Cloud Computing Policy

Purpose

Cloud computing offers a number of advantages including low costs, high performance and quick delivery of services. However, without adequate controls, it also exposes individuals and organizations to online threats such as data loss or theft and unauthorized access to networks.

This cloud computing policy is meant to ensure that cloud services are NOT used without the IT Management or CIO's knowledge. It is imperative that employees NOT open cloud services accounts or enter into cloud service contracts for the storage, manipulation or exchange of city-related communications or city-owned data without the IT Management/CIO's input. This is necessary to protect the integrity and confidentiality of data and the security of the network.

The City remains committed to enabling employees to do their jobs as efficiently as possible through the use of technology. The following guidelines are intended to establish a process whereby employees can use cloud services without jeopardizing data and computing resources.

Scope

This policy applies to all employees, no exceptions. This policy pertains to all external cloud services, e.g. cloud-based email, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc. Personal accounts are excluded.

If you are not sure whether a service is cloud-based or not, please contact the ITMD.

General Policy

1. Use of cloud computing services for work purposes must be formally authorized by the Chief Information Officer (CIO). The CIO will determine security, privacy and all other IT management requirements are adequately addressed by the cloud computing vendor.

2. For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the CIO and the departmental legal authority.

3. The use of such services must comply with the City's existing Internet Usage Policy and other adopted policies.

4. The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by the City.

5. The CIO decides what data may or may not be stored in the Cloud.

6. Personal cloud services accounts may not be used for the storage, manipulation or exchange of City-related communications or City-owned data.

Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.