DataProtech
TRUSTED • EVERYDAY • EVERYWHERE

Security

At DataProtech data security and privacy are our highest priorities. Software development and services delivery are built around robust security and data privacy policies. By delivering a service focused on these principles, we are able to ensure high availability, confidentiality, and integrity of your data.

DataProtech conforms to the UK GDPR and follows ISO27001 standards. Regular security test are carried out on our infrastructure and twice per year penetration tests are carried out.

It is the policy of DataProtech to maintain awareness throughout our organisation and supplier base of the importance of keeping information secure, whatever form that information may take. We will achieve this in part via regular Information Security (I.S.) training and awareness programmes.

Stay at the forefront of developments in relation to I.S. We will do this by remaining vigilant to the ever changing I.S. Environment by supporting a culture of Continual Improvement (C.I.). Thoroughly address any nonconformities in relation to I.S. We will ensure this is achieved by maintaining a robust nonconformance reporting system which will be regularly reviewed.

Provide necessary and proportionate resources in order to meet our I.S. obligations. We will maintain appropriate resources by regular measurement and monitoring of our I.S. Management System (I.S.M.S.).

Encrypt data and devices wherever possible and to maintain a pragmatic information classification scheme.

Adopt a risk-based approach to I.S. We will implement this by maintaining a current risk assessment and treatment plan which will be reviewed not less than once a year.

Set I.S. objectives annually and to review them regularly and at our I.S. Management Review mtgs. These objectives will be communicated to all employees via our training and awareness programmes.

Our Secure Hosting Provider

All DataProtech cloud applications are deployed in our private cloud environment fully owned and operated by DataProtech our scalable private cloud infrastructure is protected by latest security technologies and managed by our own security team.

Physical Security

Physical access is carefully restricted to only personnel that are required at the site and is then revoked when access is no longer required. Security staff utilise a mix of security cameras and ID badges, with multiple layers of two-factor authentication. Any access granted is restricted based on the role of the individual and to the relevant area of the data centre. DataProtech's Security Operations Centres continuously monitor for unauthorised entry via access logs, video surveillance and intrusion detection.

We maintain and continue to enhance our SOC reports, certifications, including SOC, PCI, ISO and many more.

Business Continuity

All of our data centres are carefully situated to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. The data centres are fitted with automatic fire and flooding detection and suppression. DataProtech utilises three regions Munich (Germany), Nuremburg (Germany) and St. Louis, Missouri (USA). Each region has multiple availability zones, each physically separated from one another ensuring high availability.

Climate and temperature are precisely controlled by personnel and systems to ensure optimal performance of servers and other hardware. All systems and equipment are monitored and receive preventative maintenance to maintain continued operability of equipment.

Environmental security

Our infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. DataProtech has designed its systems to tolerate system or hardware failures with minimal customer impact.

Core applications are deployed in an N+1 configuration, so that in the event of a data centre failure, there is sufficient capacity to enable traffic to be load balanced to the remaining sites.

Secure Product Build

Product Ownership

All products at DataProtech have an owner that is responsible for the delivery and secure development of the application. The owner will regularly review the roadmap for the product and prioritise security fixes accordingly.

Version Control

A central repository is used to manage code and access to the repository is role based. This is integrated with the development environment and version controls. A record of any change to the code is maintained and available to the customer in the form of release notes.

QA

Every release goes through a strict QA procedure, which tests functionality, performance, configuration, user experience and stability. Only once it passes these tests is the version available for use.

Architecture

Data Backup

All data is backed up at regular intervals 24 hours a day. Backups are stored at different data centres and also off site in Microsoft data centres. The backups are stored in access-controlled containers.

Auto Scaling

Automatically distribute application traffic across multiple availability zones that supports high availability, auto scaling and robust security.

Incident Management

Robust incident management procedures allowing for reporting incidents and tracking them through to resolution. Following the ITIL framework, incidents are prioritised, and SLAs tracked.