OPUS ENERGY LIMITED

CCTV Privacy Notice

1. Introduction

Opus Energy Limited ("**the Company**") is committed to the safety of its staff and visitors and as a result it has invested in a closed-circuit television system ("**CCTV**") at its sites. The purpose of this document is to set out how the CCTV system will be managed and used by the Company and to inform individuals, whose personal data may be captured on the CCTV system, about how and why that personal data may be processed by the Company.

The use of the CCTV system is overseen by our Data Protection Manager who can be contacted at data.protection@opusenergy.com or using the contact details in the "Contacting Us" section below.

The day-to-day operation of the CCTV system is managed by a third-party service provider under the direction of the Company's Security Operations Manager, with local oversight by Company security staff at Company sites.

If you have any queries about the content of this document or our use of CCTV, please contact us using the contact details in the "Contacting Us" section below.

2. Compliance

The Company is aware that images of recognisable individuals, such as staff and site visitors ("**data subjects**"), captured by the CCTV system constitute 'personal data', use of which is governed by data protection law ("**the law**").

The Company will ensure that its use of the CCTV system and the personal data that it captures complies with the law.

This document has been drafted in accordance with the Information Commissioner's Office (ICO) CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice. Copies of these codes can be found at www.ico.org.uk and https://www.gov.uk/government/publications/surveillance-camera-code-of-practice respectively.

3. Objectives of the CCTV System

The objectives of the CCTV system are:

- To increase the personal safety of our staff and visitors to our sites;
- To support our health and safety measures;
- To assist in identifying, apprehending and prosecuting any offenders on Company sites;
- To protect the Company's buildings and assets and those of its staff from intrusion, theft, vandalism, damage or disruption.

The legal basis for the Company's use of any personal data which is captured by the CCTV system is that the processing is necessary for the legitimate interests set out in this paragraph (provided that those interests are not overridden by individuals' rights and interests). The Company may also need to use this personal data in order to establish, exercise or defend against legal claims.

4. Operation

CCTV cameras are located at strategic points on our sites, primarily access points, such as the gates to the sites, in office areas and in certain production areas.

Signs are displayed prominently around the sites to inform staff and visitors that CCTV cameras are in operation and who to contact for further information.

The cameras are in operation 24 hours a day, 7 days a week and they will be monitored from the Security Control Room based at the Drax Power Station near Selby in the UK. Drax Power Limited is a company in the Company's Group of companies and manages all the footage from the CCTV cameras. In addition, the cameras can be monitored by Company security staff at the Company site. Our third-party service provider will regularly check and confirm the efficiency of the system, including that the equipment is properly recording, that the cameras are functional, that the time and date are correct and that that footage is being deleted or retained in accordance with this document.

The CCTV system will be regularly maintained in accordance with the manufacturer's instructions.

5. Information Retention

The images captured by the CCTV System will not be stored for any longer than is required in order to achieve the purposes identified in paragraph 3 above. CCTV footage will automatically be deleted on a 30-day rolling basis, unless specific images are required to be retained in order to deal with an incident or in order to respond to a request by an individual made under the law (see paragraph 9 below).

6. Security

Physical Protective Measures: The Security Control Room (within the security area) can only be accessed with the correct access control privilege, which is primarily limited to security staff. A record is kept of all those who are given access to the Control Room.

Technical Protective Measures: We have put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. This includes the fact that the CCTV hard drives are located in a secured server room and access to this room is only via a formal approval process. Password protection, technical access control and the use of encryption are also technical protection measures that we use.

We have put in place procedures to deal with any suspected personal data breach and will notify any affected individuals and/or the ICO where appropriate.

7. Access and Disclosure

Access to recorded CCTV footage is restricted to a limited number of security staff as authorised by the Security Operations Manager from time to time ("**Authorised Persons**") and all requests for disclosure of CCTV footage must be submitted to one of these Authorised Persons.

CCTV footage may only be accessed or disclosed to the extent necessary in order to deal with an incident which falls within one of the objectives identified in paragraph 3 above or in order to respond

a request made by an individual under the law (see paragraph 9 below). CCTV footage must not be accessed or used for any other purpose.

