Information Security Programme Management

Table of Contents

1. Our Company, Our Product, Our Philosophy

DeepStream Technologies is a business to business e-commerce platform, connecting businesses in exchanging information for the purposes of commercially transacting with each other. Lots of companies trust our technology

DeepStream Technologies values openness & transparency in how we provide efficient and effective value-add solutions to our customers. This document is designed with this philosophy in mind.

We are always reviewing how we protect the confidentiality, integrity and availability of your data to ensure we maintain the highest possible levels of security.

DeepStream Technologies operations are designed to be compliant to ISO 27001:2013 – the international standard for Information Security. We work with our external, UKAS accredited, auditors to gain and then effectively maintain compliance to the requirements of the ISO standard.

The scope of our Information Security Management System (ISMS) is **The development, provision and support of a secure cloud-based procurement network for buyers and suppliers of equipment and services in the energy sector**

The DeepStream Technologies ISMS encompasses:

- People … all employees and subcontractors
- Products / Services … DeepStream platform and associated products and services
- Processes … all internal business support and customer service processes
- Technology and assets … all IT and physical infrastructure at our premises / hosted sites and used by our employees / contractors whether on the premises or off-site

2. POLICY STATEMENT

To protect the information assets that DeepStream Technologies processes and has access to, and to ensure the ongoing maintenance of their confidentiality, integrity and availability.

To ensure controls are implemented that provide protection for information assets and are proportionate to their value and the threats to which they are exposed.

To ensure that DeepStream Technologies complies with all relevant legal, customer and other third-party requirements relating to information security.

To continually improve the Information Security Management System (ISMS) and its ability to withstand threats that could potentially compromise information security.

This policy applies to all people, processes, services, technology and assets. It also applies to our subcontractors of information security critical suppliers who access or process information assets.

We have created a set of objectives (contained in section 4) that we are committed to achieving - through the following means:

- Maintenance of an ISMS that is independently certified as compliant with ISO 27001:2013
- Systematic identification of security threats and the application of a risk assessment procedure that will identify and implement appropriate control measures
- Monitoring of security threats and testing / auditing of the effectiveness of control measures
- Maintenance of a risk treatment plan that is focused on eliminating or reducing security threats
- Maintenance and regular testing of a Business Continuity Plan
- Clear definition of responsibilities for implementing the ISMS
- Provision of appropriate information, instruction and training to our employees

The appropriateness and effectiveness of this policy, and the means identified within it, for delivering DeepStream Technologies commitments will be regularly reviewed by the CEO.

The implementation of this policy is fundamental to the success of DeepStream Technologies and must be supported by all employees and contractors who have an impact on information security.

All information security incidents must be reported to the CEO. Violations of this policy may be subject to the DeepStream Technologies Disciplinary and Appeals Policy and Procedure.

The continual improvement of the Management System is fundamental to our success and must be supported by all employees. This policy is publicly available to interested external parties.

Jack Macfarlane, CEO

January 2019

3. SECURITY AND RISK GOVERNANCE

We operate a cloud-based platform using a SaaS (Software as a Service) methodology that ensures all users of our platform can engage efficiently with each other. Suppliers become pre-qualified with DeepStream, with an additional layer of network-based verification.

Security, privacy and compliance are very important to our customers and DeepStream. Customers rightly want assurance, that warm and fluffy feeling, that when they engage with other Stakeholders, their data will not be lost or compromised. This document has been designed to provide answers to many of the frequently asked questions that platform users – including IT security staff – may have.

Be assured. DeepStream Technologies used advanced technology to ensure your company information is safe and secure. We have implemented and effectively maintain an extensive suite of security controls to deliver on your security expectations – and give you that warm and fluffy feeling.

4. Information Security Objectives

Our focus, our key objective is the protection of customer data.

To support this, we have a comprehensive set of objectives set by our CEO – outlined below.

Performance vs our objectives is continually assessed and reported to our CEO.

