Management Approach: Digital, Cybersecurity, and Privacy

By harnessing the power of technology, we can unlock limitless potential for both Stantec and our clients. But digital strategies come with various risks. Cybersecurity attacks or privacy breaches can disrupt our business operations, resulting in financial losses and reputational damage. To address, Stantec has implemented world-class security systems and governance.

Commitments And Practices

Our digital strategy is measured and thoughtful. We incorporate digital solutions as part of our efficiency and innovation strategies and do so with robust information technology (IT) policies, processes, practices, and safeguards in place. We are committed to respecting and protecting the privacy of our employees, clients, and business partners and all personal or sensitive data within our possession or under our control is handled with due care.

Stantec's Digital Center of Excellence manages our digital strategy while IT provides the essential foundation upon which the Center builds its capabilities. Cybersecurity is managed by our global IT function and privacy programs are managed as part of the global risk management (legal) function.

In Our Operations

Stantec innovates in the digital space in a responsible manner, with extensive governance that protects our systems and the people who entrust us.

Digital Center of Excellence

As architectural and engineering (A&E) professionals, we are trusted advisors. Our clients hire us for our qualified judgment to solve problems and develop solutions using a variety of tools. To do this work, clients continually ask for faster delivery, fewer surprises, and clearer defensibility. Digital solutions help Stantec fulfill these requirements.

Stantec integrates digital technologies and capabilities to improve the efficiency of our operational practices and the work we do every day for our clients. Our Digital Center of Excellence, led by a Chief Digital Officer, encompasses our digital strategies, platforms and architecture, governance, and talent and skill development.

The Center has established a common digital architecture, platform, and operating model, upon which digital services, products, and assets are built. This includes developing new tools that solve unique challenges and integrating automation directly into the tools our teammates already use to explore more design options, reduce errors, and respond to client challenges in real time.

Artificial Intelligence

While Stantec’s Digital Center of Excellence works with a plethora of digital options, artificial intelligence (AI) is of particular focus. Stantec recognizes AI as a powerful enabler of business transformation, and we’re staying close to the impacts and outcomes it makes possible. Incorporating AI technology into our work can result in significant efficiencies and gains for both Stantec and our clients.

AI helps manage scale, consistency, and document-heavy work so our teams can stay focused on design intent, risk tradeoffs, and client accountability. AI enables earlier-option evaluation, reduces late-stage conflicts, and improves quality control. The opportunity isn’t the technology itself; it’s the ability to make better decisions earlier and deliver stronger outcomes across the asset lifecycle.

The Digital Center of Excellence has established a Stantec-wide AI foundation grounded in pragmatism, purpose, and governance so we can adopt and expand technologies quickly, yet securely and effectively. Strategically, we take a partner-agnostic approach. Our advantage isn't tied to a single technology; it's our ability to operationalize AI without compromising trust, governance, or professional standards.

The AI-specific governance approaches Stantec has put in place, so far, include

- An AI Tools Policy that ensures compliance with laws, regulations, data privacy, security, and confidentiality standards
- Tools, training, and governance that support Stantec's conscientious adoption of AI, including a new Responsible Use of AI Tools practice and an AI risk assessment framework
- Standardizing our GenAI tool usage with Microsoft Copilot to ensuring data privacy and security and reducing the risk of confidential data leakage from non-approved tools
- Monitoring the return on investment from AI investments to ensure responsible resource allocation and alignment with corporate governance principles

AI strengthens Stantec's professional model, enhances predictability, allows for better delivery, creating new revenue opportunities, and supporting margin expansion. Stantec is committed to using AI wisely and encourages its responsible, safe, and strategic use.

IT Service Management

Stantec is one of the few A&E firms to maintain a global ISO/IEC 20000-1:2018-certified IT Service 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 employees of the principles governing the holding, appropriate use, and disposal of information.

Stantec is also one of the few A&E firms to be globally certified against the ISO 27001:2022-certified Information Security Management and United Kingdom Cyber Essentials Plus. Our approach to meeting these standards includes an Information Security Management System scoped to address personal, financial, and client information.

Stantec is certified under the Cybersecurity Maturity Model Certification (CMMC) Program for the US Department of Defense, with third-party audits from an approved CMMC audit organization and the Defense Contract Management Agency.

Stantec's Chief Information and Security Officer, who reports directly to the C-Suite, is responsible for information, cyber, and technology security 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, multi-factor 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 and standards in the territories in which we operate, including the General Data Protection Regulation(European Union), Data Protection Act 2018 (United Kingdom), and the Personal Information Protection and Electronic Documents Act and Personal Information Protection Act (Canada), and United States state privacy laws, such as the California Consumer Privacy Act (United States).

Our privacy 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. 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. A more in-depth privacy policy and practice is available internally to Stantec's systems for use by employees. 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.

Incident Response

Stantec tracks cybersecurity and privacy incidents, and has a robust Security Incident Response program in place that orchestrates incident response activities and provides multi-jurisdictional information about breach notification regulations.

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

Training and Communication

Policies and technology are not enough to fully shield us from inappropriate AI use, cybersecurity attacks, and privacy breaches. We also need our employees to be aware and identify—and stop or report—problems as soon as they see them.

Our mandatory, annual 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.

Supporting Clients

The importance Stantec places on digital tools can be seen in the topics covered by our Future Technology strategic growth initiative.

Specific to AI, Stantec is using it to improve efficiency in our operations, create measurable gains in productivity in client work, and harnessing proven AI technologies to develop solutions for clients. We've moved beyond isolated AI pilots and are now embedding AI directly into delivery workflows, while keeping professional accountability. For Stantec, AI is an opportunity amplifier, creating efficiencies, enabling new work, new service lines, and deeper client relationships. Clients who are building AI-enabled infrastructure and operations need trusted partners like Stantec who understand both engineering and data.

In addition to the processes, new tools, and safeguards noted above, Stantec has procedures in place to protect client information tailored to the client type, facility type, and level of confidentiality as required.

With Our Supply Chain

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 our digital tools meet our operational and client needs, safeguards protect the integrity of our digital solutions, 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).

Stantec's C-Suite monitors, reviews, and oversees our digital, cybersecurity, and privacy programs with additional oversight from our Board Audit and Risk Committee.

Material Topic / Value Chain Nodes Covered:

Digital, Cybersecurity, and Privacy / Operations, Downstream (Clients), Upstream (Suppliers and Partners)

See all Stantec Management Approaches