INFORMATION SECURITY POLICY

Background

This Information Security Policy is based upon the International Standard ISEC/ISO 27001 Code of Practice for Information Security Management and ISEC/ISO 27002.

Requirements for Policy

Nimbus Hosting Ltd. (hereafter referred to as the Company) has an obligation to clearly define requirements for the use of its information technology (IT) facilities and its information systems (IS) to all staff, suppliers and partners.

The objective of this requirement is to ensure that users of IT/IS facilities do not unintentionally place themselves, or the Company, at risk of prosecution or disciplinary action, by carrying out computer related activities which contravene current policy or legislative restrictions.

Information within the Company is intended to be openly accessible and available to all members of the organisation who require access to carry out their roles. Certain information (sensitive information) has to be processed, handled and managed securely and with accountability.

This policy outlines the control requirements for all information contained within the Company network and IT systems.

Policy Structure

This document forms the Company's Information Security Policy. Its purpose is to provide an overarching framework (a commitment of undertaking) to apply information security controls throughout the Company.

Supporting policies and guidance documents containing detailed Information security requirements will be developed in support of this policy. Depending upon the subject matter, supporting policies and guidance will either apply across the Company or to more specific groups or individuals within the Company.

Purpose and Scope

All processing of data and collection of information will be processed in accordance with UK law.

This policy defines how the Company will secure electronic information within the following areas:

- The Company's IS/IT infrastructure.
- Key Business System data and information.
- Security of information held in electronic form on any Company computer.

And is processed or used by:

- Company Staff and suppliers who have access to or administer the Company network or IT systems.
- Individuals who process key data and information within Key Business Systems.

Objectives

Information Security controls are designed to protect members of the Company and the Company's reputation through the preservation of:

- **Confidentiality** – knowing that key data and information can be accessed only by those to do so;
- **Integrity** – knowing that key data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and,
- **Availability** – knowing that the key data and information can always be accessed.

The Company is committed to protecting its members and Key Business Systems. Controls will therefore be deployed that mitigate the risk of vulnerabilities being exploited which adversely affect the efficient operation of the Company.

Applicability

This policy applies to all users of the Company network and IT Services and includes:

- All full-time, part-time and temporary staff employed by, or working for or on behalf of, the Company;
- Suppliers working at the Company;
- Third party contractors and consultants working for or on behalf of the Company;
- All other individuals and groups who have been granted access to the Company's network, data or IT Services.

These categories of persons and agencies are collectively known as the 'user' in the Policy document.

The Directors of the Company are ultimately responsible for ensuring that adherence to this policy is observed and for overseeing compliance by users under their direction, control or supervision.

Each user is responsible for their own actions and must ensure all actions relating to using the Company network and IT Services adheres to the principles and requirements of this policy.

1. Legislation and Policy

Legislation

Supply and use of the Company network and IT Services are bound by UK law.

Associated Policies

The Company is also governed by external policies that impose responsibilities on the provision of IT Services and network access.

The principles in this policy support and enhance the requirements contained within these documents, ensuring compliance with contractual agreements.

2. Information Security – Risk Management

Information security governance is the structure which supports the implementation of this policy. An IT infrastructure will be implemented within the Company to ensure the effective and efficient implementation of this policy across the Company.

Ownership and Maintenance of Policy

This policy is owned by the Company and is maintained, reviewed and amended by the board in accordance with Company policy, procedures and guidance. This policy will be subject to annual review.

Risk Management and Electronic Service Incidents

The Company will raise an incident report for any reported security incident.

These incidents will be recorded as 'Electronic Security Incidents'.

Electronic Security Incidents will be recorded with a unique reference number. Incident reviews will be conducted monthly..

Incidents posing unacceptable risk levels to the Company network or IT services will be investigated to identify inherent vulnerabilities

A report will be submitted to the Information Security Management Team for consideration and implementation of suitable remedial actions to mitigate future risks.

Security of Third-Party Access

Procedures will be developed to regulate third-party access to the Company's information processing facilities.

