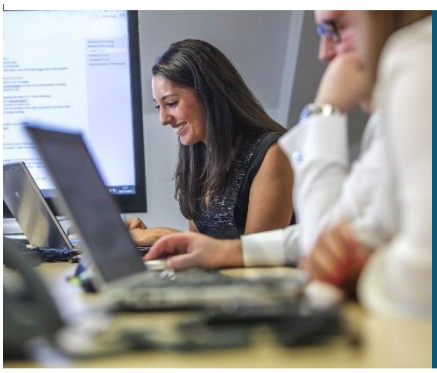

ProspectSoft

Guide to Cloud Architecture and Security with Prospect 365

Contents

Secure Expertise 3
Secure Platform 4
Secure Architecture 4
Secure Software 4
Secure Monitoring 4
Secure Compliance 5
Secure Backup 5
Secure Certificates 5
Secure Together 6

ProspectSoft

Cloud Security

Today, security is vital to every business. You need to know your data is secured by rock-steady services that are designed to keep hackers out.

Cybersecurity	Security delivered with years of experience building secure software, hosted platforms and online services.
Data Privacy	Certainty that you own your data, and a commitment from us that we will use customer information only to deliver services and not for advertisement or sharing with other organisations.
Compliance	Commitment to industry standards and organisational policies and compliance.
Transparency	Visibility into how your data is handled and used and that all data is hosted, maintained and backed up within the EU.

Secure Expertise

Security starts with commitment and expertise, not as an afterthought. ProspectSoft maintains an ISO27001 accreditation (the international standard for data security) and our security team is led by a dedicated internet networking and security expert. Members of the team have been hired specifically for their expertise and background in enterprise network security (including web services); others have come through internal departments and gained relevant Microsoft Accreditations. Having previously worked on high-profile projects such as HMRC Online Self-Assessment and HMCS MoneyClaim Online, our team's collective practical experience and expertise ensures that security is embedded into everything we do.

Members of our infrastructure and support teams have security qualifications - a Master's degree in Information Security, or CISSP (Certified Information Security Systems Professional). ProspectSoft is a Microsoft Gold Application Development Partner and a Microsoft Gold Cloud Platform Partner, and our products have been certified by Microsoft for use on Server 2008 and 2012.

Secure Platform

Prospect 365 is hosted in Microsoft Azure, Microsoft's Global Cloud platform. With Azure, Microsoft has made an industry-leading commitment to the protection and privacy of data. Microsoft were the first cloud provider recognised by the European Union's data protection authorities for their commitment to rigorous EU privacy laws. Microsoft Azure complies with ISO27001 and was also the first major cloud provider to adopt the international cloud privacy standard, ISO 27018.

Prospect 365 services, running within Azure are all load-balanced with redundancy built in. They communicate across a private network within Azure and are secured by Azure's AI monitoring and protection systems.

Secure Architecture

Our solution architecture is built on an enterprise class secure design, utilising strict security and partitioning between layers. Applications are deployed as secure Microsoft .Net components within secure pools of Microsoft IIS Cloud Services. Behind these web services sit highly robust database services managing the website and application content across load-balanced servers.

Customer databases are isolated across server sets, protected by firewall rules and Azure access control lists (ACLs) to eliminate inbound access from the Internet. Each customer's data is encrypted with a unique and randomly generated encryption key – ensuring that one customer's data is isolated and encrypted independently from the next.

Secure Software

The software running within this architecture has been specifically designed with security in mind. Each component is independently evaluated and tested for security risks, but the application as a whole also has a built-in software Security Layer. This Security Layer provides extra security, automatically filtering out attacks aimed at the software level – such as SQL Injection.

The security of our software is continuously verified internally and is also annually audited by an independent 3rd party security company.

Secure Monitoring

Our solutions are maintained and monitored 24 hours-a-day, 7 days-a-week, 365 days-a-year by qualified hardware and infrastructure professionals.

Independent automated systems then also monitor every aspect of our solution, from secure certificate expiry to the performance of individual services. With our automated alerting system, we will know about any impending fault long before you or your customers do.

Secure Compliance

ProspectSoft is compliant with ISO 27001, the international standard for data security.

Furthermore, the data centres that we use also implement the highest levels of data security. The Microsoft Azure data centres and the Amazon datacentre (where we store our backups) are both compliant with ISO 27001.

For more information, please visit https://prospectsoft.com/newsarticle?article_id=33&article_desc=ISO27001, https://azure.microsoft.com/en-gb/support/trust-center/compliance/ and https://aws.amazon.com/compliance/iso-27001-faqs/

ProspectSoft's platform is also encrypted by Let's Encrypt certificates. Let's Encrypt is a global Certificate Authority (CA), who enable ProspectSoft to obtain, renew, and manage SSL/TLS certificates with ease through a highly automated process. Their certificates can be used by websites to enable secure HTTPS connections.

Let's Encrypt

Comodo, who ProspectSoft use for PCI, has determined that **ProspectSoft Ltd is compliant with the PCI scan validation requirement**. Please ask us if you would like a copy of the Compliance Report.

Secure Backup

To mitigate against data loss through hardware failure, all critical applications, website configurations and customer data is duplicated at least *three times*… with at least two active copies of each piece of data as well as backups to a separated data centre hosted by Amazon (AWS).

Secure Encryption

With Prospect 365 your data is encrypted "at rest" (in the database) and "in transition" (as it is transmitted to and from users across the internet). But, you will want your staff and customers to *see* that it is secure. That's why we provide certificates as standard using 256-bit encryption with a 2408-bit key.

Secure Together

Ultimately, online security is a partnership. Working together we can keep your business secure.

ProspectSoft

- The Prospect 365 cloud services are built to be secure and trusted.
- We use world-class infrastructure, platforms and services with security built in.
- We provide software that includes security controls and capabilities to help you protect and control access to your data.

Customer

- As our customer, you own your data and your identities; and responsibility for protecting them and assigning and revoking access rights.
- You are also responsible for the security of your network and on-premise resources and devices.
- If you are unsure of how to implement best practice security measures and policies, you could consider the ISO27001 framework.

We take the security of your data hosted with us, extremely seriously, but it is equally important that you are confident in your own corporate security policies. Organisations can benefit greatly from taking a methodical approach to cloud security. This involves investing in organisational capabilities and policies that lead to secure environments and the secure use of data and software. We recommend that all customers regularly review their own approach to corporate security.

Governance and Security Policy	• Organisations should consider updating internal policies and staff handbooks for how to adopt and use cloud services.
Administrative Privilege Management	• Every enterprise application, including cloud applications have different access priveleges. • Your top-level, administrative priveleges should be controlled and protected
Identity and Password Management	• Policies for strong passwords, password re-use and password security are even more important in the cloud than on-premise.
Threat Awareness	• Every organisation holds diffferent data and faces different threats. • Evaluation of the particular data and secuirty threats for your organisation will help you to avoid, or be prepared for issues in the future.
Data Protection	• You own your own data and should mange how it is used, shared, updated and published. • Sensitive data should be classified and protected accordingly.