Aprio Security

Data security is fundamental to our business. Effective data security requires understanding the chain of information and data flow, from creation at your keyboard or office, through to retrieval from our website. Aprio has implemented many measures to ensure the confidentiality and security of its customer's materials and information Aprio's security is trusted by many financial institutions, crown corporations, non-for-profit organizations, First Nations, public and private companies.

>Physical Security All physical access to the data centers where nonpublic personal and company information is maintained is controlled and monitored by security personnel. Our hosting partners have third party audits that evaluate overall physical security, network architecture, redundancy, disaster recovery capabilities and operational policy and compliance to internal operational and security policies.

>Network and Data Security Data is encrypted by the strongest encryption products, both during network transmission and while resident on computing platforms, including 2048-bit SSLv3 certificate encryption which is applied to all data transmissions. Each company's content is secured into an individual repository which is completely confidential, this includes Aprio employees unless access is specifically granted by the client.

>Application Security All access to information contained within Aprio are managed by the administrator, based on groups, roles, and designated access levels. Pages are never cached, so if a user logs out, the back feature in the browser will not allow previous pages to be seen.

>Network Monitoring The entire infrastructure is continuously monitored against network attacks with an inline intrusion prevention system and enterprise level firewalls.

>System Redundancy All customers' data is backed up on primary and secondary data centers. Secondary servers come are in place if there is any interruption in the primary servers.

>User Authentication Aprio's user authentication policies enforce security without increasing complexity for the directors.

>Data Backup Procedures All of our customer's data is backed up automatically every day to both local and off-site server facilities.

>Document Management All documentation uploaded to the Aprio system is owned by the customer. Aprio employees do not have access to the information or documentation, unless by express consent and invitation of the customer.

>Independent Audits Aprio is AT101 (SAS70) SOC 2 Type 2, ISO 27001 and Smart Seal certified. Regular third-party audits continuously verify our applications' security.

>Risk Mitigation Aprio has an external legal firm hired to hold funds, pay bills and inform clients should Aprio Inc. go out of business for whatever reason. Clients then have three months from being informed to remove their data from Aprio servers.

>Service Level Guarantees Aprio provides a Service Level Agreement of 99.99% uptime.

Want to know more about how we guarantee total data security? We want you to sleep easy knowing that your data is protected by Aprio and we're happy to answer any questions you may have. Get in touch or call us toll-free at 1-855-55-APRIO (1-855-552-7746).