External Cloud Policies

When the City of Columbia purchases services from an external cloud provider, as defined in this cloud strategy, the following policies must be followed:

2.0 Responsibilities of the City of Columbia

The City of Columbia will carry out the following tasks for every external cloud deployment as defined in this cloud strategy

2.1 The City of Columbia will establish a written agreement with the cloud vendor. This agreement will explicitly state the responsibilities of the vendor.
2.2 Prior to deployment, the City of Columbia will identify the regulations and standards that in force over the data or systems that may be moved to an external cloud. The City of Columbia will develop procedures and agreements with the cloud vendors to ensure compliance with all applicable regulations and standards.
2.3 The City of Columbia will establish an acceptable time frame for the vendor to respond to open records requests
2.4 The City of Columbia will establish a plan for the lifecycle of the service. The plan for the end of the service shall include what data will be extracted from the service, how data will be delivered, how the vendor will destroy data, and the price for these services. Data extracted from any system shall include transactional metadata, such as when data was added or changed and by whom.
2.5 The City of Columbia will calculate the anticipated load that will be placed on the City of Columbia internet connection. If the internet connection cannot handle the load a load management plan will be created and implemented prior to service implementation.
2.6 The City of Columbia will establish a business continuity plan that can be put into effect if the service ever becomes unavailable.
2.7 The City of Columbia shall manage all user accounts for the service. User accounts shall be managed through the existing security track procedures.

3.0 Responsibilities of the Vendors

All external cloud vendors, defined as vendors providing any cloud services as defined in this strategy to the City of Columbia must adhere to the following policies

3.1 Records Requests

3.1.1 The vendor will respond to records request within the timeframe stated in the agreement. The vendor will accept liability if the records request is not fulfilled in the agreed upon timeframe.

3.2 Using City of Columbia Domain Names

3.2.1 All cloud deployments that are intended to perform a service for our customers will be deployed using the gocolumbiamo.com domain name.

3.2.2 The City of Columbia IT Department will be the sole entity responsible for the gocolumbiamo.com domain name. The cloud vendor shall not expect to maintain DNS records belonging to the City of Columbia

3.2.2.1 The cloud vendor will provide the IP addresses used for the service prior to deployment. The City of Columbia IT Department will update the gocolumbiamo.com domain records accordingly.

3.2.2.2 The cloud vendor shall not change the addresses used with a frequency of greater than once per year

3.2.2.3 The cloud vendor shall notify the City of Columbia IT department in writing on official letterhead 30 days in advance of any IP address changes

3.2.2.4 The cloud vendor will use the gocolumbiamo.com only for the business purposes authorized by this agreement

3.2.3 Email from gocolumbiamo.com

When sending email from the service using the gocolumbiamo.com domain name, the following additional policies will be in effect

3.2.3.1 The cloud vendor will provide the IP addresses from which email will be sent. The City of Columbia IT Department will use this information to update the gocolumbiamo.com SPF record.

3.2.3.2 The addresses provided to the City of Columbia as required in 3.2.3.1 shall be only those IP addresses that are used to send email using the gocolumbiamo.com domain name.

3.2.3.3 The City of Columbia will update the gocolumbiamo.com SPF records according to the same policies and timelines as defined in 3.2.2 of this policy.

3.2.3.4 The cloud vendor will take all reasonable precautions to ensure that SPAM is not sent using the gocolumbiamo.com domain or from any IP address under cloud vendor control that has been associated with the gocolumbiamo.com domain.

3.2.3.5 The cloud vendor will react to email abuse reports in a timely manner

3.3 Standards and Regulations

3.3.1 The cloud vendor will adhere to relevant standards. For example, SaaS vendors deploying products over the web shall adhere to OWASP or similar standards.

3.3.2 The cloud vendor shall take responsibility for all regulatory compliance.

3.3.3 The cloud vendor shall conduct regular security audits of their systems. The security audits shall include internal and external review of system security and the security of all code used by the vendor. The vendor shall react promptly to mitigate the vulnerabilities identified by security audits.

3.4 System Integration

When an external cloud deployment requires access to existing information system infrastructure the following policies must be followed

3.4.1 Software should run with least possible privilege. For example, if database access needs to be given, the system account should have the least possible privilege; it should not run as a user that has access to schema outside of its need.

3.4.2 System account names should not be easily guessed. Passwords for these accounts should not be easily guessed and should be different from other customers with the same product. Connections from system accounts should be, where appropriate and possible, controlled via access lists.

3.5 Deployment and Customization

3.5.1 The cloud vendor shall disclose any authentication information that exists by default. The cloud vendor shall work with the City of Columbia to remove or change these accounts from their default values. The vendor shall not deploy services to the City of Columbia where system accounts are shared with other entities.

3.6 Encryption

3.6.1 Cloud vendor shall establish a suitable data encryption scheme for data in transit between the City of Columbia, its customers, and the vendor. The City of Columbia will determine the suitability of the encryption scheme.

3.6.2 Cloud vendor shall establish a suitable encryption for City of Columbia data while in storage for both live and backup media. The City of Columbia will determine the suitability of the encryption scheme.

3.6.3 No encryption scheme will be considered suitable if City of Columbia data can be recovered using the same decryption key as that of another customer of the cloud vendor.

3.7 Incident Preparation

3.7.1 The cloud vendor will take responsibility for keeping their system software up to date. Vendors should monitor relevant discussion boards and mailing lists for security problems with products they use.

3.7.2 The cloud vendors shall have a method for customers and others to report security problems. This method should be well publicized and accessible. Vendors should have a method for prioritizing and acting on reports of security problems.

3.7.3 The cloud vendors shall have a method for correcting discovered vulnerabilities. Vulnerabilities should be prioritized and corrected based on the risk vulnerability exploitation would pose to its customers. Vulnerability mitigation efforts should be tested by the vendor, as appropriate, prior to their release.

3.8 Incident Response

3.8.1 The cloud vendor will take responsibility for security incident handling if their system is compromised.

3.8.2 The cloud vendor shall immediately notify the City of Columbia of any breaches and will advise what information has been compromised. If this information is later found to be inaccurate the cloud vendor will immediately notify the City of Columbia with the correct information.

3.8.3 If investigation, containment, and eradication efforts by the City of Columbia incur costs while fault lies with the cloud vendor, the cloud vendor will assume the costs.

3.8.4 The cloud vendor will provide a rapid contact method for reporting suspected abuse, 24x7x365. The cloud vendor will react in a timely manner to abuse reports from the City of Columbia

3.8.5 The cloud vendor will provide their incident response plans. Response plans will include procedures for both security incident and disaster incident response.