The St. Lawrence
Seaway Management
Corporation

Corporation de Gestion
de la Voie Maritime
du Saint-Laurent

DATA PROTECTION CONDITIONS

Last Updated: October 26, 2022

Contents

DATA PROTECTION CONDITIONS

The following Data Protection Conditions set forth the parties' mutual understanding relating to the privacy and security of SLSMC Information, access to SLSMC systems and Contractor's business continuity planning program.

1. Definitions

1.1 For the purposes of this document, the terms below have the following meanings whenever capitalized. All other terms that are capitalized but not defined have the definitions set out in the body of this document or other documents forming part of the Contract.

"**Claims**" means all claims, requests, allegations, assertions, complaints, petitions, demands, suits, actions, proceedings, causes of action, and judgments.

"**Costs**" means expenses of any kind, including legal fees, litigation costs, investigatory costs, costs of providing notice to any person or organization in the event of a Data Incident, and costs of providing consumer protection services to any person in the event of a Data Incident, including credit monitoring or identity restoration services.

"**Data Incident**" means any reasonably suspected or actual unauthorized access to or acquisition, disclosure, use, or loss of SLSMC Information (including hard copy records) or breach or compromise of Contractor's Security Program that presents a threat to any SLSMC Information or SLSMC system.

"**DPC**" means these Data Protection Conditions.

"**Privacy and Security Requirement**s" means to the extent applicable to SLSMC or Contractor:

a) federal, provincial, local, and international laws, rules and regulations, and governmental requirements currently in effect and as they become effective, relating in any way to the privacy, confidentiality, integrity, availability, or security of SLSMC Information, including but not limited to the Personal Information Protection and Electronic Documents Act (Canada) and any successor legislation;

b) industry standard measures of protection specified in the Contract Documents concerning privacy, data protection, confidentiality, integrity, availability, or security of information (e.g. information security controls), including without limitation, the Payment Card Industry Data Security Standard (if applicable), and any other similar standards;

c) all policies, statements, or notices that are provided to Contractor by SLSMC in writing, as set out in the Contract Documents; and

d) all controls required by SLSMC, including secure coding standards as set out in the Contract Documents.

"**Security Program**" means a comprehensive written information security program described below in Section 5 (Data Security Program).

"**Security Review**" refers to SLSMC's assessment and evaluation of all, or select components of, Contractor's Security Program.

"**SLSMC Information**" means the following, regardless of form or the media in which it is maintained, that may be accessed, used, or disclosed to Contractor in connection with or incidental to the performance of Services for or on behalf of SLSMC or by any other means:

a) Personal Information: Any information relating to an identified or identifiable individual irrespective of whether such individual is a SLSMC customer, employee, or other status (including, but not limited to, name, postal address, email address, telephone number, date of birth, social insurance number, driver's license number, other government-issued identification number, financial account number, credit or debit card number, insurance ID or account number, health or medical information, consumer reports, background checks, biometric data, digital signatures, any code or password that could be used to gain access to financial resources, or any other unique identifier).

b) Sensitive Information: Any information identified as "Classified", "Sensitive", "Confidential" or similar marking indicating the highly sensitive nature of the information and may include but not be limited to (i) Personal Information if of a particularly sensitive nature or (ii) federal government information relating to Canada's national interests such as R2 or MARSEC information.

c) Non-Public Information: Non-public confidential business information and information that Contractor should reasonably believe to be confidential.

"**SLSMC System**" means any SLSMC owned or licensed IT/IS/OT systems, such as, but not limited to, software developed in house or acquired, databases, Web applications, server infrastructure on premise or hosted, network infrastructure including leased and co-owned services, Cybersecurity Safeguards, end user devices, telecommunication equipment, and any other equipment that are form the electronic Enterprise and Industrial Control environments.

"**Subcontractor**" means any contractor affiliated or other direct or indirect agent acting on the behalf of the Contractor that processes or has access to SLSMC Systems or SLSMC Information.

2. Acknowledgement

2.1 Contractor acknowledges and accepts that it is solely responsible for the protection of confidentiality, safeguarding and security of SLSMC Information and, as applicable, controlling access to SLSMC systems in accordance with equal or better standards described in this DPC, whether or not such SLSMC Information is transferred or the SLSMC systems are accessed by a third-party Subcontractor, licensor or supplier or other such third party authorized by Contractor.

3. Scope

3.1 These Data Protection Conditions apply to all SLSMC Information and all access to SLSMC Systems in connection with the Contract.

4. Supervision

4.1 Contractor shall exercise necessary and appropriate supervision over its personnel and others acting on its behalf to maintain confidentiality, integrity, availability, and security of SLSMC Information and, as applicable, SLSMC systems.