CCTV footage will be viewed in a secure office and any access to and any disclosures of recorded footage will be recorded in the CCTV log. This process is overseen by the Security Operations Manager and as appropriate, with reference to the relevant member of our data protection team.

External disclosure of CCTV footage will usually not be permitted other than to law enforcement agencies or to regulators, or in order to comply with a court order. CCTV footage will not be uploaded to the internet.

8. Training

All staff who may be involved in the management or operation of the CCTV system will be trained in how to comply with this document and to ensure that the system is used in accordance with the law.

9. Individual Rights

The law provides individuals (data subjects) with the following rights in relation to their personal data held by the Company about them and this may include personal data included in CCTV footage:

The right to:

- request access to their personal data (commonly known as a "data subject access request"). This enables them to receive a copy of the personal data we hold about them and to check that we are lawfully processing it;

- request correction of the personal data that we hold about them. This enables them to have any incomplete or inaccurate information we hold about them corrected;

- request erasure of their personal data in certain circumstances. This enables them to ask us to delete or remove personal data where there is no good reason for us continuing to process it. Data subjects also have the right to ask us to delete or remove their personal data where they have exercised their right to object to processing (see below); and

- request the restriction of processing of their personal data. This enables them to ask us to suspend the processing of personal data about them, for example if they want us to establish its accuracy or the reason for processing it.

In addition, a data subject may object to the processing of their personal data where we are relying on a legitimate interest (or those of a third party) and there is something about their particular situation which makes them want to object to processing on this ground.

We will deal with any requests made from data subjects to exercise their above rights in accordance with the law. Any above request from an individual should be submitted to one of the Authorised Persons who will deal with it in accordance with the law and our Individual Rights Guidance.

Data subjects will not have to pay a fee to access their personal data (or to exercise any of the other rights above). However, the Company may charge a reasonable fee if the request for access is clearly unfounded or excessive. Alternatively, the Company may refuse to comply with the request in such circumstances.

The Company may need to request specific information from a data subject to help confirm their identity and ensure their right to access the personal data (or to exercise any of the other rights). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

A data subject has the right to make a complaint at any time to the ICO, the UK data protection regulator. The ICO can be contacted by telephone on 0303 123 1113 or by post as follows: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF or via email at casework@ico.org.uk. The Company would, however, appreciate the chance to deal with any concerns before the data subject approach's the ICO, so please contact the Company in the first instance using any of the details set out below in the "Contacting Us" section.

10. Covert Recording

Covert recording will only be carried out in very limited circumstances and with the authorisation of our Information Security Manager and/or Data Protection Manager.

Covert surveillance will only be carried out where specific criminal activity is suspected and where informing the relevant individuals would be likely to prejudice the prevention of crime and/or apprehension/prosecution of the offender.

Any authorisation to use covert recording will be documented in writing and include confirmation that it is required to obtain evidence of suspected criminal activity in a specific case, an assessment of the alternative methods of obtaining the evidence and the permitted duration of the covert recording. The authorisation will be regularly reviewed, for example, every 28 days, to assess whether it is continued to be required or should cease.

11. Breach of this Document

In relation to our staff, unauthorised access to or disclosure of CCTV footage, or other misuse of the CCTV system, or any other breach of this document or the law, may result in disciplinary action, including summary dismissal. Unauthorised use or disclosure of CCTV footage may also be a criminal offence.

12. Annual Review

This document and the use of the CCTV system will be audited on an annual basis, to include a review of:

a The effectiveness of the system in achieving the stated objectives and whether use of the system continues to be justified;

b Compliance with this document, including compliance with the rules relating to access, disclosure and deletion of the CCTV footage;

c The effectiveness of applicable security measures; and

d Compliance with the law.

12. Contacting Us

Any queries or complaints about the CCTV system should be addressed to the Security Operations Manager at Drax Power Station, Selby, North Yorkshire, YO8 8PH or via email to securityoperationsmanager@drax.com.

If you have any queries, comments or requests regarding this document or you would like to exercise any of your rights set out above, you can contact us as follows:

- Our Security Operations Manager at securityoperationsmanager@drax.com or Drax Power Station, Selby, North Yorkshire, YO8 8PH; or
- Our Data Protection Manager at data.protection@opusenergy.com or Opus Energy Limited, Opus Energy House, 8-10 The Lakes, Northampton, NN4 7YD