Management Approach: Cybersecurity and Privacy

Stantec provides robust IT security processes and practices, next-generation security systems, and cybersecurity awareness training for employees. Further, we respect and protect the privacy of employees, clients, investors, subcontractors, and others, ensuring that all personal and sensitive data in our possession or within our control is handled appropriately.

Our programs comply with applicable laws, including the General Data Protection Regulation (European Union), Defense Federal Acquisition Regulation Supplement (United States), and Cyber Essentials Plus (United Kingdom).

Stantec protects our systems and the people who entrust us with personal information in various ways:

Privacy Policy
Our Privacy Policy limits the collection and use of data to only what is needed to operate our business. In accordance with legislation, our programs ensure the accuracy, confidentiality, integrity, and security of information and provide the right to request and correct data.

IT Service Management System
Stantec is one of the few architectural and engineering firms to maintain an ISO 20000-1:2018-certified IT Service Management System (part of our Integrated Management System). This certification ensures service delivery processes (including security) meet the quality standards set by the British Standards Institute.

IT Security Programs
Our IT security programs maintain data confidentiality, integrity, and availability (whether data is stored on our premises or in the cloud). Comprehensive security systems include web filtering, intrusion protection, multifactor authentication, cloud access monitoring, cloud-based email filtering, next-generation firewalls, and advanced endpoint protection, detection, and response.

As well, we have stringent requirements for external access to our systems and wireless network and train our staff on cybersecurity best practices.

Fraud Detection
Stantec has platform-integrated IT fraud detection systems, and our programs are subject to regular audit. The director of Enterprise Risk Management leads an Integrity Management team and Fraud Risk Assessment Program. Any actual or potential security problems are reported to the chief information officer, Risk Management team, or Integrity Management team, as appropriate.

Incident Response
Stantec has comprehensive security incident response processes for identifying, containing, eradicating, and recovering from security incidents.

Underpinning our Security Incident Response program is a robust system that tracks security incidents, orchestrates incident response activities, and provides multi-jurisdictional information about breach notification regulations.

Training and Communication
Technology is not enough to fully shield us from cybersecurity attacks and privacy breaches. We also need our employees to identify—and stop or report—problems as soon as they see them.

Our comprehensive Cybersecurity Training Program gives employees the tools required to do this, and communication from management keeps employees informed about protecting assets and thwarting scams.

See Also
Management Approach: Integrated Management System