Key Information Security Objectives:

- **Certification**
  Obtain and maintain certification to ISO 27001

- **Supplier engagement**
  Ensure contracts are in place with all information security critical suppliers

- **Engagement and communications**
  Frequent information security briefing with for all employees, including at induction

- **Control assessments**
  Quarterly information security control measures assessments

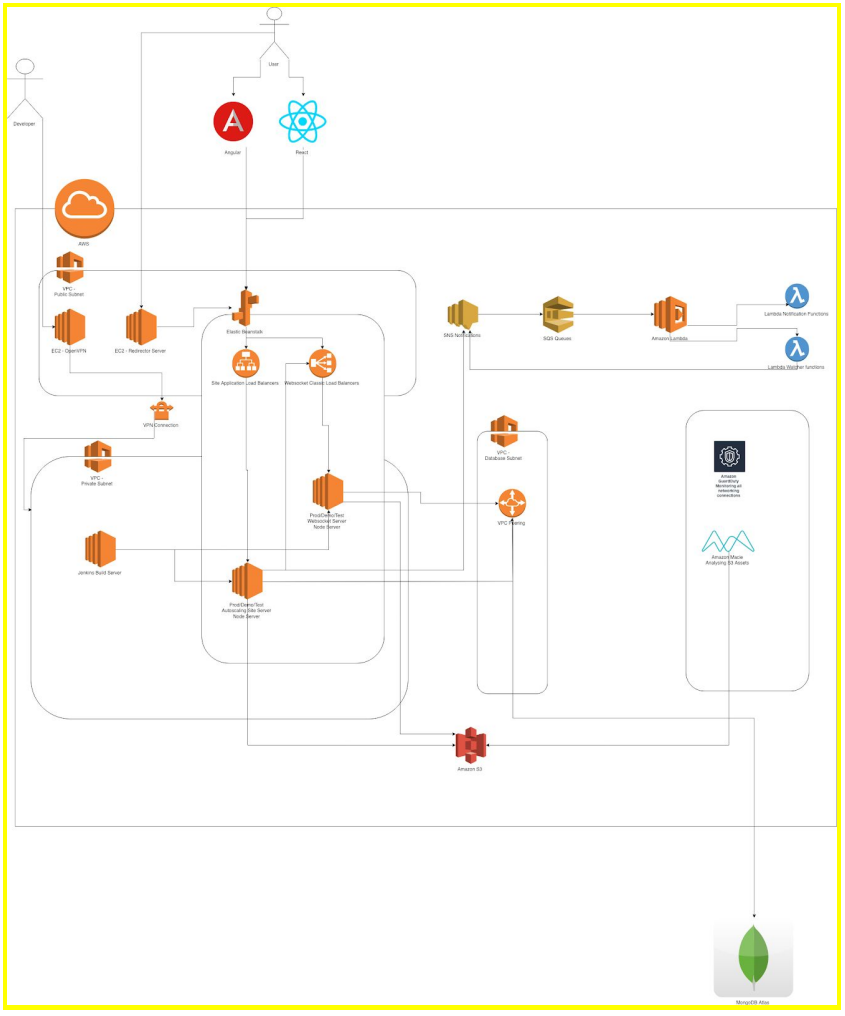
- **Security incidents / breaches**
  0 information security incidents

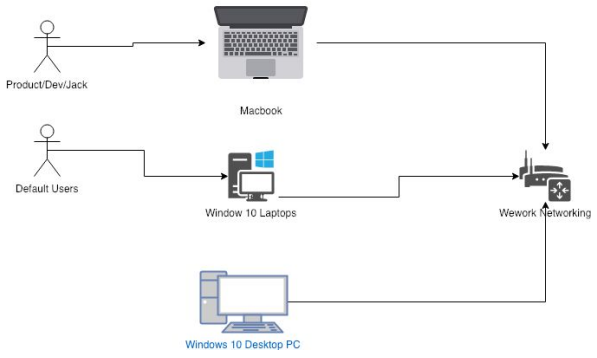
- **Legal compliance**
  Annual check of our operations vs legislative requirements – including GDPR EU 2016/679

- **Network downtime**
  To minimise the amount of network downtime

5. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

DeepStream Technologies operate a comprehensive control-based Information Security Management System (ISMS) that delivers on both your and our security expectations. Our boundaries:





The following sections provide more details on our information security controls and activities.

Physical and Environmental Security

To protect assets from physical and environmental threats (e.g. damage, theft, unauthorised access)

Physical protection of operating facilities

- All operating facilities must be secured at all times.