This access will be controlled to protect information assets and prevent data loss and damage as well as unauthorised access

The IT Manager will consider applications for access to facilities by contractors or third parties based upon a risk assessment of the proposed task.

Identification of Risk from Third-Party Access

Third parties who require access to the Company's IT/IS infrastructure will be bound by contracts which define Company security requirements.

Prior to being granted any network connectivity, they will be required to sign and undertaking to adhere to the requirements of the Company policy, and where sensitive information or sensitive business/research information is involved, they will be required to sign a non-disclosure agreement prior to access to the IT network.

3. Asset Clarification

Information assets will be categorised and recorded to enable appropriate management and control.

Inventory of Assets

The Company will maintain an inventory, subject to audit, IT-related assets.

For each item, the inventory will state:

- Item's description
- Make
- Model
- Serial number and/or service tag
- Location.

This inventory is in addition to asset records maintained under Company financial regulations.

Any system and the data it contains that is not part of the above inventory is the responsibility of the creator of that system.

However, the asset will require compliance with this policy and users will be required to adhere to the principles of this document.

All asset identification procedures must be compliant with and support the Company Business Continuity Plan.

4. Personnel Security Issues

Roles and Access Levels

Controls will be deployed to reduce the risks of:

- human error
- theft
- Fraud
- nuisance or malicious misuse of facilities.
- The Company maintains a directory of people and suppliers authorized to use the Company network, IT services, and applications. All users, staff, suppliers, external users, and guest users must:
    - Certify that they agree to the terms of this policy
- If a user's relationship with the Company changes due to a new role or employment relationship, their access level must:
- Match the new role and relationship with the Company

    All IT account access levels must comply with the requirements of the Company policy.

Training

All staff will receive training on this policy, including:

    - New starters as part of the induction process
    - Further training at least every 12 months or whenever there is a substantial change in the law or associated policy and procedure
- Initial training will be provided through seminars, with subsequent sessions delivered via a suitable method.
- Completion of initial training is mandatory before any access to Company IT systems is granted. Ongoing training is required for continued employment at the Company.
- The board will:
    - Continually monitor training needs

  - Encourage employees to request or recommend further training on any aspect of relevant law, information management, and security policy, or associated procedures.

Security in Job Descriptions:

- Security roles and responsibilities will be included in job descriptions where appropriate, including:
- Specific responsibilities for the protection of particular assets
- Execution of particular processes or activities such as data protection

5. Confidential Personal Data

Sensitive Information

All data that identifies any individual will be handled in accordance with the Data Protection Act 1998. Personal details will be held securely and in accordance with current UK legislation.

- All data classified as sensitive data will be processed and stored in compliance with current sensitive information guidelines and Company policies and procedures.
- There are restrictions on international transfers of personal data. You must not transfer personal data:
  - Internationally at all OR
  - Outside the EEA (which includes the EU, Iceland, Liechtenstein, and Norway) OR
  - Other than within the EEA (which includes the EU, Iceland, Liechtenstein, and Norway), Switzerland, Hungary, or, in some cases, Canada without first consulting the Board.

Confidentiality Undertaking:

All suppliers, members of staff, and partners are reminded of their obligation to protect confidential information in accordance with the Company's standard terms and conditions of employment. All users will be bound by the confidentiality agreement in either their contract or terms of employment.

Employee Responsibilities:
All staff (including agency and casual staff) must agree to written terms and conditions contained within the Company policies when they register to use an IT service.

- The Company shall ensure that:
    - Confidentiality agreements form part of the terms and conditions of employment.
    - Awareness training about electronic information security forms part of Company staff induction programs.
    - Information for all staff on electronic information security is maintained in the Company information.

Staff Leaving Employment:
On termination of employment with the Company, any applicable user accounts, accesses, and passwords will be changed or removed. Except where a strong business case exists, which meets the needs of the Company, all user accounts will be closed at the termination of employment. Files and folders will be deleted shortly after the user leaves the Company.

