



SilverCloud

MAKING SPACE FOR HEALTHY MINDS

Information Security

October 2019 – UK



1. INTRODUCTION 2

1.1 ISO/IEC 27001.....2

1.2 OBJECTIVE OF THE ISMS2

1.3 ISMS POLICY3

1.4 SECURITY OF SILVERCLOUDHEALTH.COM3

1.5 DATA PROTECTION4

1.6 AUDITS AND ASSESSMENTS.....4

1.7 POLICIES.....5

1.8 SUPPLIERS5

1. Introduction

This document is intended to provide SilverCloud Health customers (or prospects which have executed a Mutual Non-Disclosure Agreement (MNDA) with SilverCloud Health) with a statement about information security policy and a summary of key security information about the platform, along with the Certificate of Approval issued by Certification Europe.

SilverCloud Health has received a certificate of compliance with the ISO/IEC 27001:2013 standard for Information Security Management Systems. The initial date of certification was 14th August 2013. The certification is valid until 4th August 2022, subject to assessment through an on-going surveillance programme.

These documents are provided as evidence of our certification and are not to be published, shared or disclosed except to those parties who are under MNDA with SilverCloud Health. Any questions regarding information security and governance or the ISO 27001:2013 certification should be directed to SilverCloud Health’s Chief Information Security Officer by email to security@silvercloudhealth.com.

Thank you,

SilverCloud Health Team

1.1 ISO/IEC 27001

SilverCloud Health Limited has implemented a comprehensive Information Security Management System based upon the ISO/IEC 27001:2013 standard. The information security policies, practices and risk management have been assessed and certified by Certification Europe Ltd.

1.2 Objective of the ISMS

SilverCloud Health’s core business is providing services to healthcare and support organisations for use with their clients. A key part of this service is to ensure the security of its information and the information entrusted to it by its customers, their clients and its own staff.

SilverCloud Health’s objective of managing information security is to ensure that its core and supporting business operations continue to operate with minimal disruptions and that it can protect



the confidentiality of information of customers and their clients who use our services. SilverCloud Health shall ensure that all information created, processed and destroyed within SilverCloud Health is done so at all times with the view to protect the confidentiality, integrity and availability of that information.

1.3 ISMS Policy

- The purpose of the ISMS Policy is to protect SilverCloud Health's information assets from all threats, whether internal or external, deliberate or accidental.
- The directors of the company have approved the Information Security Policy and fully support the objectives of that policy.
- It is the policy of SilverCloud Health to ensure that:
 - Information should be made available with minimal disruption to staff, clients and authorised parties as required by the relevant business process
 - The integrity of this information will be maintained
 - The confidentiality of information will be assured in accordance with its classification
 - Regulatory, contractual and legislative requirements will be met
 - Business continuity plans will be produced to counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.
 - Information security education, awareness and training will be made available to staff
 - All breaches of information security, actual or suspected, will be reported to, and investigated by the appropriate staff members and management.
 - Appropriate access control will be maintained and information is protected against unauthorised access.
 - Where appropriate, policies, procedures and guidelines not limited to Information Security will be made available in both hardcopy and online format through an intranet system to support the ISMS Policy.
- The Internal Audit function has direct responsibility for ensuring the ISMS operates in accordance with the intent of this policy.
- All managers are directly responsible for implementing the ISMS Policy within their units, and for adherence by their staff.
- It is the responsibility of each member of staff to adhere to the ISMS Policy.
- Information security is managed through SilverCloud Health's risk management framework which will be maintained in line with ISO 27005.

1.4 Security of SilverCloudHealth.com

All data stored on the silvercloudhealth.com servers is treated with the highest level of security.

- Services and data for UK clients are hosted on servers in a data centre in Slough, England.
- The main and backup servers are hosted with trusted third-party hosting companies that have SSAE 16 and ISO 27001:2013 certifications.
- Only key personnel can access the servers. Access is granted on a needs basis and reviewed regularly. Administrative access is over a secure connection with multi-factor authentication.
- All access to silvercloudhealth.com is over a secure connection (HTTPS).
- All development for the SilverCloud Health platform is done using best practices in secure software development.



- All access to the SilverCloud Health platform is authenticated via username/password, with measures in place to protect users' accounts.
- Firewalls limit inbound and outbound access to the servers to specified ports.
- Data in the SilverCloud Health platform database is stored on encrypted storage.
- Our web application and network security has been independently tested through regular vulnerability assessments and penetration tests. Vulnerability assessments are scheduled monthly and penetration tests are scheduled twice a year.
- For additional details or to discuss security requirements contact SilverCloud Health's Chief Information Security Officer by email to security@silvercloudhealth.com.

1.5 Data protection

SilverCloud Health is compliant with GDPR and generally acts as a "data processor" on behalf of our customers who are the "data controllers" for the purpose of providing an online mental health and wellbeing platform, programmes and tools. Contracts with customers outline responsibilities and access to data. SilverCloud's standard privacy notice is available at: <https://demo.silvercloudhealth.com/help/privacy/>

SilverCloud has appointed BH Consulting as Data Protection Officer. The DPO has registered with the Data Protection Commission in Ireland. The DPO can be contacted by email at dataprotection@silvercloudhealth.com.

SilverCloud Health Data Protection Officer
BH Consulting, The LINC Centre, Blanchardstown Road North, Dublin 15, Ireland

1.6 Audits and assessments

To retain ISO 27001 certification, SilverCloud Health engages in an on-going surveillance programme that includes periodic audits conducted by Certification Europe Ltd. Additionally, to comply with the ISO 27001 standard SilverCloud Health conducts internal audits. The most recent ISO 27001 audit was conducted in May 2019.

SilverCloud holds Cyber Essentials certification, most recently renewed in November 2018.

SilverCloud Health is registered for the NHS Digital Data Security and Protection Toolkit as a Company with organisation number 8JA07. For 2018-19 SilverCloud Health achieved a status of "Standards Met".

The most recent penetration test took place in July 2019 and the next is scheduled for January 2020.



1.7 Policies

SilverCloud Health maintains and implements the following information security policies:

- ISMS Policy
- Information Security Policy
- Information Governance Policy

- Acceptable Usage Policy
- Application Security Policy
- Audit Policy
- Change Management Policy
- Incident Response Policy
- Mobile Computing Policy
- Privacy Policy – *includes data protection*
- Records Control Policy

1.8 Suppliers

Hosting services are supplied by Armor Defense Ltd. under contract

- United Kingdom Headquarters: 268 Bath Road, Slough, Berkshire, SL14DX, United Kingdom
- Slough Data Centre: 8 Buckingham Avenue, Slough, Berkshire, SL1 4AX, United Kingdom

Primary data and application hosting	Armor Defense
Backup hosting and email sending	Amazon Web Services
Technical support platform	Zendesk
SMS	Esendex

Supplier details are included in our privacy notice at <https://demo.silvercloudhealth.com/help/privacy/>