Information Security Manual

At Crownpeak we have built an effective information security program that revolves around compliance, accountability, implementation, and the allocation of resources. This page provides a description of some of the core information security measures at are in place and reviewed annually.

Governance

Our governance framework establishes guidelines, defines roles and responsibilities, assesses, and mitigates risks, ensuring compliance with industry regulations, and implementing technologies to safeguard against potential threats.

Our security program is overseen by the IT Security Committee.

General Security Information

Crownpeak maintains an information security program that is designed to protect against potential threats, protect the security and confidentiality of personal data, protect against unauthorized use, ensure the proper disposal of personal data. We do this by having policies and processes, ensuring that our technical safeguards and controls (firewalls, encryption intrusion detection and patch management) are effective and provide employee training and awareness.

Network and Infrastructure Security

Crownpeak maintains network architecture and regularly reviews firewalls rules and completed access reviews to ensure that appropriate restrictions are in place.

For infrastructure, we maintain a Security Incident Event Management (SIEM) and other security monitoring tools on production servers that host our products. Notifications are sent to the Information Security Team, who review, investigate, and mitigate any identified events.

Crownpeak applies industry standard encryption technology.

Detail access logs are maintained of our infrastructure and products which are reviewed regularly for events impacting security and availability.

Data Handling

Crownpeak maintains measure to ensure that only authorized personnel have access to personal data, that data is separated between other data and customers, and ensuring the destruction of media is carried out according to the disposal requirements.

Access Controls

Crownpeak has in place authentication methods, secure communication of credentials, password management, password hashing and session management.

Do we want to say anything about SSO?

Disaster Recover

Crownpeak maintains a Business Continuity and Disaster Recovery program, which align with industry best practices and are reviewed and updated annually.

Incident Response

Crownpeak has an incident response plan designed to promptly and systematically address incidents in a timely manner. The plan is reviewed and tested annually.

Physical Security

Crownpeak uses industry leading cloud platforms (Google Compute Cloud and Amazon Web Services) to host its production services. These cloud services provide high industry standard levels of physical security to access their data centers. Data center access is limited to authorized personnel only and physical security measures in place include on-premises security guards, closed circuit video monitoring and additional intrusion protection measures. We conduct an annual review of their physical measures and rely on their third-party attestations of physical security. Within our office locations, Crownpeak employs a number of industry-standard physical security controls and we provide annual training to our employees and contractors to protect the physical security of their assets and person.

Security Testing, audit and Training

Crownpeak engages annually a third party to conduct PEN test on our infrastructure containing or storing personal data. We also conduct internal vulnerability testing weekly. Do we want to say anymore there.

Crownpeak is certified ISO27001:2022, which is valid until 2027, and we are TISAX certified which expires in 2026.

Crownpeak provides security awareness and phishing training at the time on onboarding and annually thereafter.