6. Responding to Security Incidents

Suspected Security Breach:
Staff or suppliers using or administering the Company network or IT Services must not, under any circumstances, try to prove or collect evidence in relation to any suspected or perceived security breach.

The exception to this rule is where staff has been granted a specific policy exemption which allows them to do so as part of their role. A Director will be responsible for identifying members of staff who are responsible for security breach investigations.

- A security incident is any incident that:
  - Alters, destroys, or amends data within the Key Business Systems without authority.
  - May cause damage to or reduce the efficiency of the Company network or IT Services.
  - Contravenes Company policy, statutory or common law, legal requirements, or professional regulation or guidance.

Reporting Security Incidents:
All suspected security incidents are to be reported in the first instance to Tim Dunton. All reported security incidents and active investigations will be monitored by the Information Security Management team. An appropriate investigation and action plan will be prepared and agreed upon.

- Within the provisions of UK Law, the Company reserves the right to:
  - Intercept and monitor communications in accordance with the Regulation of Investigatory Power Act and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations.
  - Implement the above legislation in compliance with the Company monitoring provisions.
  - Monitor and record electronic communication and data in accordance with current Company Policy.
  - Intercept/monitor individual activity with prior express approval of the Company Directors, or without prior notice if deemed necessary.

Permission for undertaking monitoring or surveillance of user activity may initially be given verbally, but must be recorded in writing as soon as practical. This requirement ensures an auditable investigatory process exists for any subsequent disciplinary or criminal proceedings.

Security Incident Management / Investigation:
The Information Security Management team member responsible for

investigating the incident will ensure all steps are taken to limit damage and loss of data while preserving the reputation of the company.

- The IT Manager will maintain written procedures for the operation (e.g., start-up, backup, and change control) of Company Key Business Systems where threat, risk, and organisational impact would adversely affect operational effectiveness or reputation.

Investigating Information Security Incidents:
Upon receiving information indicating that a security incident may have taken place, the Information Security Management team will nominate a member to coordinate the investigation.

Network Isolation and Reconnection:
Any device perceived as placing the integrity of the Company IT network at risk of harm or service interruption will be isolated from the main network.

- Suspension of network connectivity will remain in force until the issue has been:
    - Investigated
    - A plan of action agreed upon with the IT Manager
- Subsequent reinstatement will only be permitted once the requirements of that action plan have been met, verified, and authorized by the IT Manager.

7. Physical and Environmental Security Controls will be implemented as appropriate to prevent unauthorised access to, interference with, or damage to information assets.

Physical Security:
Computer systems and networks will be protected by suitable physical, technical, procedural, and environmental security controls. File servers and other systems that hold or process high criticality, high sensitivity, or high availability data will be located in a suitable area. All Key Business Systems will be subject to security measures which support the Company Business Continuity Plan.

Data Storage Facility Security:

Access to the offices and server rooms and any locations containing data communications or telephone equipment will be controlled and restricted. Authority to access these areas will be managed by the IT Manager.

Equipment Security:
Servers holding corporate information will be held in a secure environment protected by:

- Physical security and access control
- Fire detection and extinguishing systems (as deemed appropriate by a risk assessment)
- External hosting of data must not take place without prior approval from the Board
- The IT Manager must ensure the IT infrastructure is covered by appropriate hardware and software maintenance and support
- Workstations must be appropriately secured and operated by Company staff who must be trained in and fully conversant with this policy and their personal responsibilities for the confidentiality of information displayed on the screen or in printed output
- Backup media must be retained in accordance with the Company Policy on retention of records and the Data Protection Act 1998
- All Company data must be cleared securely from Company IT equipment and media on disposal. The responsibility for disposal lies with the IT Manager

8. Communications and Operations Management

Controls will be implemented to enable the correct and secure operation of information processing facilities.

Documented Operating Procedure:
Design, build, and configuration documentation will be produced for system platforms. Sensitive documentation will be held securely, with access restricted to staff on a need-to-know basis.

