



## Management Approach: Cybersecurity and Privacy

Cybersecurity attacks can disrupt our business operations, resulting in financial losses and reputational damage. To address this risk, Stantec has implemented world-class security systems, security policies, processes, and practices, and invested in staff cybersecurity awareness training to help reduce the risk of network and system breaches. Furthermore, we are committed to respecting and protecting the privacy of individuals and ensuring that all personal or sensitive data within our possession or under our control is handled with due care. Stantec's programs explicitly protect employee and client information.

Our Privacy Officer oversees our privacy programs as part of the global risk management (legal) function. Cybersecurity is managed by our global IT function. The [Board Audit and Risk Committee](#) monitors and reviews risk management systems, including review and oversight of cybersecurity.

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

### IT Service Management

Stantec is one of the few architectural and engineering (A&E) services 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 Management

Stantec's Information Security Policy addresses the increasing variety and sophistication of cyberattacks and threats. This policy informs Stantec employees of the principles governing the holding, appropriate use, and disposal of information.

Stantec is one of the few architectural and engineering services firms to be globally certified against the ISO 27001:2018 information security standard and Cyber Essentials Plus (United Kingdom). Our approach to meeting these standards includes an Information Security Management System scoped to address personal, financial, and client information.

Stantec's Chief Information and Security Officer, who reports directly to the Executive Management team, is responsible for cybersecurity and oversees a group that is focused on managing IT security.

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. We have stringent requirements for external access to our systems and wireless network.

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 and Security Officer, Risk Management team, or Integrity Management team, as appropriate. The Chief Information and Security Officer directly informs the CEO of any actual or potential security incidents.

### Privacy Management

Stantec's privacy program complies with applicable laws in the territories in which we operate, including the General Data Protection Regulation (European Union), the Defense Federal Acquisition Regulation Supplement (United States), Cyber Essentials Plus (United Kingdom), and the Personal Information Protection and Electronic Documents Act (Canada).

The program is designed to ensure that Stantec limits the collection and use of data to only what is needed to operate our business and that we have an identified legal basis for our data processing activities (a more in-depth policy and practice is available internally to Stantec's systems for use by employees). In accordance with legislation, our programs ensure the accuracy, confidentiality, integrity, and security of information, and provide the right for individuals to request access to their personal data, and to request correction or erasure of data where appropriate.



---

Stantec posts an external facing [Privacy Notice](#) as a public statement to people whose data we may collect, use, and process to explain what we collect, what we use it for, and how we protect it. Also included is key information about who to contact and what rights individuals have concerning their data. Our [Privacy Policy](#) outlines how all Stantec employees should act and behave when using or accessing the personal data we collect. Specific privacy notices are provided to Stantec employees and as relevant where data is collected and processed for other purposes.

Stantec maintains a single centralized point of contact for raising privacy-related issues and concerns (including reporting of suspected personal data security breaches) at [privacy@stantec.com](mailto:privacy@stantec.com).

### **Incident Response**

Stantec tracks cybersecurity and privacy incidents and has a robust incident response program in place should the necessity to invoke it arise. Underpinning our Security Incident Response program is a robust system that orchestrates incident response activities and provides multi-jurisdictional information about breach notification regulations.

If a potential cybersecurity breach were to be identified, the IT Incident Response program would be immediately invoked to identify, investigate, contain, remediate, eradicate, and recover from the threat.

### **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 IT Security and Privacy Training gives employees the tools required to do this, and communication from management keeps employees informed about protecting assets and thwarting scams.

Through our [Partner Code of Business Conduct](#), we set similar expectations for our suppliers, partners, subcontractors, and subconsultants.

### **Accountability**

Stantec deems our commitments to be successful when we have no data security breaches or regulatory complaints and we meet all legally required timescales for dealing with data subject requests (access, corrections, updates, and deletions).

[See all Stantec Management Approaches](#)