Environmental protection of operating facilities

- All the environmental vulnerabilities and controls associated with operating facilities are identified in the Asset and Risk Assessment Register.
- All relevant facilities are protected by suitable fire alarm systems and have a fire evacuation procedure in place.
- All systems identified as being vulnerable to power outages should be protected by uninterruptible power supplies (UPS), such as a generator or battery backup, as follows:
    - Generators have the capability to meet the requirements of the Business Continuity Plan
    - Battery backup will provide at least 30 minutes of uptime to systems
- All systems that need to be maintained in a temperature-controlled environment must be suitably located where air conditioning facilities are available that are:
    - Implemented with monitoring / backup to pro-actively alert / failsafe in the event of failure
    - Adequately maintained to ensure reliability

Protection of assets at operating facilities

- Network servers are in locations designated as restricted access as per our access controls.
- Cable / wiring locations are appropriately secured to prevent interception of data and damage to the network infrastructure.
- Hard copy files are stored in accordance with our Clear Desk and Information Classification / Labelling controls.
- Assets are maintained in accordance with manufacturers' and suppliers' recommendations.
- Restricted access must always be physically controlled to prevent unauthorised access.

Access Control

To protect assets from unauthorised access

Access to assets and facilities

- Access is only provided to individuals to performed authorised tasks.
- User access must be attributed to an identifiable person.
- No single person can access, modify or use the assets without authorisation or detection.
- Access to software source codes is restricted and monitored.
- User access to information processing facilities, mobile devices, operating facilities and restricted access areas is recorded using an Asset and Access Control Review Form.
- Individuals who enable and disable access to assets do not have access to any software that monitors the use of the asset.
- Regular review of logs of system administrator access and actions.

Control of access to information processing facilities

- Access is authorised as part of new starter induction and / or following any role changes and only once formal training has been received on relevant parts of the ISMS.
- Individual access privileges are reviewed upon a change of role or change in responsibilities.
- The status of each user's access privileges in the Access Control Register.
- Redundant user access IDs are not issued to other users.
- Expired or unused accounts are removed; tests ensure accounts are no longer accessible.
- Immediate removal of all access rights of a user upon termination of their employment contract or Supply of Goods and Services Agreement, or in the event of a security incident that relates to their access rights.
- Access to assets and information processing facilities is logged and monitored.
- Access log files are not edited or deleted.

Passwords

- All passwords must satisfy the following criteria:
    - At least 8 characters in length
    - Contain 2 of 4 character sets (upper case letter; lower case letter; number; special characters)
    - Historic passwords cannot be repeated

- Users change their passwords on initial access or if access needs to be re-established for any reason.

- Password files or data must be stored in encrypted secure areas and encrypted whilst transferred

Visitors, subcontractors and suppliers

- Are asked to sign in at reception and will be accompanied at all times
- Access will only be given as appropriate to perform the contracted tasks

Teleworking

- Teleworking is approved by the CEO.
- Teleworkers will comply with ISMS requirements (e.g. mobile devices and protection from malware controls) when connecting to DeepStream Technologies networks.
- DeepStream Technologies provided equipment for teleworking.
- Where equipment is provided to the teleworker for teleworking, the teleworker must comply with the Acceptable Use of Assets Policy, Mobile Devices Policy and Use of Software Policy.

Use of owned equipment for teleworking

- Teleworkers are permitted to use their own equipment in accordance our access controls.
- All equipment used has the current version of its operating system installed, defined as a version for which security updates continue to be produced and made available for the equipment.
- All equipment has anti-virus software installed that meets the requirements of the protection from malware controls.
- All equipment has comprehensive password protection implemented for account access, application access and screensavers
- The teleworker is responsible for ensuring the equipment is not accessed by any unauthorised person while the equipment is being used for work purposes.
- Teleworkers must take extra care when using any equipment for teleworking to protect it from theft and damage.
- The teleworker must notify the CEO of the disposal of any equipment and be willing to pass, by mutual agreement, the equipment to the CEO for the purpose of removing any of DeepStream Technologies information assets that may still reside on it.

