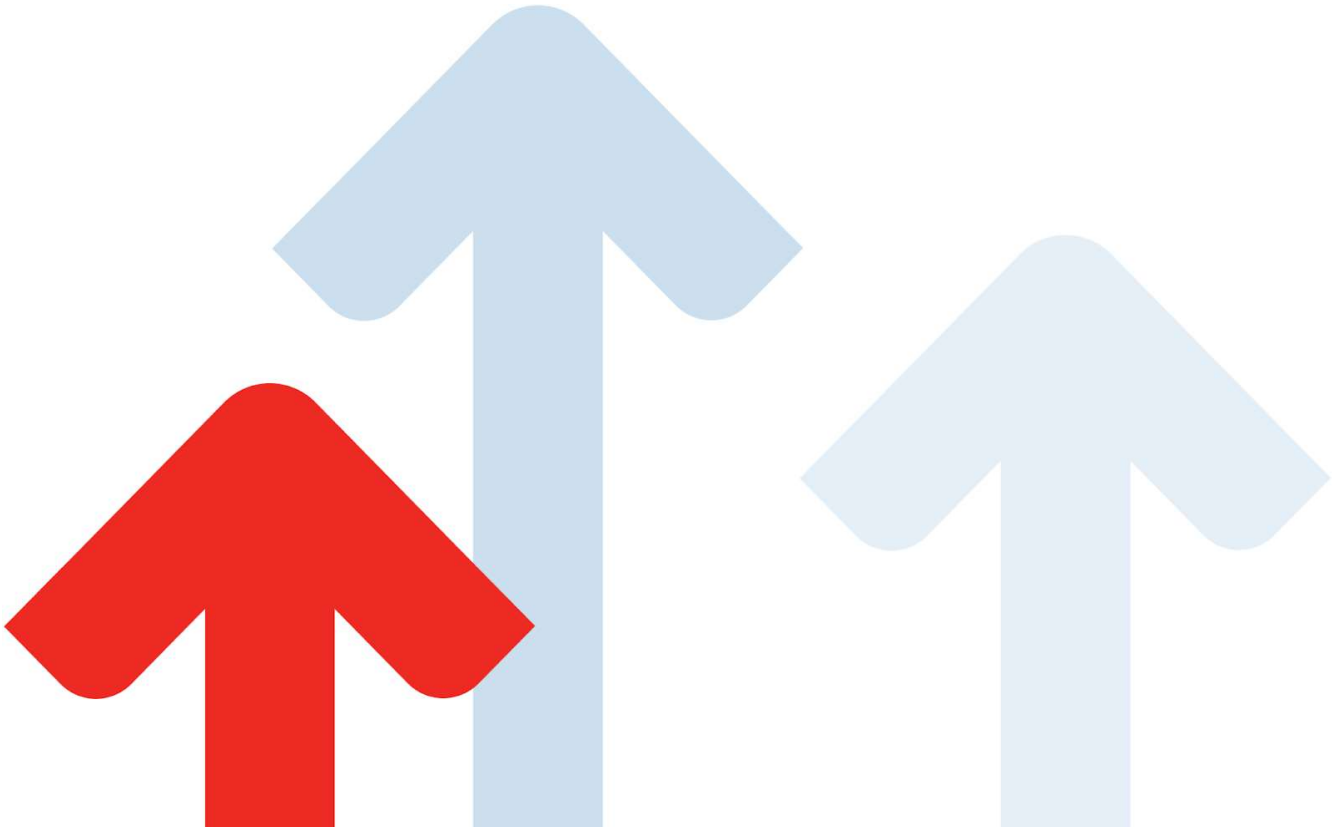
webexpenses

Classification - Proprietary
March 2022
v2.0

Assured Compute Platform



Classification - Proprietary
March 2022
v2.0

Assured Service Platform

The platform on which we run Webexpenses services is designed and maintained around the security triad: Confidentiality-Integrity-Availability. These three tenets lead our InfoSec policy and ensure we always have security and business continuity at the forefront of all we do. Our security trained operations and development teams ensure we are ever vigilant.

Privacy

Our policies are procedures are aligned with the following privacy laws:

- UK General Data Protection Regulation (UK GDPR)
- EU General Data Protection Regulation

We collect only PII data (Personal Identifiable Information) that is essential and use this only as agreed. Apart from our authorised Sub-Processors, no information is passed to third parties.

Whilst in our care your data is safeguarded with encryption when:

- Transmitted over public networks
- Stored in stand-alone files
- Stored in databases

Storage of PII on workstation, laptops, mobile and storage devices is prohibited under company policy.

Data Centres

We utilise Amazon Web Services (AWS) data centres in London, Ireland, Paris, Melbourne and Sydney. In most cases this is region specific.

AWS Controls

A list of physical, security, and other controls can be found on the AWS website
https://aws.amazon.com/compliance/data-center/controls/

AWS Compliance

AWS has a comprehensive list of compliance controls that can be found on the AWS website
https://aws.amazon.com/compliance/programs/

Storage Device Decommissioning

Once a storage device has reached its service lifetime it is decommissioned by AWS and sanitised with techniques detailed in NIST 800-88 (https://aws.amazon.com/compliance/data-center/controls/#Device_Management).

Compliance (Webexpenses)

- ISO27001:2013
- Payment Card Industry Data Security Standard (PCI DSS) - Please contact an account manager for a copy of the Attestation of Compliance (will require a NDA).
- Cyber Essentials (UK Office)

Data Encryption

- User web traffic - AES 128-256 bit & TLS 1.2 and above
- At rest storage - volume encryption AES 256
- Database storage - AES 256 bit
- Passwords - Hashed and salted – SHA256
- AWS Backup - AES 256 bit

Application Security

Authentication

- Forms based with strong password policy and configurable MFA.
- SAML 2.0
- Azure AD
- ADFS on premise

Permissions

Role based permissions determine user rights.

Attack & Penetration Testing

- Performed Annually or upon significant change.
- Program of monthly internal and ASV-accredited external scans.

Classification - Proprietary
March 2022
v2.0

Network Based Security

We have designed our network around the three tenets Confidentiality-Integrity-Availability. This ensures your data is protected and available at all times.

- AWS web-application firewall in front of all public-facing services
- Strong password policy and MFA required for operational environment
- AWS infrastructure is protected by AWS Shield against DDoS attacks
- “Least privilege” principle followed in all areas of the business
- Network segmentation of production and operational networks
- Hardened configuration of all network appliances
- Load balanced solution with multiple redundancy to ensure capacity and performance
- Log aggregation, analysis and management solution
- Intrusion detection and File integrity system
- Traffic controlled via virtual firewall

Vulnerability Management

We actively monitor many first alert sources for vulnerabilities and threats that may affect us. Relevant issues are risk accessed and where necessary controls are put in place to mitigate risk.

Security patches are applied to both production and operational environments as soon as possible. Sufficiently serious patches may be considered for out of maintenance period installation.

Disaster Recovery

- Recovery point objective (RPO) - 24 hours
- Recovery time objective (RTO) - 12 hours