St James's Place

Our approach to cyber security, resilience and data protection

At St. James's Place we take Cyber and Data Security extremely seriously. We adopt UK Government guidelines, best practice, and industry recognised standards and then go further, to ensure that we maintain the confidentiality, integrity, and availability of your personal data.

We were one of the first FTSE 100 organisations to obtain Cyber Essentials Plus (CE+) in 2017 and have since maintained accreditation every year.

SJP Partner

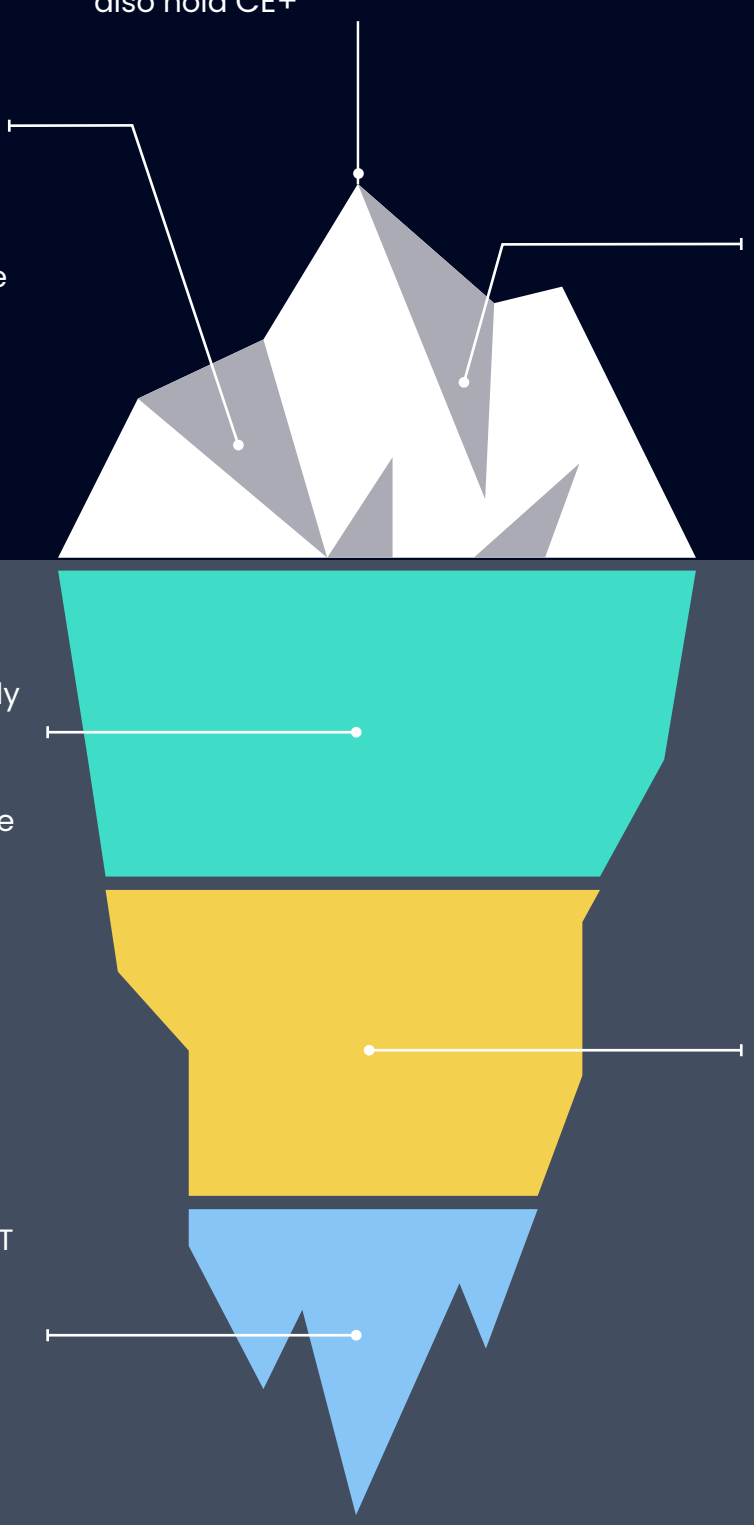
- To further protect client and business data throughout its lifecyle, all SJP Partners must remain compliant with CE+ requirements
- Your SJP Partner will be responsible for ensuring that any outsourced or 3rd party providers that have access to your data also hold CE+

Data Protection

- We have a published Privacy Policy on our corporate website which provides detail on how your data is collected, stored and processed by St. James's Place, its subsidiaries and our Partners as Joint Data Controllers
- We take all appropriate steps to ensure that data is protected in accordance with the Data Protection Act 2018 and the requirements of the Information Commissioner's Office (ICO) and our regulators

Fraud Controls

- Your SJP Partner is responsible for verifying your identity before processing a monetary withdrawal
- Our Administration Centre will ask security questions to validate your identity and verify any information details provided
- Any suspicious activity is flagged to our central Financial Crime Prevention Team to investigate



Risk Management

- We utilise industry leaders to continually assess our strength, maturity and resilience against cyber threats
- External expertise is leveraged to advise on the cyber threat landscape and inform our operational teams
- Users accessing SJP networks are trained in Data Protection, Information Security, Acceptable Use of IT systems and more

Security Assurance

- We conduct independent security testing against our public and private IT infrastructure to validate our resilience to cyber threats
- We have a robust third-party risk management process to ensure third parties meet our principles and standards
- We monitor and measure our security performance, using industry benchmarks and 3rd party advisories to ensure our controls are appropriate and operating effectively

Technical Controls

- Corporate devices are fully encrypted and protected from cyber attacks through a layered control approach aligned with National Cyber Security Centre (NCSC) guidance and industry standards
- Multi factor authentication (MFA) is used across our business systems to protect data and system integrity
- Our Cyber Security team is supported by a 24/7 Security Operations Center (SOC) that provides continuous monitoring and incident response capabilities to prevent and respond to security threats
- Data is secured throughout its lifecycle ensuring encryption of data in transit and at rest

The security controls outlined in this document are reflective of the systems and services that St. James's Place provide and maintain.

CYBER ESSENTIALS PLUS