Supplier Management

Effective engagement with our suppliers

Information security critical suppliers (ISCS)

- Use of ISCS is approved by the CEO.
- Up-to-date records relating to the status of information about ISCS security controls, certifications and key personnel are maintained in the Approved Suppliers Register.
- Information security risks identified that relate to the use of ISCS are assessed and recorded in the Asset and Risk Assessment Register.
- ISCSs must not deliver goods or services that are not covered within the scope of a current Supply of Goods and Services Agreement. The current Supply of Goods and Services Agreement must include the following information:
    - The scope of goods and services supplied by the ISCS covered by the agreement
    - The obligations of the ISCS to protect information assets in respect of availability, integrity and confidentiality
    - The obligations of the ISCS to comply with our Information Security Policy and relevant processes, policies and procedures in our ISMS
    - The minimum information security controls implemented and maintained by the ISCS to protect information assets and the arrangements for monitoring their effectiveness
    - The arrangements for reporting and managing security incidents
    - The arrangements for managing changes to any asset
    - The contact details of those responsible for information security within the ISCS
- The information security controls detailed above will include the following considerations:
    - Subcontracting of the supply of goods and services by the ISCS to third parties
    - Resilience, recovery and contingency arrangements to ensure the availability of any assets including any data processing facilities provided by the ISCS
    - Accuracy and completeness controls to ensure the integrity of assets
    - Processes and / or procedures for transferring information and/or information processing facilities between the ISCS, DeepStream Technologies and other third parties
    - Screening checks undertaken on ISCS employees and subcontractors
    - Any legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met
    - ISCS obligation to periodically deliver an independent report on the effectiveness of controls

Use of Software

The use and installation of software on assets

Use of Software

- Software must only be used in connection with authorised business use.
- Users of software must be authorised in accordance with our access controls.
- Users must not make copies of any software provided by the organisation without the express written consent of the software publisher and the organisation.

Installation of software

- Installation of software onto an asset must be authorised by the CEO and must be done in accordance with our change control procedure and backup controls.
- Users must not install, or in any way make use of, software from sources other than those provided by the organisation unless authorised to do so by the CEO.
- Any software installed must carry a valid license that covers the scope of use.

Software Development

Controls applied within the development of DeepStream Technologies' software products

Requirement identification

- Requirements are identified as part of project pre-engagement
- We will formally capture requirements to ensure all stakeholders requirements and expectations are confirmed and trackable throughout the project
- All potential work is initially captured in the sprint backlog pending the next appropriate sprint

Project definition

- DeepStream Technologies use an Agile framework / SCRUM methodology to develop software
- Work is packaged into Sprints and resources allocated to tasks
- Risks and issues per development / sprint are identified, assessed and controlled throughout the lifecycle
- As appropriate to the sprint, testing (e.g. UAT, MAT) is planned, completed and output retained

System release

- Release / multiple release iterations are planned and run as per requirements
- Jira is used to capture all changes within each release
- Prior to release, all knowledge is captured within the SCRUM as well as transferred to stakeholders as necessary
- A post sprint review should be carried out to identify potential lessons learnt and look for any opportunities to improve the next sprint

Protection from Malware

Controls applied to computer systems and mobile devices to protect them against malware threats

Installation of anti-virus software on computer systems and mobile devices

- Effective anti-virus software is installed and updated on all computer systems and mobile devices.
- All computer systems and mobile devices must not be used unless they have up-to-date and operational anti-virus software installed.
- All anti-virus software installed must have real-time scanning protection to files and applications running on the computer system or mobile device. The scanning must automatically assess the threat posed by any electronic files or software code downloaded onto a computer system or mobile device.
- All anti-virus software must be configured to ensure it can detect, remove and protect against all known types of malware.
- All anti-virus software must be configured to automatically start on device power-up and to continuously run for the duration that the computer system or mobile device is powered.
- All anti-virus software must be configured to run automatic updates provided by the anti-virus software supplier.
- All anti-virus software must be configured to conduct periodic scans of the computer system or mobile device on which it is installed.
- All anti-virus software must be configured to generate log files, and to store these log files either locally on the computer system or mobile device or centrally on a organisation-wide anti-virus server (if applicable). All logs must be kept for a minimum of 12 months.

