City of Culver City

Mike Balkman Council
Chambers
9770 Culver Blvd.
Culver City, CA 90232

Staff Report

File #: 15-876, **Version:** 1 **Item #:** C-22.

CC: Approval of (1) a Two-Year Agreement with Iron Mountain Inc. for the Purchase of Cloud Backup Services for Data Backup and Recovery, through Zones Inc. as the Authorized Account Reseller, in an Amount Not-To-Exceed $162,657 for the First Year for Associated Hardware, Setup, Professional Services and Storage Fees, and $80,960 for the Second Year for Ongoing Annual Maintenance; and (2) Three Optional One-Year Extensions for Annual Maintenance in Amounts Not-To-Exceed the Prior Year's Cost by More than 15%, Subject to the Approval of the City Manager.

Contact Person/Dept: Michele Williams (IT) / Capt. Ron Iizuka (PD)
Phone Number: 310-253-5950 / 310-253-6396

Fiscal Impact: Yes [X] No [] **General Fund:** Yes [X] No []

Public Hearing: [] **Action Item:** [X] **Attachments:** Yes [X] No []

Commission Action Required: Yes [] No [] **Date:**
Commission Name:

Public Notification: (E-Mail) Meetings and Agendas - City Council (06/08/16); Iron Mountain (06/02/2016)

Department Approval: Michele Williams and Chief Scott Bixby (06/06/16)

RECOMMENDATION

Staff recommends that the City Council approve (1) a two-year agreement with Iron Mountain Inc. (Boston, MA) (1) for the purchase of cloud backup services for data backup and recovery, through Zones, Inc. (Auburn, WA), as the authorized account reseller (Attachment 1), in an amount not-to-exceed $162,657 for the first year for associated hardware, setup, professional services and storage fees, and $80,960 for the second year for ongoing annual maintenance; and (2) three optional one-year extensions for annual maintenance in amounts not-to-exceed the prior year's cost by more than 15%, subject to the approval of the City Manager.

BACKGROUND

Backup of data files and servers is a critical function. Backups are used to recover from server failures, human error, and malicious activities such as ransomware or computer viruses. They are also used to restore information or configurations if an update or change is determined to be detrimental or information has been lost.

The volume of data being stored continues to grow and managing large amounts of data is a critical function of technical support in addition to the backup/recovery processes. Traditional backup processes are performed using one of two technology approaches:

- Tapes - Using tape drives in a library/device that loads and unloads tapes as they are needed.
- Hard Disks - Transferring the data from the source hard disks to store on another disk system which is either held online or held offline like a high capacity tape and stored in another location.

Tape and disk technologies have increased in capacity storage and speed but will always have an upper storage limit on each tape or the disk. The window of time available for completing a backup overnight has decreased as a result of the need to have high availability of many systems in the evenings and at night or on the weekends; while the volume of data to be backed up continues to increase. The volatility of data is also a factor. In any work day City staff are processing more transactions and customers are using self-service options to input requests, forms, and carry out transactions. As a result daily backup is much more common than weekly backup; and takes up much more space and time each week.

Current Solutions
Over time the Information Technology (IT) Department has purchased additional tape capacity in an effort to keep up with the demand (increased storage requirements). Sessions that span multiple tapes are used to increase efficiency and enhanced procedures involve only capturing the changes to databases. However, there is always a risk with the possibility of a corrupt tape in a series which will result in the inability to recover data from the set.

The Police Department (PD) has utilized disk-to-disk approaches for data backup/protection. This approach has the advantage of enabling the use of disks which can contain much more data than a tape, and have a higher transfer rate. However disks are also susceptible to damage as they have electronics and moving parts and are generally not designed to be moved around.

Specific challenges with traditional tape and disk backup utilities include:

- Software or hardware failures that take several days to resolve with the hardware maintenance vendor or software vendor.
- Corrupt tapes discovered when a recovery is needed requiring stepping back to an earlier backup.
- Completing overnight backup before staff arrives to use the systems in the morning. If the backup is still running access and/or responsiveness issues are reported sometimes the backups have to be cancelled for the day.
- Attempting to recover data on old tape technology or that were made with obsolete versions of

the software the City uses.
- Moving from daily full backups to daily incremental backups to save time and space sometimes result in a bad tape in the set impacting the ability to recover days of work.

DISCUSSION

IT and PD staff have been exploring alternatives to enhance their respective backup operations and recommend moving to a cloud based backup strategy. This has the potential to alleviate the backup challenges that both departments are facing. It provides a solution for scalability, reliability of backups, and disaster recovery issues.

Staff reviewed the following backup vendors:

- Iron Mountain (Boston, MA)
- Barracuda Inc. (Toronto, Canada)
- Zetta.net (Sunnyvale, CA)
- Keepitsafe (a subsidiary of j2 Global; Los Angeles, CA)
- Mozy Inc. (Seattle, WA)
- Google Inc. (Mountain View, CA)

Staff analyzed each of the vendors with regard to the following criteria: use of an onsite appliance to hold a local copy of the data and queue up backups and recoveries, cost, existing government clients, and compliance with encryption and storage standards. Mozy and Google did not advance beyond initial discussions. Of the four remaining vendors, they were evaluated as follows:

Vendor	**Appliance**	**Existing Gov't Clients**	**Compliance**	**Cost**
Iron Mountain	Yes	Yes	Yes	$112,442*
Barracuda	Yes	Yes	Yes	$300,000
Zetta.net	No	No	No	Non-Compliant
Keepitsafe	Yes	No	No	$100,000

Note - These prices are a comparison of IT's backup requirements only. Requirements for PD were added after initial pricing
* First year including setup. Year 2 and ongoing service is $50,400/year.