Segregation of Duties:
Access to Key Business Systems and key data and information will only be granted based on the user role and access classification. When deemed

necessary, segregation of duties between operations and development environments will be strictly maintained, ensuring that all work on Key Business Systems is segregated.

- Permanent and full access to live operating environments will be restricted to staff based on role requirements.
- Sensitive operations will be identified, and action will be taken to implement split functional controls where appropriate.

9. System Planning and Acceptance

System Changes:

All changes to live Key Business Systems will follow a predefined change management process. This ensures that activities are undertaken in accordance with stringent change control processes.

Controls Against Malicious Software:

Controls will be implemented to check for malicious or fraudulent code being introduced to Key Business Systems. All systems will be protected by a multi-level approach involving firewall, router configuration, email scanning, and virus and spyware/malware protection on all workstations on the Company network.

- All Company workstations will have appropriate anti-virus software installed and set up to update anti-virus signatures automatically. This must not be turned off by users with unlocked desktops.
- Any device found to pose a threat to data or the Company network will be isolated from the network until the security issues are resolved.
- Staff and suppliers may use their own PC hardware to connect to the Company guest Wi-Fi network. Any equipment wishing to join the Company network will be subject to security checks and prerequisites before being allowed to establish a connection.
- Network traffic will be monitored for any anomalous activity that may indicate a security threat to the network.

Virus Protection:

A virus protection procedure will be implemented to prevent the introduction and transmission of computer viruses both within and from outside the Company. Failure to maintain a device in a state which prevents or detects virus infection will leave the device liable to exclusion from the Company network until the security issue is resolved.

Security Patches, Fixes, and Workarounds:
The IT Manager will be responsible for the day-to-day management of systems. System backups will be performed automatically by the relevant systems or manually by staff in accordance with documented procedures.

- The procedure will include keeping backups off-site. Periodic checks will be made to ensure backup media can be read and files restored. Records of backups will be monitored by the IT Manager and be subject to random audits.
- The IT Manager will ensure that security patches, fixes, and workarounds are applied in a timely manner to reduce vulnerabilities within the Company network.
- Such patches, fixes, and workarounds must be tested and approved before deployment. The efficiency of the deployment will be monitored to ensure the effective mitigation of risk due to known vulnerabilities.

10. IT Housekeeping and Storage

Data Storage:
Backups protect electronic information from major loss or failure of system software and hardware. However, backups are not designed to guard against accidental deletion or overwriting of individual user data files. The backup and recovery of individual user files is the responsibility of the information owner.
Network Management:
Controls will be implemented to achieve, maintain, and control access to computer networks, including wireless LANs.

- No IT equipment may be connected to the Company network without approval. Any device found to be installed without prior authority will be disconnected, the equipment removed, and an investigation commenced to establish the cause of the network compromise.

- Users should be aware that the installation of such devices is potentially a disciplinary and criminal offense under the Misuse of Computers Act 1990.

Devices Disposal:
Removable magnetic and optical media containing Key Business System data or Sensitive Information will be reused or disposed of through controlled and secure means when no longer required, in accordance with the Disposal of IT Equipment Advice.

- Redundant computer equipment will be disposed of in accordance with the Waste Electrical and Electronic Equipment (WEEE) Regulations and through secure and auditable means.
- Procedures will be made available for the secure disposal of removable data storage media containing Key Business System data or sensitive information when these become defunct or unserviceable.

Software Usage and Control:
Software will be used, managed, and controlled in accordance with legislative and Company policy requirements in relation to asset management and license agreements.

- All major software upgrades and in-house systems development for Key Business Systems will be appropriately controlled and tested through a managed process before live implementation and deployment.
- All software used on devices managed by the Company must be installed in compliance with current software licensing policies.
- Software installed without prior authority and agreement may leave a user liable to prosecution under the Misuse of Computers Act 1990 and disciplinary action.

