Reseller Code of Conduct

ORIIUM Channel Policy Document

14 Nov. 25

Summary Statement

ORIIUM is committed to high standards of, amongst others, environmental sustainability, human rights, antibribery and corruption, integrity and business security. We anticipate that all of our resellers will abide by similar standards as detailed below and conduct their business in an ethical manner. As a minimum, resellers should comply with all applicable local, national and international legislation.

Human rights, equality and diversity

ORIIUM believes in fairness, equality and, above all, values diversity. We expect our resellers to:

- comply with all relevant legislation including the Human Rights Act 1998 and the Equality Act 2010;
- respect the personal dignity, privacy and rights of all individuals, including your employees and those in your supply chain;
- not tolerate discrimination on the basis of gender, age, disability, race, religion, sexuality, social class or in any other way;
- ensure equal opportunities are available to all
- understand diversity through inclusion of all people, regardless of age, disability, gender, racial origin, religion, belief, sexual orientation, language.

Fair employment practices & conditions, slavery, human trafficking and child labour

ORIIUM is committed to ensuring that employment is freely chosen, child labour shall not be used, and no harsh or inhumane treatment will occur. Our resellers are expected to (and must ensure that their supply chain shall):

- respect the rights of employees to freely associate and bargain collectively
- not use any forced labour or involuntary prison labour and allow all employees the choice to leave their employment freely upon reasonable notice;
- not force the relocation or movement of any workers;
- not use or promote forced or child labour in any way;
- understand that all staff are entitled to work in an environment which respects their personal dignity and take steps to ensure that the working

environment is free from harassment, bullying or any other type of intimidation.

Health and safety

ORIIUM aims to provide each employee with a safe working environment. We expect our resellers to:

- ensure that all operational locations meet, as a minimum, all local health and safety regulations;
- ensure all employees are appropriately trained and aware of all health and safety risks;
- procedures within their working environment;
- record all accidents and/ or near misses and investigate these to determine if preventative action is required to prevent further accidents.

Environmental sustainability

ORIIUM believes that it has a responsibility to identify and manage activities which affect the environment and we are committed to continually improving the environmental impact and sustainability of our business. Accordingly, we expect our resellers to:

- minimise the environmental impacts of existing operations and ensure that the environmental impacts of new operations are assessed;
- minimise waste and maximise recycling through the reuse and reconditioning of devices and other materials;
- make a responsible effort to minimise the use of packaging, reuse where practicable and avoid, where possible, the use of packaging which consumes a disproportionate amount of energy or resources during the manufacturing process;
- introduce programmes which aim to minimise waste;
- promote the ownership and control of environmental issues at business level;
- conserve energy and minimise carbon emissions, where practicable;
- reduce your energy expenditure and increase energy efficiency as much as reasonably practicable especially in relation to lighting, heating, air conditioning and kitchen appliances (including water conservation).

Business Continuity and Disaster Recovery

Resellers shall ensure that they have in place and is able to implement the provisions of a business continuity plan for the continued provision of the services. The reseller shall:

- maintain a Business Continuity Plan (BCP) that ensures the continued provision of the Services during and after disruptive incidents;
- regularly review, update, and test the BCP to ensure its effectiveness and alignment with current risks and operational changes;
- include Disaster Recovery (DR) provisions for critical IT systems and data, with defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs);
- ensure BCP/DR plans are proportionate to the nature, scale, and criticality of the services provided;
- provide assurance upon request (e.g., summary of BCP, test results, certifications such as ISO 22301) to demonstrate preparedness;
- notify ORIIUM promptly of any incident that may impact service delivery and cooperate fully in mitigation and recovery efforts;
- ensure key subcontractors or third parties involved in service delivery also have appropriate BCP/DR arrangements in place.

Anti-Bribery, corruption and anti-competitive practices

ORIIUM adopts a zero-tolerance approach towards bribery, fraud, and corruption and is committed to the highest levels of ethical conduct and integrity in business activities. We expect our resellers to:

- refrain from and prevent any and all forms of corruption, extortion, bribery, and fraudulent activity in accordance with the Bribery Act 2010 and other applicable legislation;
- ensure that appropriate prevention procedures are in place to mitigate the risk of tax evasion and to comply with the provisions of the Criminal Finances Act 2017;
- implement robust anti-fraud controls, including internal checks, due diligence processes, and regular monitoring to detect and prevent fraudulent behaviour;
- apply this policy to all employees and directors, as well as to temporary workers, consultants, contractors, agents, and subsidiaries acting for and on behalf of our suppliers;

- understand that it is the responsibility of all employees and associated persons to assist in the prevention, detection, and reporting of bribery, corruption, and/or fraud;
- ensure all employees are aware of how and to whom to report any concerns or suspicions of unethical or illegal conduct, and encourage a culture of transparency and accountability;
- ensure new business is procured in a responsible and ethical manner, with appropriate due diligence on third parties;
- ensure employees disclose any actual or potential conflicts of interest in a timely and transparent manner;
- not partake in any anti-competitive practices, including collusion with peers, suppliers, or any other parties with the aim of influencing pricing, bid rigging, participating in or being involved with a cartel, or any other practice which is intended to or which has the effect of reducing free competition in any marketplace.

Secure business

ORIIUM is committed to maintaining the highest levels of security. We expect our resellers to:

- implement appropriate and proportionate measures to minimise exposure to physical security threats, including terrorism, crime, pandemics, and natural disasters;
- implement robust controls to mitigate cybersecurity risks, including threats from malware, hacking, data breaches, and other malicious activities;
- comply with the Data Protection Act 2018 and any applicable data protection laws, ensuring that suitable technical and organisational measures are in place to safeguard personal data. Any actual or suspected data security incidents must be reported promptly to the designated contact; and
- protect all confidential information and intellectual property belonging to ORIIUM, its clients, and other third parties, ensuring it is not disclosed, misused, or compromised.

Privacy / GDPR

ORIIUM requires all resellers to comply fully with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, including the need to demonstrate accountability and readiness for more stringent enforcement than under the original UK Data Protection Act. Resellers must:

- Demonstrate compliance with UK GDPR principles, including lawfulness, fairness, transparency, data minimisation, and purpose limitation, and be able to provide a formal GDPR Compliance Statement upon request;
- Implement appropriate technical and organisational measures to ensure the security of personal data, including encryption, access controls, and breach detection protocols;
- Conduct regular internal audits and risk assessments to monitor data protection practices and identify areas for improvement;
- Ensure that all employees and subcontractors handling personal data are trained in data protection responsibilities and understand their obligations under UK GDPR;
- Maintain up-to-date records of processing activities, including data flows, retention periods, and lawful bases for processing;
- Enter into appropriate data processing agreements where acting as a processor, ensuring that contracts include all mandatory clauses under Article 28 of UK GDPR;
- Undertake due diligence on any sub-processors or third parties involved in data processing, and ensure that international data transfers are covered by valid safeguards such as the UK international data transfer agreement;
- Notify ORIIUM promptly of any actual or suspected data breaches, and cooperate fully in breach investigations and remediation efforts.