5. Data Security Program

5.1 Contractor represents and warrants that it has implemented and shall maintain a Security Program that, at minimum, complies with the Privacy and Security Requirements. Contractor's Security Program must be comprised of appropriate administrative, technical, and physical safeguards that assure the confidentiality, availability, integrity, and security of SLSMC Information and SLSMC systems and includes the minimum safeguards in the list below to the extent required by the Contract Documents unless deviations are approved by SLSMC in writing:

a) **Information security policies** are documented by the Contractor using a security control framework based upon an accepted industry standard for governing the information security practices (e.g., NIST, ISO, etc.).

b) **User authentication controls**, including secure methods of assigning, selecting, and storing access credentials, restricting access to active users, and blocking access after a reasonable number of failed authentication attempts. Multi-Factor Authentication (MFA) is used for any user accessing Contractor systems supporting services performed for SLSMC pursuant to this Contract.

c) **Secure access controls**, including controls that limit access to SLSMC Information and SLSMC systems to individuals that have a demonstrable genuine business need-to-know, supported by appropriate policies, protocols, and controls to facilitate access authorization, establishment, modification, and termination.

d) **Appropriate and timely adjustments to Contractor's Security Program** based on: periodic risk assessments; regular comprehensive evaluations (such as third-party assessments like SSAE SOC 2, Type 2 audits) of Contractor's Security Program; monitoring and regular testing of the effectiveness of safeguards; and a review of safeguards at least annually or whenever there is a material change in Contractor's technical environment or business practices that may implicate the confidentiality, availability, integrity, or security of Contractor's information systems.

e) **Training and awareness programs** designed to ensure Contractor personnel and others contracted by Contractor, or acting on Contractor's behalf, are aware of and adhere to Security Program policies, procedures, and protocols.

f) **Performance of security testing** on applications or software code developed on behalf of SLSMC to ensure that the Service is secure against the vulnerabilities described in the latest version of the OWASP Top Ten List.

g) **Monitoring of systems** designed to ensure data integrity and prevent loss or unauthorized access to, or acquisition, use, or disclosure of, SLSMC Information and, as applicable, SLSMC systems.

h) **Technical security measures**, including firewall protection, IDS/IPS, antivirus protection, vulnerability scans, security patch management, secure system configuration, logging of access to or use or disclosure of SLSMC Information, intrusion detection, and encryption of data in transit and at rest.

i) **Vulnerability management** and patching include a process for remediating critical vulnerabilities with 48 hours, high vulnerabilities with 7 days, and medium vulnerabilities within 30 days.

j) **Network and communication controls** must be implemented to ensure that only authorized devices are provisioned network access when physically connected to the network. All Contractor controlled wireless connections must be secured utilizing Wi-Fi Protected Access 2 ("WPA2") or better security protocol.

k) **Physical facility security measures**, including access controls, designed to restrict access to SLSMC Information and, as applicable, SLSMC systems to individuals described in item (b) above. Equipment must be protected from environmental threats and hazards, and from power failures and other disruptions caused by failures in supporting utilities.

l) **Physical or logical segmentation of SLSMC Information** from data of others.

m) **Risk Management process** including a risk assessment methodology must be defined by the Contractor. Contractor must conduct regular risk assessments to ensure security controls are properly operating and document the results and action plans.

n) **Segregated development/testing/production environments**: Development, testing, and operational environments are separated to reduce risks of unauthorized access or changes to the operational environment.

o) **Background checks** on personnel and others acting on behalf of Contractor who otherwise will or are reasonably anticipated to have access to SLSMC Information and, as applicable, SLSMC systems and only authorize access to personnel and others that have cleared at the time of hire such background checks. Contractor shall not knowingly permit personnel or others that have been convicted of theft or have any fraud related convictions for which a pardon has not been granted access to SLSMC Information or SLSMC systems.

6. Transfer of SLSMC Information

6.1 SLSMC Information:

a) shall not be stored on or transported via a laptop, any other mobile device, or any removable storage media, including USB, thumb drives, DVDs, or CDs, unless such devices or media are encrypted using an encryption methodology approved in writing by SLSMC;

b) must be transferred via secure FTP or other protocol or encryption methodology such as TLS v1.2 or higher or approved in writing by SLSMC; and

c) shall be physically moved, removed, destroyed or transferred only according to controls developed or approved in writing by SLSMC.

7. Data storage

7.1 Contractor shall encrypt all SLSMC Information regardless of its location at rest and in transit.

7.2 Contractor shall utilize dedicated encryption keys. All encryption keys used to protect SLSMC Information shall be uniquely associated to SLSMC.

