HAMPTON VA

No. IT–052	Policy Name: Hosted or Cloud Computing Security Procedure
Effective Date: 06-03-2016 Last Revised Date: 06-03-2016	Citywide Policy_ IT Policy _ IT Procedure X
Approved By: IT Director	

Hosted and Cloud Computing Security Procedure

Background

The City utilizes vendors to provide application and computing resources on systems outside of the City's data center and owned by service providers. These are referred to has hosted or cloud computing environments. The following procedure applies in evaluating and reviewing hosted and cloud vendor solutions.

Scope and Purpose
References

IT-021 IT Security Policy

Usage Guidelines and Application
The Process

The IT department will periodically review hosted and cloud services for cyber security compliance. The IT Department will coordinate with City departments to review vendor services to ensure the following minimum security requirements are met and address gaps. Data which is critical or confidential may require higher than minimum standards.

Minimum Technology Security Requirements

1. Data Ownership – Data created, changed and managed by the City but located on vendor resources will remain under the control and ownership of the City. Vendors should have processes to allow the City to download or copy data at the end of a contract term in a generally available electronic format.
2. Data Disposal and Deletion – Vendors will not delete or dispose of City data until the end of a contract. The City and the vendor will agree on a time and method to delete data from the vendor's environment. Secure data destruction methods should be deployed for sensitive City data.
3. Data Segmentation – Vendors shall provide methods to ensure City data is segmented or segregated from other customer data. The exception being where the City agrees to a sharing arrangement.
4. Data Back Up – Vendors will back up City data and identify the method and frequency of back up.
5. Disaster Recovery – Vendors will have a disaster recovery plan in place and the City may request information on the plan and evidence of successful disaster recovery plan tests.
6. Physical Security – Vendors will have a physical security procedures and safeguards in place at data centers. Vendors will provide information on the physical access control methods utilized. Data center security and monitoring should be in place to quickly identify and address fires, break-ins, or other natural or man-made risks.
7. Security Controls – Vendors will deploy the concept of least privilege and role based access for their

employees and subcontractors to ensure only those individuals with a need to perform a function have access to that hardware, software or function.

8. Network Security – Vendors shall secure their perimeter through controlled devices on the edge and points throughout their network. Access Control Lists (ACL), firewall rules and other methods should be deployed to safeguard customer data. Logging should be implemented. Antivirus, Antimalware and Patching – Servers and other appropriate equipment should have antivirus/antimalware software deployed regularly. Servers should be kept up to date and patched frequently.
9. Change Management – Vendors should have a documented change management process in place.
10. Security Breach Prevention – Vendors should conduct periodic penetration tests and employ other methods to prevent security incidents. Vendors should also have methods for preventing or reducing the risk of DDOS attacks.
11. Breach Detection – Vendors should deploy Incident Detection or Incident Prevention systems and other methods to detect breaches quickly.
12. Incident Response – Vendors will have an incident response plan in place.
13. Independent Audits – Independent security audits and risk assessments should be conducted periodically.

PCI Compliance - Departments that are utilizing vendors for credit card transactions must request the vendor to provide evidence of PCI compliance.
HIPPA Compliance – Departments that are utilizing vendors for health data much request the vendor to provide evidence of HIPPA compliance.

Additional Documents/ Forms