Public Security Policy

ORIIUM Public Policy Document

13 Nov. 25

Contents

1. Policy Summary

ORIIUM recognises that information and the associated processes, systems and services are valuable assets to the company. ORIIUM also acknowledges that the management of data has important implications for employees and other individuals associated with the company.

Through its quality assured security policies, procedures and systems, ORIIUM will strive to adhere to best practice as detailed in ISO 27002:2013 and keep its ISO 27001:2013 accreditation

The policies outlined in this document are intended to support information security measures throughout ORIIUM supported by further quality assured policies, procedures and systems.

1.1 Scope

The information policies in this document relate to all information assets owned and controlled by ORIIUM. ORIIUM is based in the UK and the majority of its information assets will be stored in Tier 3 Data Centres all of which will be located in the UK and which operate under ISO 27001 and be accredited by a recognised body.

Information security is defined as the preservation of Confidentiality, Integrity and Availability as defined below:-

- Confidentiality - refers to the limitation of, access to, and disclosure of, information to authorised users and the prevention therefore to unauthorised users
- Integrity - refers to the trustworthiness of the information. Consistency, accuracy and the validity of data must be maintained throughout its entire lifecycle and so measures are put in place to ensure data is not changed inappropriately
- Availability - Information resources are only of use when they are available in the first place. The security systems and policies must ensure that data is available for use

Information assets may be stored and transmitted in many forms, including but not limited to:

- Stored in databases or file systems

- Stored on computers or mobile devices
- Transmitted across internal and public networks (encrypted where appropriate)
- Printed or handwritten on paper, white boards etc
- Sent by facsimile (fax), telex or other communications method
- Stored on removable media such as CD-ROMs, hard disks, tapes and other similar media Stored on fixed media such as hard disks and disk sub-system
- Presented on slides, overhead projectors, using visual and audio media
- Spoken during telephone calls and meetings or conveyed by any other method

1.2 Information Security Responsibilities

ORIIUM believes that information security is the responsibility of all members of staff. Every person handling information or using ORIIUM information systems is expected to observe the information security policies and procedures.

This Policy is the responsibility of the ORIIUM Board. Management of the Policy will be undertaken by the ORIIUM Security Forum. This policy will be supplemented by other policies and procedures for specific sites, systems and services. Implementation of information security policy is managed through the Security Forum and other designated personnel with security responsibilities within specified areas of ORIIUM.

1.3 Information Security Training

ORIIUM recognises the need for all staff and other users of ORIIUM systems to be aware of information security threats and concerns, and to be equipped to support ORIIUM's security policy in the course of their normal work. The Security Forum will implement a training / briefing programme for all staff.

1.4 Legal and Contractual Compliance

ORIIUM intends to fully comply with the requirements of Data Protection legislation in so far as it directly affects ORIIUM's activities.

1.5 Procurement

Procurement of services, systems and items will be obtained in accordance with ORIIUM purchasing policies and an asset register is maintained.

1.6 Information Access Control

Access to information assets will be controlled to provide a balance between information security and availability. Only authorised users will have access to ORIIUM information assets.

1.7 Information Handling and classification

ORIIUM have implemented and maintain a classification scheme for all information assets to control access to information and data. Information shall be processed and stored in accordance with the classification of the information

1.8 Monitoring and Auditing

ORIIUM IT facilities must only be used for authorised purposes. ORIIUM may from time to time monitor or investigate usage of IT facilities. Any person found using IT facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary action, and where appropriate, legal proceedings may be taken. All users of ORIIUM IT facilities must abide by the ORIIUM Acceptable Use statements in the Information Security Management Policies.

1.9 Cyber Crime

ORIIUM will implement and maintain policies that minimise the possibility and impact of attacks on the network (such as Denial of Service and Virus attacks) and allow for collection of evidence for prosecutions.

1.10 Personnel Security

ORIIUM holds and processes information about employees, customers and other data subjects for administrative and commercial purposes. When handling such information, ORIIUM and all staff or others who process or use any personal information must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). Responsibilities under the 1998 Act are set out in the Data Protection Policy.

ORIIUM ensures that Senior and field-based personnel have an enhanced DBS disclosure which will allow them to operate in schools.

1.11 ORIIUM Premises Security

ORIIUM will implement security safeguards for its Premises which will include card access to its buildings and cameras. Internal and customer services are not

provided from its Head Office with the exception of the landline phone system. All services are to be provided in a Tier 3 Data Centre which operates under ISO27001.

1.12 Security Incident Management

ORIIUM will provide mechanisms and encourage all security incidents, physical or virtual, to be reported by ORIIUM staff using the ORIIUM Security Forum. The Security Forum incidents will be managed and reviewed on a regular basis by the Security Forum Team and any risks managed and treated, if appropriate, with updated and new procedures or changes to working practices or physical systems. Security incidents from customers can be logged using their normal service desk procedures. These incidents, if appropriate, will then be lodged in the Security Forum for review.

1.13 Business Continuity

ORIIUM will implement and test business continuity procedures to ensure that systems and processes are available for all key functions that underpin ORIIUM as a business and the services it provides to customers. The customer systems business continuity will vary depending on the service levels purchased.

ORIIUM will implement, and regularly update, a business continuity management process to counteract interruptions to normal activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

This policy has been approved by the ORIIUM Board.