Appendix D.1 - Mandatory Requirements Form

| **ID** | **Requirement** |
| --- | --- |
| M-1 | Proponent must confirm employees working on the City’s network are willing to sign a Non-Disclosure Agreement and complete a security clearance. |
| Response: | |
| M-2 | Proponent must confirm they will use Microsoft Teams or Virtual Private Network (VPN) to access any software on the City’s network. |
| Response: | |
| M-3 | Proponent must agree to have software and their network subject to a Threat Risk Assessment(s) (TRA), Security Audit(s), security scan, and/or penetration test. If this has already been completed, provide evidence and documentation. |
| Response: | |
| M-4 | Proponent must disclose whether their company and/or software has ever had a security breach or experienced a cybersecurity event that compromised the system or client base. If yes, describe the nature of the breach(es) or event and how it was resolved. |
| Response: | |
| M-5 | Proponent must confirm they will permit the City of Saint John to connect or add their solution to the City’s Security Information and Event Management (SIEM) system. |
| Response: | |
| M-6 | Proponent must confirm all mandatory requirements which apply to the Proponent will also apply to any sub-contractors or 3rd Party and that the amount of information shared with sub-contractors must be limited to the minimum amount required for the specific purpose. |
| Response: | |
| M-7 | City data stored on the Proponent’s servers must be on Canadian data centers in geographically diverse locations. Describe how this requirement will be met. |
| Response: | |
| M-8 | City data stored on the Proponent’s servers must be physically or logically separated from other clients’ data. Describe how this requirement will be met. |
| Response: | |
| M-9 | Public facing user interfaces must be configurable in both French and English languages. Describe how this requirement will be met. |
| Response: | |