VirtualCabinet

Document Portal

Security & Availability

The Virtual Cabinet Portal solution adheres to the highest industry standards for security. You can publish and access your documents and files with confidence, safe in the knowledge that we use the same security methods and principals as the most diligent of institutions such as banks and government bodies.

Documents and files stored in the portal are far safer than those stored on your own systems in most cases and are available 24/7 with an uptime of 99.9%.

We have a team of experts using the latest technologies and best practices to ensure that the Virtual Cabinet Portal is, and remains, a safe and protected environment for your confidential and sensitive information.

The Virtual Cabinet Portal is tested for security vulnerabilities to the highest degree by specialist, independent and industry recognised third party penetration specialists.

PROCESSES

Security of the application, including how it is designed, built, tested and worked on, and by whom, is our highest priority. We are proud to be ISO 27001 compliant and stringently aim to exceed industry standards.

ENCRYPTION

All data in transit, including data sent and received from the portal is encrypted using TLS. Data, documents and files stored in the portal are hashed or encrypted using AES-256 (where applicable).

DATA CENTRES

We use infrastructure and services provided by Amazon Web Services (AWS) to provide the Virtual Cabinet Portal.

AWS, like us, treat security as their highest priority. AWS documentation on the security of their infrastructure and services is comprehensive and can be found here https://aws.amazon.com/security

Specific details about physical and environmental security and network architecture can be found in their white paper AWS: Overview of Security Processes

PENETRATION

The Virtual Cabinet Portal is secured behind multiple firewalls. It has been hardened to resist attack methods such as brute force password ciphers, cross-site scripting (XSS), cross-site request forgery (CSRF), JSON hijacking and SQL injection at every level of the application architecture.

All hardening is tested internally by experienced CREST certified test engineers and verified by independent 3rd party security specialists.

AUDITING

Every action that occurs within the portal is logged and recorded against the individual that performed it, providing a complete and compliant audit log.

AVAILABILITY

We leverage the best that AWS has to offer in order to provide high levels of availability, redundancy and scalability.