Online Security in Hong Kong Legal Cloud

eBRAM Online Dispute Resolution Centre Limited

eBRAM 一邦國際網上仲調

Hong Kong Legal Cloud is a cybersecurity-by-design and privacy-by-design cloud platform with facilities situated in Hong Kong to provide safe, secure and affordable services for legal and dispute resolution communities.

Security is always our top priority.
The followings are the major measures to safeguard your journey in the Hong Kong Legal Cloud.

Don't forget to follow the Best Practice of web surfing recommended by the Office of the Government Chief Information Officer: https://www.infosec.gov.hk/en/best-practices/person/surfing-the-web-and-e-shopping

Data Security

- ✓ Separated containers for individual users to avoid unauthorized access to files.
- ✓ Data and files are encrypted in the storage.
- ✓ Data of deleted users and unsuccessful registration will be removed from the system.
- ✓ Blockchain technology is adopted to trace every action on Legal Document Exchange to protect the files from tampering.
- ✓ Regular data backup is in place.

Application Security

- ✓ Multi-Factor Authentication is enforced.
- ✓ Password complexity mixing uppercase and lowercase characters, numbers and special characters is enforced.
- ✓ Guest users requires One-Time-Password to access files shared with them.
- ✓ Forced logout for long idle sessions.
- ✓ Continuous security patching to mitigate vulnerabilities.

Infrastructure Security

- ✓ Infrastructure is provided by one of the largest cloud providers with data centres located in Hong Kong and compliant with ISO 27001 and ISO 27018.
- ✓ High Availability for the critical system components.
- ✓ Disaster Recovery to protect from single data centre failure.
- ✓ 24 x 7 Monitoring and Alerts on monitor system resources as well as security events.
- ✓ Routine virus scanning on files to identify threats from viruses and ransomware.
- ✓ Vulnerability assessment and risk analysis tool keeps running to identify risk.
- ✓ Anti DDoS (Distributed Denial of Service) is enabled.
- ✓ Network firewall is enabled to deny traffic to unauthorized ports.
- ✓ Web application firewall is enabled to protect the web application from common attacks identified by Open Web Application Security Project®.
- ✓ End-to-end HTTP traffic is encrypted with TLS 1.2.