INFOSECTRAIN

THIRD PARTY INFORMATION SECURITY ASSESSMENT CHECKLIST

BUILD SECURITY GOVERNANCE

Vendor's Information

Requested information	Response
Vendor Name	
Name of person and position filling this questionnaire	
Completer address of the Vendor	
Vendor Telephone Number	
Vendor Contact Name & Job Title	
Vendor Contact Email	
Vendor D&B Number	
Is the vendor a public or private company?	
How long has the vendor been in business under any name?	
Does the vendor hold any Information security related certifications?	
Type of legal entity and state of incorporation	
Are there any material claims or judgements against the vendor?	
If yes, describe the impact it may have on the services in scope of this document?	
Has the vendor sufffered a data loss or a security breach in the last 3 years?	
If yes, please describe the loss or breach.	
What is the physical address of the backup site?	
Are there any additional locations where Scooped System and Data is stored?	
If yes, please provide each location (address, city, state, or country)	

Information Request List

Please provide a copy of the documents listed below. Redacted copies are acceptable. We have limited our documentation request to those that are directly relevant to our assessment.

Please provide the following documents.
Please explain unavailability or any deviations in column B.

Document (A)	**Notes** (B)
Information Security Strategy	
Information Security Policy	
Acceptable Use Policy	
Access Control Policy	
Asset Management Policy	
Incident Response Plan	
Business Continuity Plan	
Password Policy	
Physical Security Policy	
Change Management Policy	
System Development Lifecycle (SDLC) Policy	
Patch Management Policy	
Encryption Policy	
Recent Vulnerability Scan or Penetration Test Results	
Recent Application Security Scan Results	
Implemented encryption types	
Information Security Certifications (e.g. ISO 27001, SOC, PCI)	
BCP Testing Report	
BCP Plan	
BCP Policy	
SOC2 Report	

RISK Questions

Vendor Question	Vendor Response (Y/N)	EVIDENCE
Information Security Governance		
Q1. Does the organization have a dedicated information security position? (Officer/Manager/Practitioner)		
Q2. Does the organization have an Information Security Framework?		
Q3. Does the organization have a Information Security Strategy?		
Q4. Does your organization conduct risk assessments at least annually?		
Q5. Does your organization have an information security program in place?		
Q6. If your organization has an information security program, does it apply to all operations and systems that process sensitive data?		
Q7. Are relevant staff and managers professionally certified in information security?		
Q8. Does organization have security metrics to measure Information Security Program?		
Q9. How do you prioritize your organization's most critical assets?		
Q10. Has your organization conducted a risk assessment to identify the key objectives that need to be supported by your information security program?		
Q11. Has your organization identified critical assets and the functions that rely on them?		
Q12. Do you have a process in place to monitor federal, state, or international legislation or regulations and determine their applicability to your organization?		
Q13. Does your information security function have the authority it needs to manage and ensure compliance with the information security program?		
Q14. Is someone in the information security function responsible for liaising with units to identify any new security requirements?		
Q15. Does the information security function report regularly to institutional leaders and the governing board on the compliance of the institution to and the effectiveness of the information security program and policies?		
Q16. Is responsibility clearly assigned for all areas of the information security architecture, compliance, processes and audits?		
Q17. Does your organization outsource functionalities related to security management?		

Vendor Question	Vendor Response (Y/N)	EVIDENCE
Policies and Procedure		
Q18. Does your organization have an Information Security Policy?		
Q19. Does your organization document, publish, and enforce security policies?		
Q20. Does your organization document and enforce HR policies?		
Q21. What is the time interval at which security policies are reviewed and updated?		
Q22. Does your organization document and enforce policies for the authorized use of company email, internet, and intranet?		
Q23. Does your organization document and enforce policies regarding the storage, use, and disposal of sensitive data?		
Q24. Do policies and procedures adhere to and comply with privacy laws and regulations related to the security, concealment, and safeguarding of customer data?		
Q25. Is a complete set of your organisation’s security policies available for review?		
Q26. Are the penalties associated with noncompliance to your organization’s policies well documented?		

Vendor Question	Vendor Response (Y/N)	EVIDENCE
Compliance with Legal Requirements - Identification of applicable legislation		
Q27. Do you have a process to identify new laws and regulations with IT security implications?		
Q28. Has the vendor experienced a legally reportable data breach within the past seven years?		
Q29. Do you have procedures for the preservation of electronic records and audit logs in case of litigation hold?		
Q30. In the event of a security incident, do you provide the consumer with the ability to perform digital forensics?		
Q31. Are any information systems audit tools (e.g., software or data files) accessible to any users in any unprotected area?		
Q32. Are there procedures to ensure compliance with legislative, regulatory, and contractual requirements on the use of material where intellectual property rights may be applied and on the use of proprietary software products?		
Q33. How does your organization stay updated on changes in laws and regulations that impact your business?		
Q34. Does your organization implement appropriate security controls to comply with relevant data protection and privacy laws and regulations (e.g., GDPR, CCPA, etc.)?		
Q35. Has your organization ever been involved in any legal disputes or infringement claims regarding intellectual property rights? If yes, please provide details.		
Q36. Does your organization have policies and procedures in place to prevent corruption, bribery, and unethical practices?		
Q37. Does your organization have a formal process for reporting and addressing compliance issues or violations? If yes, please describe the process.		
Q38. Can your organization provide documentation, such as certifications, licenses, or audit reports, to demonstrate compliance with relevant laws and regulations?		
Q39. Is there a compliance risk management system that addresses the quality and accuracy of reported consumer data?		
Q40. How long does your organization retain records related to compliance? What is your organization's process for record retention and disposal?		
Q41. Has your company experienced any data breaches in the last 5 years? If so, please describe.		

