INFORMATION SECURITY COMMITMENT

Serendipiti (IT Services) Limited

Version 2026.03

serendipiti

Table of Contents

Information Security Commitment

How we protect your systems, information and privileged access.

Version 2026.03

Company Name:	Serendipiti (IT Services) Limited
Registered Office:	15 High Street, Brackley, Northamptonshire, NN13 7DH
Company Reg No:	05215060
VAT Reg No:	855 2789 82

Introduction

This document explains how Serendipiti (IT Services) Limited protects privileged access, confidential information and client data whilst delivering IT support and managed services.

It forms part of our commitment to delivering secure, professional and trusted IT services and complements our Terms of Engagement and Service Level Agreement.

Whilst this document does not form part of the contractual agreement between Serendipiti and the Client, it reflects the standards, principles and working practices that guide the delivery of our managed IT services.

Purpose

This document explains the principles and standards that Serendipiti follows when privileged access is granted during the delivery of IT support, consultancy and managed services.

Its purpose is to provide reassurance that privileged access will only be used where reasonably necessary, professionally, responsibly and in the best interests of the Client.

Our Commitment

Whilst providing services to the Client, Serendipiti is committed to ensuring that all privileged access to systems, applications, devices and information is exercised solely for the purpose of delivering the agreed IT services.

We will act with professionalism, integrity and due care at all times.

Privileged Access

The Client may provide Serendipiti with privileged or administrative access to systems including, but not limited to:

- Microsoft 365
- Servers
- Network infrastructure
- Firewalls and routers

- Cloud services
- Backup platforms
- Security systems
- End-user devices
- Business applications

Such access will only be used where reasonably necessary to deliver the agreed services requested by the Client.

Information Security

Serendipiti is committed to maintaining the confidentiality, integrity and availability of all information encountered during the provision of services.

Accordingly, we will:

- Keep privileged credentials secure
- Use privileged accounts only when necessary
- Access only those systems and information required to perform the requested work
- Treat all Client information as confidential
- Follow recognised cyber security best practice
- Take reasonable steps to prevent unauthorised access, disclosure or alteration of Client information
- Notify the Client promptly if we become aware of any suspected security incident relating to their environment

---

Confidentiality

Any information accessed whilst providing services shall remain confidential unless disclosure is:

- required by law
- authorised by the Client, or
- necessary to protect the Client's interests during the delivery of services

This obligation continues after the termination of our business relationship.

Acceptable Use

Serendipiti will not knowingly:

- access information unrelated to the requested work
- disclose Client information to unauthorised persons
- use privileged access for personal benefit
- make unauthorised configuration changes
- intentionally disrupt business operations except where necessary to prevent or minimise an immediate security risk

---

Compliance

Serendipiti will perform its services in accordance with:

- applicable UK legislation
- data protection legislation, including the UK GDPR where applicable
- recognised information security principles
- the Client's documented security policies where these have been made available to us

---

Changes to Client Policies

Where the Client has specific information security policies, privileged access procedures or cyber security requirements, the Client agrees to make these available to Serendipiti.

Serendipiti agrees to familiarise itself with any such documentation and, where reasonably practicable, comply with those requirements whilst delivering services.

Access Logging & Accountability

Where appropriate, remote access sessions, privileged administrative activity and significant configuration changes may be recorded or logged for operational, quality assurance and security purposes.

Access is granted only to authorised Serendipiti personnel who require it to perform their duties.

Credential Management

Client credentials are stored using secure password management systems where appropriate and are only accessible by authorised personnel.

Credentials are reviewed periodically and securely removed when no longer required or upon termination of services, subject to any agreed retention requirements.

Professional Competence

Serendipiti ensures that personnel requiring privileged access possess the appropriate knowledge, experience and professional competence to perform their duties responsibly.

We invest in ongoing technical training and continuous professional development to help our team keep pace with evolving technologies, cyber threats and industry best practice.

Security Controls

Serendipiti maintains appropriate technical and organisational measures to protect client information, which may include:

- Multi-Factor Authentication (MFA)
- Encrypted password management
- Device encryption
- Secure remote access
- Endpoint protection
- Role-based access
- Secure disposal of credentials
- Regular software updates
- Security awareness training
- Secure backup and recovery procedures
- Secure disposal of retired equipment and storage media (where applicable)
- Periodic review of privileged access permissions

Working Together

Security is most effective when both parties work together.

By combining Serendipiti's technical expertise with the Client's knowledge of its own business, policies and users, we can help reduce operational risk whilst maintaining practical, proportionate and commercially appropriate security.

Client Responsibilities

Information security is a shared responsibility.

Clients are encouraged to:

- maintain secure passwords;
- enable MFA where available;
- promptly report suspected security incidents;
- maintain supported systems;
- implement reasonable security recommendations.

These responsibilities complement the Client Responsibilities described within our Terms of Engagement.

Continuous Improvement

Serendipiti continually reviews its security practices, operational procedures and technologies to reflect emerging cyber threats, evolving best practice and changes in legislation.

Where appropriate, our internal policies and technical controls are updated to maintain high standards of information security and professional service delivery.

Our Security Philosophy

Information security is not a single product or technology. It is an ongoing process involving people, processes and technology working together.

Serendipiti is committed to continually improving our security practices and helping our clients reduce operational and cyber-security risk through practical, proportionate and commercially sensible solutions.

Further information

If you have any questions regarding our information security practices or the way we protect your systems and information, please contact us.

Serendipiti (IT Services) Limited

✉ helpdesk@serendipiti.co.uk

☎ 01933 229133

🌐 www.serendipiti.co.uk