Information Exchange Requests:
Use of the Company network will be governed by the Information Security Policy and the Policy for using IT Resources. Failure to comply with these

requirements will leave a user liable to disciplinary and/or possible criminal legal penalties.

Exchange of Information with Outside Organisations

Requests by external bodies for the provision of electronic information from Key Business Systems will in all instances be referred to the information owner. This includes Data Subject Access Requests made under the auspices of the Data Protection Act 1998.

- Requests for information under the Freedom of Information Act will be referred to the Company Directors. All applications will be handled in accordance with the FOI Application Procedure.
- Confidential information must not be removed from our offices without permission from the Board, except where that removal is temporary and necessary (e.g., for attendance at court, client meetings, or at a conference with counsel).
- In such circumstances, all reasonable steps must be taken to ensure that the integrity of the information and confidentiality are maintained. This will include (but not be limited to):
  - Not transporting files in see-through or other unsecured bags or cases
  - Not reading files in public places (waiting rooms, cafes, trains, etc.)
  - Not leaving files unattended or in any place where they are at risk (e.g., in conference rooms, car boots, cafes, etc.)
- Postal, document exchange (DX), fax, and email addresses and numbers should be checked and verified before information is sent to them. Particular care should be taken with email addresses where auto-complete features may have inserted incorrect addresses.
- All sensitive or particularly confidential information should be encrypted before being sent by email, or be sent by tracked DX or recorded delivery.
- Sensitive or particularly confidential information should not be sent by fax unless you can be sure that it will not be inappropriately intercepted at the recipient's fax machine.

Home working

Confidential or other sensitive information may only be taken to your home with the permission of the Board. The Board will grant permission if they are satisfied that you have appropriate technical and practical measures in place to maintain the continued security and confidentiality of that information.

- No confidential information is to be stored on any home computing device (PC, laptop, or tablet).

Confidential information (both electronic and physical) must be kept in a secure and locked environment where it cannot be accessed by family members or visitors

11. Access Control

Procedures for the registration and deregistration of users and for managing access to all information systems shall be established to ensure that all users' access rights match their authorisations.

User Responsibilities:

Users of the Company network must comply with Company Policies and the Information Security Policy. All staff (including agency and temporary staff) must agree to written terms and conditions covering the use of IT when they register to use Company IT services.

- The HR function within the Company shall ensure that:
  - Confidentiality Agreements form part of the terms and conditions of employment
  - Awareness training about electronic information security forms part of Company Staff Induction Programs
  - Information for all staff on electronic information security is maintained in the contract of employment and staff handbook
- The Company must ensure that specific security roles and responsibilities are documented in all relevant job descriptions and that there is appropriate screening of applicants.
- Access to Company systems may be withdrawn and Company disciplinary procedures invoked where a serious or deliberate breach of the policy is made.

Guest Users and Open Access:
Guest user accounts and open access facilities may be used to allow visitors strictly limited access to public Company IT. Written records of such IT use (who, when, and where) must be maintained by the Company.

- Access to corporate systems-protected electronic resources, Company email services, and personal file stores will not be permitted for guest users.

12. Company Key Business System Access

Subject Access Management and Administration:

Formal procedures will be implemented for granting access to both the Company network and IT services. This will be supported by a formal review of user privileges on a regular basis to ensure that they remain appropriate to the role and relationship with the Company.

- Accounts identified as dormant will be closed in accordance with current procedures.

Remote Access:
Controls will be implemented to manage and control remote access to the Company’s network and IT services. Users should note that failure to comply with Company policies will leave the user liable to disciplinary action and possible criminal law prosecution under the appropriate legislation.

Mobile Computing:
The Company recognises the inherent dangers of information stored on portable computers (laptops, notebooks, tablets, and smartphones) as well as removable media.

- The Company will provide security advice to staff as requested. The advice is issued as a guideline for users, and failure to follow recommended guidance will leave a user vulnerable to disciplinary action should Key Business System Data or sensitive information be lost or altered.