Vendor Question	Vendor Response (Y/N)	EVIDENCE
Privacy		
Q42. Are identified privacy risks and associated mitigation plans formally documented and reviewed by management?		
Q43. Is there a Privacy management program?		
Q44. Do you have a privacy policy? If yes, can you provide a copy?		
Q45. Are reasonable resources (in time and money) allocated to mitigating identified privacy risks?		
Q46. Is personal information collected directly from individuals? If yes, describe.		
Q47. Are there controls in place to ensure that the collection of personal information is limited?		
Q48. Are there controls in place to ensure that the collection and usage of personal information is limited and in compliance with applicable law?		
Q49. Is there a compliance risk management system that addresses the quality and accuracy of reported consumer data?		
Q50. Do policies and procedures adhere to and comply with privacy laws and regulations related to the security, concealment, and safeguarding of customer data?		
Q51. Does the business area have an inventory of where personal information is collected, stored, processed, or managed?		
Q52. Are the penalties associated with noncompliance to your organization's policies well documented?		
Q53. Are there documented agreements in place with external organizations, when transferring data between a company entity and an external organization, requiring the external organization to comply with the company's privacy expectations?		
Q54. Are identified privacy risks and associated mitigation plans formally documented and reviewed by management?		
Q55. Is there a compliance risk management system that addresses the quality and accuracy of reported consumer data?		
Q56. Are there regular privacy risk assessments conducted? If yes, provide frequency and scope. If no, explain the reason.		
Q57. Are controls in place to ensure that the collection and usage of personal information is limited and in compliance with applicable law?		
Q58. Are you transparent about your data collection and processing practices?		
Q59. How do you inform users about any updates or changes to your privacy policy?		
Q60. How do you obtain user consent for data collection and processing?		

Q61. What security measures do you have in place to protect personal data?		
Q62. Is personal data processed or stored outside the country? If yes, how is cross-border data transfer regulated?		

Vendor Question	Vendor Response (Y/N)	EVIDENCE
Personnel Security		
Q63. Are background checks conducted for all prospective employees who have access to sensitive information?		
Q64. Are employees required to attend mandatory annual information security training?		
Q65. Do any subcontractors/third parties have access to sensitive data?		
Q66. Does your organization store, transmit, or access PII (Personally Identifiable Information) or PHI (Protected Health Information)?		
Q67. Do you have an ongoing training program in place to build skills and competencies for information security for members of the information security function?		
Q68. Do you conduct Security awareness training for employees?		
Q69. Do you conduct Post Awareness Training Phishing Campaigns?		
Q70. Verify that personnel attends security awareness training upon hire and at least annually.		
Q71. Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of data security.		
Q72. Does your awareness and education plan teach proper methods for managing information Security and personal/private information (Social security numbers, names, addresses, phone numbers, etc.)?		
Q73. Are your employees able to identify and protect classified data, including paper documents, removable media, and electronic documents?		
Q74. Are employees taught to be alert to possible security breaches?		
Q75. Is responsibility clearly assigned for all areas of the information security architecture, compliance, processes and audits?		

Vendor Question	Vendor Response (Y/N)	EVIDENCE
Physical Security		
Q76. Does your organization have a designated Physical Security Manager?		
Q77. Does organization have any Physical Security Policy?		
Q78. Does Controls access to server rooms and follows the least privilege and need-to-know practices for those facilities?		
Q79. Does Controls access to secure areas. e.g. key distribution management (both physical and electronic), paper/electronic logs, monitoring of facility doors, etc.?		
Q80. Are special safeguards in place for computer rooms. e.g. cipher locks, restricted access, room access log, card swipe access control, etc.?		
Q81. Does Positions desktops, which display confidential information, in order to protect from unauthorized viewing.?		
Q82. Does Escorts all visitors in computer rooms or server areas. ?		
Q83. Does appropriate environmental controls, where possible, to manage equipment risks. E.g. fire safety, temperature, humidity, battery backup, etc.		
Q84. Does Team follow forensically secure data destruction processes for confidential data on hard drives, tapes & removable media when it's no longer needed and at the end of the contract term.		
Q85. Does organization have Redundant UPS for Critical Server?		
Q86. Does external signage indicating the content or value of the server room or any room containing confidential customer information.		

