Security

The security of our software and our client's confidential information is our top priority. We apply all relevant legislative requirements of the Australian Privacy Principles and GDPR in Europe at all times. Further, no services or data is provided to off shore parties. We do use our development partner based in India for some assisted development of both our Apple and Android apps.

With government departments including the Department of Finance, Tier 1 contractors, large mining companies and ASX listed companies subscribed to Skytrust, our security measures are continually being tested and scrutinised. Our commitment to you is to ensure your data remains safe and free from external intrusion.

Single Sign On (SSO)

Single Sign-On Corporate allows your users to login to Skytrust on the PC and mobile apps using your existing Microsoft Azure AD account and multi-factor authentication allowing for a streamlined login process. There is a modest cost for this feature otherwise Skytrust Secure ID is included at no additional cost.

Password security

We have implemented a limit of three (3) login attempts before a User is temporarily suspended and a configurable lock out process should an attempt be made with multiple usernames concurrently which can lockout our application. In addition, we enforce strong password requirements, password encryption to SHA 2, with all traffic on our secure sockets layer (SSL) using global standard 256-bit encryption.

Application security

Skytrust also uses Imperva, a market leading security Web Application Firewall (WAF) service as the leading protection for web application security, DDoS mitigation, content caching, application delivery, load balancing and failover services. Imperva has recently been named Gartner Magic Quadrant WAF Leader for the sixth consecutive year, the only 6-time leader. Safety is our first priority and this is exemplified by our commitment to employing only the best in the industry.

Data Security

Secure data centres

Our primary server is located in Melbourne, Australia within the World Class Fujitsu Data Centre. This facility has ASIO T4 Certification, ISO 27001 Certification, is a fire proofed facility with security guards and CCTV systems. The centre has automated air sampling systems to detect air impurities, uptime guarantee of 99.98% as well as numerous redundant power supply systems.

Your data is our priority

At Skytrust your data security is paramount to us, hence in addition to the above measures, we keep a further three sets of your data (a total of 4 sets of your data at any point in time). We also keep the servers physically separated by over 500kms to ensure your data is protected from geographical association threats such as natural disasters, war or terrorism. In a worst case scenario, your data can be easily retrieved and restored within 24 hours. This is our commitment to you, to ensure your organisation is compliant without the unnecessary worry of data control.

Access to Skytrust for programming purposes is only possible from within our head office and all staff sign a confidentiality agreement on joining our team. On a frequent periodical basis and on staff departure, all Skytrust internal passwords are re-set and managed by our programming supervisors for an added measure of security.

Penetration testing

As part of our best practice, we have a constant focus on the security of our Skytrust software. We have previously engaged HackLabs and have now collaborated with Pure Security to conduct periodical penetration tests on our security protocols. The scope of these tests are to verify the security of the software which includes but is not limited to: simulated DDoS, brute force login attacks, testing against OWASP, CREST and other known security vulnerabilities.

Browser and app support

Skytrust is supported on all modern browsers including Google Chrome, Firefox, Safari and Microsoft Edge. Ideally, it is recommended to use Google Chrome as your main browser for Skytrust. Chrome automatically updates every six weeks with the latest security features and fixes while important security bugs are pushed out with a fix within 24 hours.

The Skytrust App is available on the App Store and Google Play Store for iOS/Android devices. The app provides offline capability allowing for quick access to adding Incidents & Hazards on site, completing required Inspections and the ability to scan custom QR codes to view information on a particular Plant & Equipment item. The Home button also dovetails neatly into your Home Tile page, providing a seamless transition into the full version of Skytrust, using access privileges.