## ATTACHMENT F: CRM / DMS Information Security & Data Privacy

1. Please describe your information security policies, and your information security organization.
   1. Do you have a CISO?
   2. Is there a formal information security program in place? If so, please describe.
   3. Do you have security awareness training for employees and contractors? If so, please describe the training and how often it is performed.
   4. Is there a formal access review process? If so, please describe.
   5. Do you perform staff background checks?
   6. How have you implemented the least-privilege principle?
   7. Is vulnerability scanning, tracking and remediation management a defined business function in your organization?
   8. Do you conform with a specific industry standard security framework? (e.g. NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)?
   9. Do you regularly conduct penetration testing performed by a third-party vendor? If yes:
      1. How frequently are these conducted?
      2. When was the last one?
      3. What were the results?
      4. Have you ever rotated vendors for the penetration testing?
2. How are data protected in transit between your data centers and clients? How are the data protected in transit between your data centers, your developers/QA team, and your third-party vendors? Is all customer data encrypted in-transit throughout your service delivery infrastructure? Is all customer data encrypted in-transit between your service delivery infrastructure and customers’ infrastructure?"
3. Please describe your cybersecurity monitoring program.
4. Have you experienced a cybersecurity breach? If yes, please describe.
5. Is there a formal incident management program in place? If so, please describe.
6. Do you have a business continuity/disaster recovery plan? When was the last time you tested this/them? Will there be down time in the event of enacting your business continuity plan? How are clients notified?
7. Would you please provide us with your historical system uptime percentage? For example, in the past year, how much time has your system been out of service?
8. Data Center(s)
   1. What is/are the geographic location(s) of your data center(s)?
      1. Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?
      2. Describe at a high level how you maintain logical and physical separation between the data of different customers.
   2. Please describe the physical security of your data centers.
   3. Are your systems cloud based?
      1. If so, please describe.
      2. If not, do you have plans for the cloud?
9. System access:
   1. What is the process for adding or removing authorized users?
   2. Are we able to define access levels such as read only, power user, local administrator?
   3. What, if any, are your requirements for passwords/passphrases?
   4. Do you offer multi-factor authentication? If yes, what option(s) are available?
   5. Do you offer Single Sign On (SSO)?
10. Do you have a formal change management procedure for system upgrades and modifications?
11. Regarding Software Development/Systems:
    1. Do you have separation of duties between developers and testers?
    2. Do you consistently follow a defined software and/or system development lifecycle for product development?
    3. Do you follow industry standards (e.g. OWASP) to integrate security into your Systems/Software Development Lifecycle (SDLC)? If so, please indicate which standard.
    4. Do you review your applications specifically for security vulnerabilities and address any issues prior to deployment to production?
    5. What is the process for implementing/publishing changes?
    6. Does your application perform data integrity validation at all input/output interfaces to prevent intentional and unintentional processing errors or corruption of data?
12. Do you have full disk encryption on all your company owned computers?
13. How is retired media (hard drives, flash drives, CDs, documents, etc.) sanitized/purged?
14. Can you eliminate customer data from your environment, include data in backup archives, at customers’ request upon termination of service?
15. Do you outsource any of the services sought within this RFP? If so:
    1. Describe due diligence that is performed on contractors and vendors prior to and post contract.
    2. Do you have NDAs with these vendors?
    3. Have you reviewed their cybersecurity policies? If so, how frequently do you repeat reviews?
16. What are your policies regarding data privacy?
    1. Do you have a chief privacy officer or data protection officer?
    2. Do you have a documented privacy policy?
    3. Does your organization's employees, contractors, and third-party users receive formal privacy training to ensure confidentiality and privacy of data transferred under this engagement?
    4. Does your organization have processes in place to enforce privacy and confidentiality requirements with employees, contractors, and other third parties?
    5. Does the organization have a documented privacy policy that sets forth the operating standards for the organization's privacy practices?
    6. Are removable media controls in place to prevent unauthorized distribution or sharing of the data processed in connection with the business activity?
    7. Does your organization have a formal process for reporting and responding to privacy complaints involving personal information?
17. Have you conducted a Privacy Impact Assessment (PIA), Data Protection Impact Assessment (DPIA), or other privacy and security risk assessment within the last 12 months?
    1. Please provide the date of last assessment.
    2. Was this conducted internally or by an independent third party?
    3. What was the level of residual risk determined by the assessment?
    4. Has an action plan been created based on the results of the risk assessment?

**Apparent winners agree to assist UWINCO in completing the TrustArc privacy assessment for their product.**