Vendor Question	Vendor Response (Y/N)	EVIDENCE
Contingency Plan		
Q87. Does your Company have a written Policy for BCP?		
Q88. Does your Company have a BCP/DR Plan?		
Q89. Does your Company have emergency procedures and responsibilities documented and stored securely at multiple sites?		
Q90. Does your Company store backup media in a secure manner and controls access?		
Q91. How frequently are backups conducted? (choose from drop list)		
Q92. Is the BCP/DR Plan tested on a regular basis?		
Network Security		
Q93. Are Firewalls used to isolate systems containing sensitive data?		
Q94. Examine documented procedures to verify there is a formal process for testing and approval of all network connection		
Q95. Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:		
Q96. Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to data, including any networks.		
Q97. Does your Solutions offer Content security to protect your network from viruses, spam, spyware, and other attacks?		
Q98. Are employees able to access sensitive information from personal devices?		
Q99. Are there intrusion detection/prevention systems (IDS/IPS) in use?		
Q100. Does a Secure wireless network provide safe network access to visitors and employees on the go?		
Q101. Does Compliance validation make sure that any device accessing the network meets your security requirements?		
Q102. Is multifactor authentication used?		

Vendor Question	Vendor Response (Y/N)	EVIDENCE
Access Control		
Q103. Are unique user IDs required for all users?		
Q104. Are complex passwords required for all users?		
Q105. How often are passwords changed?		
Q106. Ensures that critical data, or systems, are accessible by at least two trusted and authorized individuals in order to limit having a single point of service failure.		
Q107. Ensures that users have the authority to only read or modify those programs or data which are needed to perform their duties.		
Q108. What is the time frame that access is revoked for terminated employees or contractors? (choose from drop list)		
Operations Security and Encryption		
Q109. Are anti-malware applications installed on all systems?		
Q110. How frequently are antivirus signature files updated?		
Q111. Is there a data loss prevention (DLP) tool in use?		
Q112. If the vendor provides applications as part of their service, are applications security scans conducted to ensure secure coding?		
Q113. If wireless networks are used in your environment, is WPA2 encryption implemented?		
Q114. Is all in-transit data encrypted?		
Q115. Is sensitive data encrypted at rest?		
Q116. Is full-disk encryption implemented on laptops?		
Q117. Are operating system and application patches implemented as per your policy?		
Q118. Do you have users who save sensitive data on their local hard drives or removable media?		
Q119. Are vulnerability scans performed at least quarterly?		
Q120. Are penetration tests conducted at least annually?		

Vendor Question	Vendor Response (Y/N)	EVIDENCE
Mobile		
Q121. Does your organization have a media sanitization process? (Removal of information from storage media) If yes, please describe.		
Q122. Do you allow teleworking? If so, please describe your remote security implementation.		
Q123. Do you have a Mobile Device Management (MDM) system in place?		
3rd Party Insurance Coverage - Complete this Section in Consultation with your Risk Management Consultant		
Q124. Is there a written contract between the municipality and the vendor?		
Q125. Does the contract include the JIF recommended indemnification and hold harmless language in favor of the municipality?		
Q126. Does the contract include language that forbids the vendor or their insurance company from waiving the subrogation rights of the municipality?		
Q127. Does the contract require the vendor to name the municipality as an "Additional Insured" on the vendor's Cyber Liability Policy?		
Q128. Does the contract require that the vendor provide the municipality with a copy of the endorsement to the vendor's Cyber Liability Policy indicating the municipality is an "Additional Insured" on the policy?		
Q129. Is the vendor's insurance policy "Primary" (not requiring a contribution of coverage from the municipality) in the event of a loss?		
Q130. Does the contract require the vendor to provide minimum limits of $3,000,000 Each Claim and $3,000,000 Annual Aggregate of Cyber Liability coverage?		
Q131. If the contract is with an IT vendor or financial institution that has access to more than $3,000,000 in municipal assets, are the minimum limits of coverage equal to or greater than the potential loss?		
Q132. Does the Cyber Liability Policy provide 3rd Party Coverage, including Privacy & Security, Media, Privacy Regulatory Defense, PCI (Payment Card Industry), and DSS (Data Security Standards)?		
Q133. Does the coverage include loss, theft or failure to protect PII (Personal Identifiable Information), PHI (Protected Health Information) or confidential information (including violation of any related privacy/security laws/regulations), as well as failing to prevent a security breach and failing to comply with your own privacy policies?		
Q134. Does the Cyber Liability Policy provide **"Breach Response"** services or reimbursement of the cost of breach response services?		
Q135. Does the contract require the vendor to provide proof of Errors & Omissions (professional liability) Insurance?		

Q136. Does the Errors & Omissions coverage include the peril of Cyber or an affirmative Cyber coverage grant?		
Q137. Are the limits of the Errors & Omissions Insurance at least $5,000,000 Each Claim and **$5,000,000 Annual Aggregate**?		