Installation of anti-virus software on mail servers

- Mail servers must have either an external or an internal anti-virus scanning application that scans all mail destined to and from the server.
- Local anti-virus scanning may be disabled during any backup or system downtime periods if an external anti-virus application still scans inbound emails during this period.

Other processes, systems and tools to deter malware

- All computer systems and mobile devices must run the organisation's approved operating system at its latest supported version with all relevant updates and patches installed.
- Web filtering must be implemented to reduce the potential access to websites that may contain malicious code.
- Web browsers must be configured to reduce the possibility of issues arising from mobile code.

Requirements of DeepStream Technologies employees & contractors

- Any activity intended to create and/or distribute malware on an information processing facility, computer system or mobile device is strictly prohibited.

- Must not interfere with the anti-virus software installed on any computer system or mobile device.
- Must immediately report any issues, or suspected issues relating to malware and any anti-virus warnings and alerts communicated to them from a computer system or mobile device.
- Must check the authenticity of attachments/software to be installed from internet sources.
- Must not install applications that arrive on unsolicited media.

Clear Desk and Clear Screen

Controls to minimise risk arising from unauthorised access to desks, visual aids and display screens

Paper assets, visual aids and portable storage media

- Information assets held on paper or portable storage media must be stored in cabinets, drawers, etc. when not in immediate use.
- All information assets stored on visual aids should be removed from display immediately after used and before vacating the room in which they are held.

Display screens

- Equipment that utilises display screens must have a screensaver enabled with password protection that activates automatically after 5 minutes of inactivity.
- Users of company equipment that utilises display screens must enable a screensaver or lock their screen whenever they leave the room.

Reproduction devices (printers, photocopiers and scanners)

- Media used, or created using reproduction devices, must be removed from them immediately after use.

Acceptable use of Assets

Controls to minimise the risk of misuse or unauthorised use of assets

Use of electronic communication facilities (ECFs)

- DeepStream Technologies users must only use ECFs (phones, laptops, etc.) for the reasons for which they have been authorised.
- Extreme caution must be used when opening email attachments received from unknown senders.
- Users must not:
    - disclose IDs and personal passwords unless authorised by the CEO
    - introduce viruses / sources of malware into DeepStream Technologies ECFs
    - access external sources that are not authorised or access, download or store materials that are illegal, immoral, unethical or deemed to be indecent or gross in nature
    - send unsolicited, unauthorised or illegal materials to any recipient
    - install, modify, delete or remove software in a way that contravenes use of software controls
    - use any ECFs for any personal reasons, other than those authorised by the CEO
- Any user supplied equipment must be approved by the CEO for connection to any of DeepStream Technologies ECFs.
- DeepStream Technologies will right to monitor the use of all ECF.

Backup

Controls to ensure effective backups are taken of software and other information assets

- Google Drive Sync is used to create an effective backup of files and restore earlier versions of files – to support this, all files are stored in the company Google Drive Sync.
- Where backup copies are taken, they must be encrypted in accordance cryptographic controls and in accordance with the information classification, labelling and handling controls.

Storage of backups

- Any backup copies will be stored at a sufficient distance to escape any damage from a disaster at the primary site.
- Backup information is given an appropriate level of physical and environmental protection consistent with the standards applied at the primary site.
- Any third parties store and maintain backups should comply with our supplier management controls.

Testing of backups

- Backups of software and electronic files, and media used to store them, must be tested at least quarterly in accordance with the Business Continuity Plan and the Electronic Data Backup Register.

Communications

Controls to ensure internal and external communications do not compromise data

Communication with third parties

- All information security queries from third parties will be referred to the CEO.
- Any information exchanged with third parties will be in accordance with our information classification controls.

Communication with Employees

- All employee briefings on information security matters are held regularly, or if any significant issues arise or decisions are made that have consequences for employees.
- Employees are encouraged to raise any concerns they have relating to information security.
- All employees complete an information security induction programme when starting with us.

Information Classification, Labelling and Handling

Controls applied to all information assets that are processed and stored by DeepStream Technologies

Classification

- Information assets are classified according to their value, criticality, legal requirement, sensitivity.
- Rules are applied by all information asset owners, employees and third parties with whom we exchange or provides access to information assets.

