ensure that we operate effective access control processes to prevent unauthorised access to company and client information and to our data centres
6. implement a culture of information security through the provision of cyber and information security training and awareness
7. ensure that our Business Continuity arrangements are in place, maintained and tested to ensure that information and vital services are available to our clients when required.
8. ensure that risks associated with the use of suppliers are identified, assessed, controlled, and reviewed on a regular basis
9. ensure that our HR procedures and JLT processes are standardised and secure
10. ensure that our information systems and networks are effectively maintained and protected against internal and external threats
11. ensure that all issues within the ISMS and breaches of information security, actual or suspected, are reported, investigated and addressed in a timely manner
12. ensure we have the competence necessary to operate, maintain and improve the ISMS.

To achieve these information security objectives and ensure the effective management and continual improvement of information security, employees, contractors, and others working under our control are required to be aware of and comply with this policy and with the ISMS that implements this policy.

We are committed to the continual improvement of our ISMS and have established processes to support, periodically review, and continually improve the ISMS framework. This policy, and other topic-specific subsidiary policies, will be reviewed at least annually to ensure it remains suitable and reflects any changes that may impact the ISMS.

Responsibilities

Our CEO has overall responsibility, accountability, and authority for the management of information security risk across the Group and is supported by the Security Control Committee (SCC) who report directly to the Board of Directors and ensure that the ISMS continues to meet our Group strategic objectives as well as the needs of our customers and other stakeholders. The SCC provides executive oversight and direction to the ISMS and is made up of members of top management of Global Switch including:

- The Chief Executive Officer
- The Chief Operating Officer
- The Chief Legal Officer
- The Chief Financial Officer
- The Group Director, Information
- The Group Security Advisor
- The Information Security Director

The Information Security Director is responsible for the day-to-day operation of the ISMS and sits on other cross-functional bodies that represent business functions across the Group such as the Security Coordination Group and the ISMS Management Committee.

All employees and others working within the scope of the ISMS are required to comply with this policy and with other requirements of the ISMS that implement this policy. The consequences of breaching our information security requirements are set out in our disciplinary policy and in contracts and agreements with third parties. In addition, all staff and contractors are required to contribute actively to the continual improvement of the ISMS.

All Line Managers responsible for implementing and operating information security controls and processes and for monitoring and ensuring compliance with ISMS requirements within their area of responsibility.

Definitions

In this policy, ‘information security’ is defined as the preservation of:

the availability,

This means ensuring that information and associated assets are accessible to authorized users or systems when required and that our information systems are resilient and capable of meeting customer demands by implementing and operating controls that ensure the continued availability of assets, systems, and information and by establishing appropriate business continuity plans.

confidentiality,

This means ensuring that information is only accessible to those persons, systems and processes that are specifically authorized to access it by implementing and operating controls that prevent deliberate and accidental unauthorized access to our information and information systems including mobile devices, virtual and physical servers, networks, applications, or websites.

and integrity

This means ensuring that the information we store, process, or otherwise rely on is complete and accurate by implementing and operating controls that prevent deliberate or accidental, partial or complete, destruction or unauthorized modification, of information whether in digital or analogue form.

of the physical (assets)

Our physical assets include the buildings or rooms where we work or meet, data centre facilities where we store and manage our servers and network devices, the endpoint devices that we use to access or process information such as laptops, desktops, or phones, any physical media used to store data, and the documents or records that we keep on paper, such as contracts, reports, or invoices

and information assets

Our information assets include any kind of information that we create, use, store, or share in our work including analogue data printed out or written on paper, verbal information spoken in conversation and over the telephone, information stored in digital format on computer devices and digital or magnetic media, and information transmitted digitally by any means.