CHECKLIST FOR EVALUATING THE SECURITY AND DATA STORAGE STANDARDS OF VENDOR MANAGEMENT SYSTEM (VMS) SUPPLIERS:

Access Control: Verify that the VMS offers powerful access controls allowing you to calibrate roles and permissions for different types of users.

Traceability and Transparency: Request information from the supplier about how transaction traceability in the system will be maintained and how the supplier will secure data reliability.

Authentication and Authorization: Confirm with the supplier that the system supports strong authentication methods (e.g. multi-factor authentication for suppliers or SSO for employees) and offers finetuned authorization settings.

Compliance with Data Protection Laws: Ensure that the supplier complies with relevant data protection regulations such as GDPR and other industry-specific standards.

Data Backups and Recovery: Check that the supplier has reliable procedures for data backups and recovery to protect against data loss.

Incident Management and Monitoring: Find out if the supplier has plans for incident management and if it has the monitoring capabilities to detect and respond to security incidents in real-time.

Network Security: Assess what measures are in place to protect against network-based attacks including firewalls, intrusion detection/prevention systems, and network segmentation.

Physical Security of Data Centers: Make sure that the supplier's data centers have proper physical security such as access controls, monitoring, and disaster recovery plans.

Supplier's Security Certificates and Audits: Verify that the supplier holds security

certificates relevant to the industry and undergoes regular security audits.

Secure Software Development Lifecycle (SDLC): Inquire about the processes and practices the supplier follows to evaluate if security is integrated into the development of their software.

Handling of Program Updates: Understand how the supplier handles program updates and patches to help address vulnerabilities quickly.

Disaster Management and Redundancy: Confirm that the VMS has dependable disaster management plans and redundant systems to ensure uninterrupted service in case of operational disruptions.

Data Protection and Ownership Rights: Review data protection policies and ownership rights to determine if they align with the requirements of your own organization.

Contractual Security Agreements: Examine the contract in detail to verify that security responsibilities, liabilities, and obligations are clearly defined.

Data Encryption: Ensure that data is encrypted both during transmission (using protocols such as HTTPS) and at rest (secure storage).

References and Reputation: Request references from existing customers to assess their satisfaction with the supplier's security standards.

Security Training and Awareness: Ask about training and awareness programs available to the supplier’s own employees to ascertain understanding and best practices.

Compliance with Industry Standards: Check if the supplier adheres to industry-specific security standards and certifications relevant to your organization.

Remember, thoroughness and due diligence in security and hosting is crucial for ensuring the protection of sensitive data and the overall integrity of your VMS solution.

Inkopio AB
Mäster Samuelsgatan 36
111 57 Stockholm, Sweden
Org: 556974-2108