7.3 All keys will be protected against modification; secret and private keys need to be protected against unauthorized disclosure.

7.4 Contractor shall implement full disk encryption on any Contractor controlled personal computer device which may access, store, process, transmit, or create SLSMC Information. All such encryption shall minimally meet the Advanced Encryption Standard with a 256-bit cypher key (“AES-256”) as outlined in the Federal Information Processing Standards publication 197 (“FIPS 197”).

7.5 If tapes are used for system backup, such tapes shall be encrypted and appropriately inventoried and logged as to location and planned destruction date.

8. Data Residency

8.1 SLSMC Information may not be transferred, stored, or processed outside Canada for any reason without prior written approval from SLSMC, inclusive of transfers to Subcontractors or agents, notwithstanding the provisions of Section 10 (Third Party Processors).

9. Management of Data Incidents

9.1 Data Incidents must be managed as follows:

a) Contractor must immediately notify SLSMC's Operations Centre by phone at (613) 932-5170, ext. 2232 (Quebec) or ext. 5370 (Ontario) and SLSMC's Cybersecurity Department by email at cybersecurity@seaway.ca of any Data Incident.

b) While the initial phone notice may be in summary form, a comprehensive written notice must follow within 48 hours and directed to SLSMC's Cybersecurity Department.

c) The notice shall identify Contractor's point of contact for all matters relating to the Data Incident, summarize in reasonable detail the nature and scope of the Data Incident (including a description of SLSMC Information affected) and the corrective action already taken or to be taken by Contractor. The notice shall, as soon as possible, be supplemented with additional detail reasonably requested by SLSMC.

d) Contractor shall promptly take all necessary corrective actions and shall cooperate with SLSMC to investigate the Data Incident, mitigate adverse effects, and prevent recurrence. Such cooperation shall include responding to SLSMC's inquiries about the Data Incident in a timely fashion.

e) The parties shall collaborate on whether it is necessary or advisable to provide notice of the Data Incident to any person, governmental entity, the media, or other party. The parties shall collaborate on the content of the notice. SLSMC will make the final determination as to whether notice will be provided and to whom, the content of the notice, and which party will be the signatory to the notice.

10. Third Party Processors

10.1 Contractor may transfer, disclose, or otherwise provide access to SLSMC Information (including through use of third-party hosting or cloud services) or SLSMC systems to a Subcontractor or agent if SLSMC has provided its prior approval in writing to such transfer, disclosure or access to the identified third party, which approval will be conditional on the following being met:

a) the Subcontractor or agent, including the proposed access to SLSMC Information or SLSMC system by the Subcontractor or agent, has been evaluated in a manner substantially similar to SLSMC's Security Review of Contractor, to SLSMC's complete satisfaction;

b) the Subcontractor or agent maintains an information security program substantially equivalent to the Security Program required of Contractor by this DPC as demonstrated to SLSMC and to SLSMC's complete satisfaction;

c) Contractor has executed an agreement with the Subcontractor or agent that is substantially equivalent to this DPC, as demonstrated to SLSMC to SLSMC's complete satisfaction; and

d) the Subcontractor or agent has a demonstrable genuine business need-to-know or business need-to-access the SLSMC Information or SLSMC system to which it is provided access for purposes of the delivery of Services in accordance with the Contract.

11. Notice of Process

11.1 In the event Contractor receives a governmental or other regulatory request for, or legal process or demand requesting any SLSMC Information or access to SLSMC system, Contractor shall immediately notify SLSMC in order that SLSMC will have the option to respond.

12. Requests or Complaints by Individuals

12.1 Contractor shall immediately notify SLSMC in the event that Contractor receives: (i) requests from individuals relating to SLSMC Information, including requests to access or rectify Personal Information; or (ii) complaints of any kind from individuals relating to the privacy, confidentiality, or security of SLSMC Information. Contractor shall not respond to any such request or complaint without SLSMC's prior written approval.

13. Use Restrictions

13.1 Unless SLSMC provides prior written approval, Contractor shall not use, access, disclose, reconfigure, or aggregate SLSMC Information, whether or not in anonymized form, nor permit any of the foregoing, for any purpose other than performing Services pursuant to the Contract, fulfilling the obligations of this DPC, or as strictly necessary to comply with law.