Labelling

- Upon creation or receipt from a third party, all information assets will be labelled.
- Whenever information assets are modified, consideration must be given as to whether the labelling applied to it should be changed.

Copying

- The copying of all information assets should be avoided wherever possible.
- Where necessary, copying will be actioned in accordance with company Information Classification, Labelling and Handling rules.

Distribution

- Information assets should only be distributed:
    - To comply with client requirements
    - To comply with legal requirements
    - On a need to know basis
- Where necessary, distribution will be actioned in accordance with company Information Classification, Labelling and Handling rules.

Destruction

- Destruction of information assets will be actioned as per documented information controls.

Mobile Devices

Controls for the issue, use and return of mobile devices

Issuing of mobile devices

- The CEO will authorise the issue of all mobile devices

Use of mobile devices

- User of mobile devices must comply with all applicable controls in this programme overview.
- Mobile devices must only be used for their authorised business use.
- Users must immediately notify the CEO if a mobile device is known or suspected to be lost.
- Mobile devices must not be used or stored in environments or areas where there is a reasonable risk of them becoming damaged by impact, water ingress, extreme temperatures or electromagnetic fields.
- Mobile devices must be carried as hand luggage when travelling.
- Mobile devices must not be left unattended at any time in a vehicle or public place.
- Mobile devices must always be protected from unauthorised use by an access password in accordance with access controls.
- Mobile devices must not be used to store passwords, safe/door combinations, or classified, sensitive or proprietary information.

Return of mobile devices

- Upon request by the CEO, termination of contract or change of role, a user must return any mobile devices they have been issued with to the CEO.

Cryptographic Controls

Controls applied to confidential information

General principles

- All applications, systems and information processing facilities are appropriately protected to prevent unauthorised access by applying a level of encryption to sensitive or critical information which is proportionate to the level of business risk.
- All removable media, including memory sticks, must be encrypted.
- Emails should be encrypted whenever confidential information is contained or attached. Emails automatically encrypted where recipient supports TLS.
- Encryption keys must be stored such that all information encrypted can be decrypted if required.
- Access to encryption keys must be controlled as per access controls.
- All passwords are required to be stored in an encrypted vault, using the Deepstream approved password manager, 1password.

Encryption of data in transit

- Confidential information in transit should always be encrypted.

Software Password Encryption Policy

- All application passwords must be salted and hashed using industry standard algorithms.
- The number of salt rounds is to be reviewed annually.

Protection of Personal Information

Controls to protect personal information where we act as a Controller or Processor of information

General principles

- DeepStream Technologies can demonstrate compliance with all relevant legal, customer and other third-party requirements relating to the processing of personal information including The Data Protection Act 2018 and the General Data Protection Regulation EU 2016/679 (GDPR).
- The CEO is the Data Officer within the company and ensures necessary resources are in place to carry out tasks required by the legislation listed above.
- DeepStream Technologies are registered with the Information Commissioner's Office.

Personal Information protection principles

- Personal information shall be processed lawfully, fairly and in a transparent manner.
- Personal information shall be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.
- Any Personal information processed shall be accurate, kept up-to-date (where necessary) and every reasonable step is taken to ensure that Personal Information that is inaccurate with regards to the purposes for which it is processed is erased or rectified without delay.
- Personal information shall not be kept in form that permits identification of Information Subjects for longer than is necessary for purposes for the which the information is processed (Personal information may be put beyond use where deletion is not reasonably feasible).
- Appropriate technical and organisational measures shall be taken to ensure appropriate security of the personal information.
- A Personal Information Processing Register is maintained for all personal information where DeepStream Technologies act as Controller or Processor on behalf of a Controller or other Processor

Privacy Notices

- All Privacy Notices are available on the DeepStream Technologies website.
- Each Privacy Notice details the scope and justification for processing information provided, as well the rights of Information Subjects and how they can be exercised.
- Where explicit consent is needed for special case information, this will be obtained prior to processing commences.

Personal Information Breaches

- In the event of a Security Incident that compromises the confidentiality, integrity of availability of any Personal Information actions shall be taken and records maintained in accordance with the Security Incident Management Procedure.