Title	Information Security Policy	Version 1.0

The Senior Management team of DGP Intelsius Ltd located at 1 Harrier Court, Airfield Business Park, Elvington, York, YO41 4EA, UK, are committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout their organisation, in order to preserve its legal, regulatory and contractual compliance and public image. Information and information security requirements will continue to be aligned with DGP Intelsius Ltd's targets and the integrated Information Security Management System (ISMS) is intended to be an enabling mechanism for information sharing, for electronic operations, and for reducing information-related risks to acceptable levels.

DGP Intelsius Ltd's current strategic plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. The Information Security Officer is responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

Business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and sites, and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in this and are supported by specific documented policies and procedures.

DGP Intelsius Ltd aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organisation, the results of risk assessments and the risk treatment plan.

All employees of DGP Intelsius Ltd are expected to comply with this policy and with the ISMS that implements this policy. All employees, and certain external parties, will receive appropriate training. The consequences of breaching the information security policy are set out in the Organisation's disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement. We have established a top-level management commitment to support the ISMS framework and to periodically review the security policy. This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan.

In this policy, 'information security' is defined as:

Preserving
This means that management, all full-time and part-time employees, 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 (in line with the policy) and to act in accordance with the requirements of the ISMS. All employees will receive information security awareness training and more specialised Staff will receive appropriately specialised information security training.

The availability
This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The computer network must be resilient, and DGP Intelsius Ltd 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.

Confidentiality
This involves ensuring that information is only accessible to those authorised to access it and therefore to preventing both deliberate and accidental unauthorised access to DGP Intelsius Ltd's information, proprietary knowledge, and its systems including its networks and website.

And integrity
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, data backup plans and security incident reporting. We must comply with all relevant data-related legislation in those jurisdictions within which it operates.

Of the 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, websites, extranets, intranets, PCs, laptops, mobile phones and PDAs, as well as on CD ROMs, floppy disks, USB memory devices, backup tapes 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 how to manipulate information (i.e., the software: operating systems, applications, utilities, etc.) of DGP Intelsius Ltd, and such partners that are part of our integrated network and have been made aware of our ISMS.

And of the physical (assets)
The physical assets of DGP Intelsius Ltd including, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

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 DGP Intelsius Ltd.

This Policy is communicated to all employees and contractors at induction and upon significant change. It is available to all interested parties on request. This policy is reviewed for effectiveness and suitability on at least an annual basis or upon significant organisational change.

Signed:

Alastair Harries
Chief Operating Officer

Approval Date: 18Jan22

Review Date: 17Jan23