Information Security Policy

April 5, 2023

Purpose

The purpose of this information security policy is to safeguard information belonging to, or entrusted to,Stantec and its stakeholders (e.g., clients, employees, and all other 3rd parties). “Information” is data that is received, stored, processed, created, transformed, or transferred by Stantec. This policy informs Stantec employees of the principles governing the handling, appropriate use, and disposal of Information.

The objectives of Stantec are that:

- Information will always be protected against unauthorized access, disclosure, modification,destruction, or misuse.
- Staff will review and abide by Stantec’s Acceptable Use Policy without exception.
- Access to Information will only be provided to Stantec authorized users and will be approved according to Stantec’s access approval policies and procedures.
- Information will be managed and controlled in alignment with all regulatory, contractual, andlegal requirements, including regional jurisdictional privacy regulations.
- The confidentiality and integrity of Information will always be maintained and the availability of Information and the systems on which it resides will be maintained as necessary for service delivery.
- Information should be marked and classified based on its intended audience or client requirements and will only be stored in secure locations sanctioned and approved by Stantec and in accordance with our policies and practices for information governance.
- Information will be retained and disposed of in strict accordance with Stantec’s records retention policies and practices.
- The confidentiality of personally identifiable Information will always be maintained.
- The physical security of our facilities and the environments in which we operate will berespected and maintained.
- The security of Stantec’s corporate network will be maintained and no unauthorized connectionto the network will be allowed.
- All Information security incidents will be reported immediately to the IT Service Center.
- Employees will periodically review, be aware of, and consider the objectives of this Policy when performing work activities.

Infringement of this policy may result in disciplinary action, up to and including termination of employment or criminal prosecution.

Our Information Security Policy is a core component of Stantec’s Information Security ManagementSystem [ISMS] and will be updated on a continuous basis to align with changes to the evolving cybersecurity threat landscape.

All changes to the Information Security Policy are under the control of the change management process.