Password Management:
Users are required to follow good security practices in the selection, use, and management of their passwords and to keep them confidential. Primary access to Company IT services is governed by username and password giving access to the set of services.

- System administrator passwords will be issued on the express authority of the Managing Director on a need-to-know basis. Such passwords will be changed regularly and when authorized systems administrator staff leave.
- For all Company-issued IT equipment, the following password requirements must be observed:
    - Passwords must be a minimum of seven characters, which must include 3 of the following 4: lowercase, uppercase, numerical, and non-alphabetic characters.
    - Passwords should be subject to periodic change. The life of a chosen password will be 60 days.
    - Reuse of the last 12 password changes is not allowed.
    - Accounts should be locked on the third failed login attempt.
- The policy on password complexity will be reviewed periodically and in line with current industry guidance.
- Passwords for all third-party services should meet the above complexity requirements, using 2FA where possible. The Nimbus company 1Password vaults can be used for shared accounts; the vault password needs to be extremely complex.
- The Information Security Manager must be notified when staff leave and will be responsible for closing the associated accounts.
- The account type should at all times reflect the business relationship existing with the member of staff. As a staff member moves to a less formal relationship with the Company, the account associated with that person should reflect this new relationship.
- The Company will maintain a list of staff with access to key business systems and services. A password matrix will be maintained to ensure business continuity and mitigate risk. This password matrix will be kept securely to ensure a swift response to critical incidents.

Unattended User Equipment:

Users of the Company network and IT services are responsible for safeguarding Key Business System Data and sensitive information. In order to protect these information assets, users are required to ensure that devices are not left logged on when unattended and that portable equipment in their custody is not exposed to opportunistic theft, unauthorised access, or observation of sensitive information.

- Where available, password-protected screensavers and automatic logout mechanisms are to be used on office-based systems to prevent individual accounts from being used by persons other than the account holders, but not on cluster computers that are shared by multiple users.
- Users should utilise the following security features of the system:
  - Logging out of sessions when the session is finished
  - Locking desktop sessions when a computer is to be left unattended
  - Whenever possible and at the end of the working day, switching off computers when not in use
- Users are required to follow the guidance on user responsibilities and Personal Responsibilities for Information Security.
- Failure to adhere to these recommendations could leave the Company or user liable to possible disciplinary or criminal prosecution.

13. Monitoring Systems Access and Use

Access to and use of the Company network and IT systems will be monitored in accordance with the provisions of the Policy for Using IT Resources.

Remote Access by Third-Party Contractors:

Remote access by third-party contractors to maintain and support Company IT systems will be subject to appropriate monitoring and control measures defined by IT services.

Third-Party Access:

Third-party access will only be granted where the applicant has agreed to the terms and conditions of the ICT Acceptable Use Policy.

14. Compliance

Compliance with Legal and Company Policy:

Supply and use of the Company network and IT services are bound by UK law current at the time of any reported incident. The Policy for Using IT Resources provides guidance on the most common legal and policy requirements pertaining to Company network use.

Guest Users:

- Guest users may be permitted limited rights to use IT services.
- The Company will review this policy periodically.

Monitoring and Reporting:

- The Information Security Manager will maintain and monitor, at six-monthly intervals, reports of electronic security incidents.
- Reports will be considered by the Board, which will then decide if further action or investigation is required.

Password Matrix:

- The IT services password matrix, listing members of staff with access to key systems and services, will be maintained by the Information Security Manager.
- The master copy of the password matrix will be held in a secure public folder.

External Users:

- People who are neither staff nor suppliers do not normally have an automatic right to use the Company network or IT services.

- Authorisation for such external users will be subject to sponsorship from a member of Company staff and written agreement from the user to abide by Company policies.
- All applications for external users will be subject to approval by the Company Directors or a nominated representative.

Outsourcing:

Any outsourcing must include express provisions with respect to IT security and control, and comply with applicable UK law in relation to data processing and confidentiality.

[End of Document]