INFORMATION SECURITY POLICY

NIRAS-LTS International (hereafter NIRAS-LTS) operates an information system to store and process confidential and non-confidential data required for NIRAS-LTS management and operations.

NIRAS-LTS does not store, copy, disclose, or use client data except as necessary for the performance of our obligations under contract or as otherwise expressly authorised in writing. Client data that we collect or process in the delivery of our contract can be made available to the client at any time and we take responsibility for preserving the integrity of client data and preventing the corruption or loss of client data.

This IT and data security policy helps us:

- Reduce the risk of IT failure
- Plan for problems and deal with them when they happen
- Keep working if something does go wrong
- Protect company, client and employee data
- Keep valuable company information, such as plans and designs, confidential
- Meet our legal obligations under the General Data Protection Regulation (GCPR) and other laws
- Meet our professional and contractual obligations towards our clients and customers.

IT and data security problems can be expensive and time-consuming to resolve. We take an approach based on the assumption that prevention is much better than the cure.

1 Responsibilities

The Managing Director has overall responsibility for information security.

The Support Services team has day-to-day operational responsibility for IT matters and responding to questions, suggestions or feedback.

IT planning, maintenance and support is managed in collaboration with our specialist IT operation teams within the NIRAS Group.

Effective security is a team effort requiring the participation and support of everyone. It is your responsibility to know and follow these guidelines. You are personally responsible for the secure handling of confidential information that is entrusted to you. You may access, use or share confidential information only to the extent it is authorised and necessary for the proper performance of your duties. Promptly report any theft, loss or unauthorised disclosure of protected information or any breach of this policy to the Managing Director.

2 Principles

2.1 Information classification

We only classify information which is necessary for the completion of our duties. We also limit access to personal data to only those that need it for processing. We classify information into different categories so that we can ensure that it is protected appropriately. The categories are:

- **Unclassified.** This is information that can be made public without any implications for the company, such as information that is already in the public domain.

- **Employee confidential.** This includes information such as medical records, contact details, contracts and pay of our employees.
- **Company confidential.** This includes information such as contracts, source code, business plans, passwords for critical IT systems, client contact records, accounts etc.
- **Client confidential.** This includes personally identifiable information such as name or address, passwords to client systems, client business plans, new product information, market sensitive information etc.

Personal data are found in employee confidential, company confidential and client confidential folders. Files are not marked individually, but classified by virtue of their location. For this reason, NIRAS-LTS staff are given clear guidance on these categories.

2.2 Access Controls

Internally, as far as possible, we operate on a 'need to share' rather than a 'need to know' basis with respect to company confidential information. This means that our bias and intention is to share information to help people do their jobs rather than needlessly raise barriers to access.

As for client information, we operate in compliance with the GDPR 'Right to Access'. This is the right of data subjects to obtain confirmation as to whether we are processing their data, where we are processing it and for what purpose. Further, we shall provide, upon request, a copy of their personal data, free of charge in an electronic format.

However, in general, to protect confidential information we implement the following access controls:

- **Company confidential.** This information is restricted to the Executive Team through restricted access to folders on the shared drive.
- **Client confidential.** This tends to be on a project specific basis and is restricted to certain project team members.
- **Employee confidential.** The HR manager, Finance Team and Company Directors have access to the Personnel folders of staff members and staff can request access to their personal data at any time.

In addition, admin privileges to company systems will be restricted to specific, authorised individuals for the proper performance of their duties. Under the GDPR, where a data breach is likely to result in a 'risk for the rights and freedoms of individuals' we must notify the data subjects and the Information Commissioners Office (ICO) 'without undue delay'. We will ensure we inform the data subject within 72 hours and report to the ICO.

2.3 Employees joining/leaving

When a new employee joins the company, we provide them with a company email address and access to the company systems and include them into relevant email groups. Access for sub-contractors and project staff may be granted at a more restricted level.

We provide training to new staff and support for existing staff to implement this policy. This includes an initial introduction to the Information Security Guidelines, covering the risks, basic security measures, company policies and where to get help. All staff receive training on how to use company systems and security software properly.

When people leave a project or leave the company, their access to all company systems and IT is terminated.

2.4 Backup, disaster recovery and continuity

NIRAS-LTS servers are located on a science park with 24-hour security service, entry barrier, and doors requiring electronic passes to gain entry. Data is backed-

up continuously throughout the day, and the back-ups are managed and stored off-site by the NIRAS Group.

In the case of potential interruptions to our business we hold our business email on the cloud which can be accessed anywhere and anytime, and our off-site backups can be restored within 48 hours.

Patrick Abbot

Managing Director, NIRAS-LTS International

5th November 2020