14. SLSMC Security Review

14.1 SLSMC may conduct a complete Security Review no more than once per year, or more frequently in the event of any Data Incident and Contractor shall fully cooperate in the Security Review, including making available and/or providing relevant information required for the Security Review. The Security Review may be conducted on-site by SLSMC personnel or SLSMC's contracted third party assessors or through surveys and interviews, at the option of SLSMC. When an on-site Security Review will be conducted, SLSMC shall provide Contractor with reasonable advance notice of not less than 15 business days, except in the event of a Data Incident or if SLSMC has a reasonable basis to believe Contractor may not be in compliance with this DPC, in which case advance notice shall be not less than 48 hours.

14.2 At SLSMC's request, Contractor shall provide SLSMC copies of its data privacy and security policies and procedures that apply to SLSMC Information and, as applicable, access to SLSMC systems. Contractor also may be asked, upon SLSMC's reasonable request, to submit written responses to questions regarding its privacy and information security practices that apply to SLSMC Information and, as applicable, access to SLSMC systems. Contractor shall submit written responses within 10 business days of receipt of SLSMC's request.

14.3 As they become available throughout the term of this Contract, Contractor shall provide SLSMC with notice of findings that are likely to adversely impact SLSMC Information or SLSMC systems that are identified through any security assessment or review of Contractor's systems or Security Program performed by Contractor or a third party, including vulnerability and penetration assessments. Notice of these findings may be provided in the form of a written summary. Contractor shall keep SLSMC informed of its remediation efforts to address any negative findings.

15. Compliance

15.1 Contractor shall at all times comply with the SLSMC-approved Privacy and Security Requirements specified in the Contract Documents.

16. Security Certification

16.1 Contractor shall maintain a level of security certification or assessment consistent with best practices and conducted by a qualified third party reasonably acceptable to SLSMC. Such certifications shall be provided to SLSMC upon reasonable request.

17. Indemnification

17.1 Contractor shall indemnify, defend, and hold harmless SLSMC for and from any Claims, and reimburse SLSMC for or bear any Costs, related to any Data Incident or Contractor's noncompliance with this DPC except to the extent Claims and Costs are caused by SLSMC's negligence.

18. Termination

18.1 SLSMC may terminate the Contract, in the event: (i) of a Data Incident that SLSMC determines is likely to have a substantial adverse impact on SLSMC's relationship with its customers, employees, the federal government or any other stakeholder or may otherwise substantially harm its reputation; (ii) of a material violation of this DPC by Contractor, including any violation of Section 10 (Third Party Processors); (iii) of any material misrepresentation made in connection with any Security Review, assessment, or process described in Sections 10 (Third Party Processors) or 14 (SLSMC Security Review); or (iv) that Contractor or a third party reviewed pursuant to Section 10 (Third Party Processors) fails to timely or effectively remediate material adverse findings from a Security Review, assessment, or other process described in Sections 10 (Third Party Processors) or 14 (SLSMC Security Review), as applicable. This Section in no way limits any other termination rights provided under the Contract.

19. Secure Return or Disposal; Termination of Access

19.1 Contractor shall return or, if requested, dispose of SLSMC Information in its possession, custody, or control: (i) if no longer needed for SLSMC's business or legal purposes or upon termination of the Contract of which this DPC forms a part, whichever is longer; or (ii) upon SLSMC's direction which direction may be given at any time.

19.2 Notwithstanding the foregoing, Contractor will be permitted to retain: (i) SLSMC Information for a longer period if such retention is strictly necessary to meet Contractor's legal compliance obligations, is done pursuant to Contractor's fully implemented and documented records management program, and is limited to the minimum SLSMC Information and minimum retention period needed to meet these obligations; and (ii) backup media containing SLSMC Information for so long as is permitted by Contractor's fully implemented and documented records management program, which retention shall not be indefinite and shall not exceed industry standards.

19.3 Any disposal of SLSMC Information must ensure that SLSMC Information is rendered permanently unreadable and unrecoverable.

19.4 To the extent Contractor accesses or has contact with SLSMC systems, Contractor must ensure that such access is discontinued upon termination of the Contract.

19.5 Upon reasonable notice and if requested by SLSMC, Contractor shall provide SLSMC with a certification by an officer attesting to Contractor's compliance with this Section.

Appendices to the DPC

Appendix A – Hosting facilities, Subcontractors and affiliates
Appendix B – Technical and organizational security measures

APPENDIX A

Hosting facilities *Where data is stored*	
Full name and address of the organization	Nature of processing
	Type of engagement

Subcontractors *Full list of all companies being used by the Contractor for the work being done by this Contract, including their physical location*

Affiliates *Full list of all affiliated companies being used by the Contractor for the work being done by this Contract, including their physical location*

APPENDIX B

Description of the technical and organizational security measures implemented by the Contractor in accordance with this DPC