optos®
Building *The* Retina Company

Queensferry House
Carnegie Campus
Enterprise Way
Dunfermline
Fife, KY11 8GR
UK

Contents

1. Introduction

This document outlines the Technical and Organisational Measures that Optos currently have implemented with regards to information systems and data security.

2. Organisation of Information Security

Objective: An overview of Optos current security configuration:

a) Optos employs trained/certified Staff responsible for information security.
b) The information security function reports directly to the Optos senior leadership team.
c) Optos has a comprehensive set of information security policies, approved by senior management and disseminated to all staff.
d) All applicable Staff have signed legally reviewed confidentiality agreements.
e) All Optos staff are given training in information security when inducted into the company.

3. Information Security Management

Optos has internal policies and procedures in place to ensure staff adhere to the controls outlined in the management of internal and external data security.

4. Physical Access

Objective: To protect the physical assets that contain Customer Data.

Measures:

a) All Optos facilities are secured via centralised access control systems, using RFID passcards controlled by a WinDSX control system, complete with magnetic locks, anti-passback and IR detectors where appropriate.

b) All Optos offsite datacentres are sited within industry standard facilities with multiple identification requirements, mantraps, biometric security and named-user only access.

c) All production datacentres undergo rigorous third-party audits to maintain their certification(s)

d) The production datacentres and their equipment are physically protected against natural disasters, unauthorized entry, malicious attacks, and accidents.

e) All Optos facilities are provided by as many redundant power and telecommunications links as are practical for the specific locations.

f) Production-Line and assembly areas, stock management areas, are very strictly controlled with access restricted to named staff only.

5. Systems Access

Objective: To protect the access to physical assets that contain Customer Data.

a) Access to Optos systems is restricted to Optos staff only, and/or subcontractors as deemed appropriate by Optos.

b) All Optos users authenticate using unique credentials to allow effective auditing

c) Optos has defined a robust password policy to ensure user passwords are adequately secure, require periodic changing and to prevent password re-use.

d) Access to Optos systems from outside of Optos facilities is secured via a secure VPN, requiring authentication.

e) Optos has well defined procedures for the handling of users and their systems access during both the onboard and departure processes.

6. Data Access

Objective: To ensure Customer Data is not read, copied, altered or deleted by unauthorized parties during transfer/storage

a) All customer facing, and distributor portals are secured using current SSL/TLS technology.
b) All access into CRM systems and order processing systems is logged for audit compliance and access control.
c) Only Optos staff who require the use of CRM and customer-data containing systems are granted access to such systems.

7. Data Transmission/Storage

Objective: To ensure Customer Data is not read, copied, altered or deleted by unauthorized parties during transfer/storage.

a) All critical external facing websites are secured with SSL/TLS and Digicert provided certificates.
b) Optos uses TLS encryption for all email transmissions, regardless of content.
c) All customer access into Optos systems is secured by individual customer logins.
d) In full compliance with GDPR and other applicable legislation, with alteration/deletion requests promptly handled.
e) Optos hardware having contained customer data is wiped or destroyed prior to exiting Optos ownership, with proof of adequate destruction being retained.

8. Confidentiality and Data Integrity

Objective: To ensure Customer Data remains confidential throughout processing and remains intact, complete and current during processing activities.

a) As part of the induction process, all Optos staff understand and sign the acceptable use and security policy agreements.
b) All Optos products go through rigorous validation and verification processes, with a centralised change management and tracking system.
c) Optos has a secure central repository for source code, with access to the system restricted to appropriate users only.
d) All changes to Optos product hardware is strictly controlled and documented through the approval process/validation.
e) All customer-critical systems are monitored 24x7 for system health and functionality via a variety of monitoring tools.
f) Optos backs up critical data on its corporate systems on a regular basis, with integrity checks and periodic test restores to ensure system stability.

9. Availability

Objective: To ensure Customer Data is protected from accidental destruction or loss, and there is timely access, restoration or availability to Customer Data in the event of a service incident.

a) Optos protects customer data and operational systems by storing these in geographically separate facilities.
b) Each Optos datacentre facility has multiple redundant links to other sites, the internet and power grid.
c) Optos has a comprehensive disaster recovery and backup plan, enabling rapid recovery and business continuity in the event of a major incident.
d) Optos undergoes annual auditing to ensure the integrity and availability of customer data containing systems.

10. Data Separation

Objective: To ensure each Customer's Data is processed separately and to avoid cross contamination.

a) Optos separates customer healthcare data and non-customer data onto specific systems, to ensure customer healthcare data is never exported or transferred inadvertently.
b) Customers utilizing the Optos online image storage systems only have access to their own data, secured by unique login to prevent inadvertent exposure of sensitive information.

11. Incident Management

Objective: In the event of any security breach of Customer Data, the effect of the breach is minimized, and the Customer is promptly informed.

a) In line with all relevant legal requirements, Optos maintains an up to date incident response and disclosure plan.
b) In the event of a breach or incident, Optos will inform customers and relevant bodies as required by current legislation.

12. Audit

Objective: To ensure the Optos document, maintain and follow their stated policies and procedures which protect data.

a) Optos undergoes regular third-party audits, to ensure both business compliance and information security adherence.
b) Optos conducts regular internal audits of its practices.
c) Optos have policies and procedures in place to ensure staff are aware of and comply with these measures.
d) Optos conducts independent 3rd party testing on its network infrastructure.