Content

Version Control

Version	Date	Description	Approved By
1	19/04/2024	Recreation, modification and version reset.	George Tye

Introduction

At Migrate Data, we are committed to securing and protecting the data you entrust to us. This Data Transmission Security Statement outlines the measures we take to ensure the security of your data during transit within and outside our network.

Secure Transmission Methods

We use Secure File Transfer Protocol (SFTP) for all data transfers, ensuring that your data is encrypted while in transit. Our SFTP site is protected with an active SSL certificate, guaranteeing that all connections are secure and verified.

An SSL certificate, or Secure Sockets Layer certificate, is a digital certificate that authenticates the identity of a website and enables an encrypted connection. It functions by initiating a secure session between a web server and a client (such as a browser) using a process called the SSL handshake.

During this process, the server presents its SSL certificate containing a public key to the client, which verifies it against trusted authorities. If verified, all data transmitted between the client and server is encrypted using symmetric encryption keys established during the handshake, ensuring that any data sent over the connection is secure and private. This protocol is integral for protecting sensitive information in transit and is a standard practice for secure communication on the internet.

System Architecture and Data Flow

Our network architecture is designed to maximise security. It includes a Demilitarized Zone (DMZ) server that acts as the first point of contact for all incoming and outgoing connections. This server securely routes traffic to our internal server hosted on Azure, where your data is processed and stored securely.

Access Control

Access to our Titan MFT system is strictly limited to three senior staff members, ensuring highly controlled and monitored access. Each client has access only to their designated data folders on our SFTP site, with permissions managed on an individual basis to prevent unauthorised access to others' data.

Data Encryption

We employ stringent encryption protocols for all data in transit. By using the SFTP protocol, we ensure that your data remains confidential and intact until it reaches its intended destination.

Client Data Segregation

Your data is stored in individual folders accessible only to you. We implement strict access controls and permissions settings to ensure that your data is isolated from other clients' data, providing you with enhanced privacy and security. Additionally, Migrate Data adheres to a policy of not retaining your data longer than necessary.

We regularly review our data retention periods to ensure that your information is only kept as long as it serves the purpose for which it was collected, complying with legal obligations and our commitment to protect your data.

Incident Management

We have procedures in place for responding to security incidents. Our Incident Response Plan outlines steps for effective handling and resolution of any security issues that may arise, ensuring minimal impact on your data and our operations.

Policy Review and Enforcement

This policy is reviewed regularly to ensure it remains aligned with industry best practices and regulatory requirements. Compliance with this policy is mandatory for all staff, and failure to adhere can result in disciplinary action. We also provide ongoing training to our employees to ensure they understand their role in protecting your data and are equipped to handle security challenges effectively.

Migrate Data is dedicated to maintaining the highest standards of data security. This statement reflects our ongoing commitment to protecting your information and our proactive approach to data security management.

Contact Information

Should you have any questions or concerns about how we protect your data, please do not hesitate to contact us. You can contact our IT Manager, Joshua Rodgers, directly at jrodgers@migratedata.co.uk