Minneapolis
City of Lakes

OneNeck Security & Privacy Consultation

City of Minneapolis – Internal Audit Department
February 5, 2018

The security and privacy controls at OneNeck were designed, implemented and operating as intended.

Contents **Page**

Internal Audit Department
350 South 5th Street, Suite 310 1/2
Minneapolis, MN 55415-1316
(612) 673-5938

Date: February 5th, 2018

To: Mayor Jacob Frey, City Council Members, Chief Information Officer (CIO) Otto Doll and City Coordinator Spencer Cronk

Re: OneNeck Security and Privacy Risk Consultation

Background

OneNeck IT Solutions (OneNeck) was the primary Information Technology (IT) service provider to the City's IT department. They provided infrastructure hosting and managed IT services. To better understand the risks to the City data and network, a consultation on the security and privacy practices at OneNeck was performed in 2017.

Consultation Results and Recommendations

The Service Organization Control (SOC) 2 report for OneNeck was reviewed for the following security and privacy domains to note their controls and if they were designed, implemented, and operating effectively: -

- **Governance:** Review of people, policy, process, tools, training and awareness practices governing the organization.
- **Information Asset Management:** Review of data classification, multi-tenant, privacy, legal jurisdiction and encryption.
- **Access Control:** Review of access controls, segregation of duties, role-based access, and the request and approval processes.
- **Regulatory Compliance and Certifications:** Review of internal and external attestation reports including, certification reports, penetration tests and vulnerability scans.
- **Incident Response:** Review of the incident process, tracking tool, accountability, escalation procedures, resolution, etc.
- **Network Security:** Review of firewall, IDS / IPS, segmentation, DLP and communication services (i.e. HTTPS / FTP / RFC).
- **Infrastructure Security:** Review of the hardening baselines and practices for the platform / OS, middleware / DB, and application layers.
- **Change Management:** Review the change management process including, change record system, business description, testing evidence and management approval.
- **Software Development:** Review the Software Development management process including, code development methodology, secure coding best practices, developer training, and code scanning.

- **Logging & Monitoring:** The capturing and alerting associated with security events: failed logon attempts, administrator functionality, transactions, privilege escalation, etc.
- **Physical & Environmental:** Review of the owned or outsourced data center facilities controls including: badge access, parameter security, CCTV, guards, HVAC, raised floor, redundant power, fire suppression, etc.
- **Resiliency:** Review of crisis management, disaster recover & business continuity measures documented and periodically tested.
- **Vendor Management:** Review of the vendor's process for performing risk assessments of other sub-vendors that have network access or the ability to handle customer confidential data.

No exceptions were noted in the review of the above areas within the SOC2 report and hence, we conclude that the security and privacy practices at OneNeck meet industry standards and are designed, implemented and operating effectively.