# Lighthouse Dental Practice

# **Network Security Policy**

This Network Security Policy is the overarching policy for data security and protection for Lighthouse Dental Practice. It shows the protection of confidentiality, integrity and availability of the network, establishes responsibilities for network security and provides reference to documentation relevant to this policy and applies to all staff, including temporary staff and contractors.

Lighthouse Dental Practice’s information network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information.

The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this we undertake to:

* Protect all hardware, software and information assets under its control;
* Provide effective protection that is commensurate with the risks to its network assets;
* Implement the Network Security Policy in a consistent and timely manner;
* To comply with all relevant legislation.

This policy applies to our networks which are used for:

* The storage, sharing and transmission of clinical and non-clinical data and images;
* Printing or scanning clinical and non-clinical data or images;
* The provision of internet systems for receiving, sending and storing clinical and non-clinical data or images.

## **Risk assessments**

We carry out security risk assessments in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network that are used to support those business processes.

The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

## **Physical & environmental security**

Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.

Mohamed Elbadri is responsible for ensuring that door lock codes are changed periodically, following a compromise of the code, if he suspects the code has been compromised.

Critical or sensitive network equipment will be protected from power supply failures, intruder alarms and fire suppression systems.

Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

Reception staff are responsible for authorising all visitors to secure network areas and for making visitors aware of network security requirements. Visitors are required to log in and out, which will contain name, organisation, purpose of visit, date, and time in and out. Receptions are also required to inform all relevant staff of procedures for visitors and make sure the visitors are escorted, when necessary.

## **Access control to secure network areas**

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it.

Mohamed Elbadri will maintain and periodically review a list of those with unsupervised access.

## **Access control to the network**

Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network will conform to the Remote Access Policy.

Third party access to the network will be based on a formal written contract. All third-party access to the network must be logged.

## **External network connections**

We will ensure that all connections to external networks and systems have documented and approved System Security Policies.

Mohamed Elbadri must approve all connections to external networks and systems before they commence operation.

## **Maintenance contracts**

Mohamed Elbadri will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment.

All contract details will constitute part of the Information Asset register (IAR).

## **Data & software exchange**

Formal agreements for the exchange of data and software between organisations must be established and approved by Mohamed Elbadri

All exchanges of data between organisations will be recorded on the Record of Processing Activities (ROPA).

## **Fault logging**

Mohamed Elbadri is responsible for ensuring that a log of all faults on the network is maintained and reviewed. A written procedure to report faults and review countermeasures can be located on the Practice policies google drive.

## **Security & Network operating procedures**

Our security operating procedures are in a separate policy located on the practice’s google drive. Changes to operating procedures must be authorised by Mohamed Elbadri.

## **Data backup & restoration**

Data backup procedures are outlined in the Emergency and Business Continuity Plan document.

## **User responsibilities, awareness & training**

Wewill ensure that all users of the network are provided with the necessary security guidance, awareness and training to discharge their security responsibilities. These procedures will be outlined in the staff handbook.

## **Accreditation of network systems**

Mohamed Elbadri is responsible for ensuring that the network does not pose an unacceptable security risk to the organisation. They will require checks on, or an audit of, actual implementations based on approved security policies.

## **Malicious software**

We will ensure that measures are in place to detect and protect the network from viruses and other malicious software.

## **Secure disposal or re-use of equipment**

We will ensure that where equipment is being disposed of all data on the equipment (e.g. on hard disks or tapes) is securely overwritten/ disposed of appropriately with certificates provided.

## **System change control**

Mohamed Elbadri isresponsible for updating all relevant Network Security Policies, design documentation, security operating procedures and network operating procedures.

## **Reporting security incidents & weaknesses**

All potential security breaches must be investigated and reported to the Data Protection Officer and an Information Security Incident Report Form must be completed.

We will follow the procedures set out in the Data Security Policy.

## **Business continuity & disaster recovery plans**

We will ensure that business continuity plans are produced for the network and reviewed/ tested on a regular basis.

|  |  |
| --- | --- |
| Name | T Hale |
| Date | 16.03.2021 |
| Review Date | 16.03.2022 |