Iron Mountain had the best combination of background in the industry, technology approach, compliance, and pricing. IT worked with Iron Mountain to further reduce the cost and included the backup/recovery requirements for PD. A cost savings was achieved by working with one of their Authorized Resellers, Zones Inc. Using Zones as the account reseller the City received pricing through the TIPS (The Inter-local Purchasing System) contract which reduced the proposal price dramatically. For this reason IT recommends using Zones Inc. as the authorized reseller to process the order and contract.

Security Compliances

Iron Mountain encrypts all the data being moved from the City to its facility while it is in transit over the Internet. Once in their data center the City's information is also encrypted while it is at-rest. The ability to decrypt it is part of the recovery process requiring the City and Iron Mountain to both participate.

Iron Mountain utilizes FIPS (Federal Information Processing Standards) approved AES encryption. This is certified by NIST (National Institute of Standards and Technology) as specified by FIPS Publication 197. FIPS 197 designates AES as the standard for encrypting data used by federal departments and agencies, and all FIPS-approved encryption modules comply with that standard.

In addition Iron Mountain maintains the following data protection and privacy standards in their operations:

- Statement on Standards for Attestation Engagements (No. 16) (SSAE 16) Compliance.
- International Standards Organization / Information Sharing Environment (ISO/IEC) 17799. This is an internationally recognized security standard that is being followed by most financial service organizations in the United States and Europe.
- Control Objectives for Information and related Technologies (COBIT). This is an authoritative, up-to-date, international set of generally accepted IT Control Objectives for day-to-day use by business managers as well as security, control and audit practitioners. COBIT has been developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.
- Information Security Forum (ISF) standard. The ISF standard is known for refining proven practices and addressing 'hot topics', such as electronic commerce, Public-key Infrastructure (PKI) and malicious 'mobile' code (including viruses and Web-based threats). The ISF standard is based on BS7799 (British Standard of practice section 7799) and COBIT, and attempts to restructure the policies outlined in BS7799
- Health Insurance Portability & Accountability Act (HIPAA). Aka Public Law 104-191, amends the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act, this act authorized the Secretary of Health and Human Services to develop security and privacy standards to protect electronic healthcare information. The security and privacy standards were to cover the processing, storing and transmission of data to prevent inadvertent or unauthorized use or disclosure of an individual's health information.
- Children's Online Privacy & Protection Act (COPPA). Applies to the online collection of personal information from children under the age of 13.
- Gramm-Leach-Bliley (GLB). This regulates the sharing of personal information about individuals who obtain financial products or services from financial institutions.
- Payment Card Industry (PCI) Data Security Requirements. These requirements apply to all members, merchants, and service providers that store, process or transmit cardholder data. Additionally, these security requirements apply to all system components which is defined as any network component, server, or application included in, or connected to, the cardholder data environment.

How the Solution Operates

The Iron Mountain solution works as follows:

- Iron Mountain will initially send the City two storage devices (one will be located at City Hall/IT data center and the other one will be located at PD). The initial backup will be performed locally on the respective device. It is then shipped back to Iron Mountain and they create the initial image.

- The purchased appliances will also be setup on site at the IT data center and at the Police Department. It acts as a gateway to their storage facilities in the Cloud. All the backup sessions are queued to the local device and sent offsite in a steady transfer. The solution has the ability to bypass the appliance if needed to send the backup or receive the restore directly but speed is increased using the appliance.
- An agent is placed on each server which is programmed with the backup requirements for that server.
- Initially the server's image is sent to Iron Mountain being a clone of the data image as a starting point. From then on all changes (incremental) are uploaded to the stored image and marked by date/time.
- At intervals based on city specified configuration, the image and updates are merged and the process continues with a new base image and changes.

The onsite appliance that is part of Iron Mountain's solution contains a local copy of the most recent backups. In the event that a restore is called for on a recent backup IT or PD would not have to go to the Cloud to retrieve anything it would be restored from the onsite copy. This would speed up the recovery process since there is no transfer over the Internet. Only older backups would have to be recalled from Iron Mountain's site.

Since the appliance is a local backup in addition to the full cloud history the City does not have a single point of failure in the backup or restore process. It can function without the appliance but utilize it for speed and efficiency when available.

Pursuant to Culver City Municipal Code (CCMC) Section 3.07.045.G, the purchase of the goods and supplies is excepted from formal competitive bidding requirements when competitive bid procedures have already been utilized by the City or another public agency or non-profit entity whose main purpose is to help public agencies make purchases. As discussed the TIPS program (https://www.tips-usa.com/index.cfm) will be used to obtain the best pricing for the City. TIPS is a National Cooperative Purchasing Program used by schools, cities, counties and non-profits and incorporates a competitive bidding process to obtain price schedules. This program gives the City preferential pricing using the buying power of multiple award contracts.

Pursuant to CCMC Section 3.07.085.A, professional services are exempt from competitive bidding requirements. The professional service portion of the project will be provided directly by Iron Mountain for their product. For the reasons discussed above, competitive bidding of this component is not practical.

FISCAL ANALYSIS

Funding to support the Online Backup Recovery Project has been appropriated in the following accounts:

IT Repairs & Maintenance	10124100.600200	$80,000
IT Computer Replacement Fund	42080000.732150.PZ388	$34,442
PD Computer Hardware	10140200.732150	$20,000
PD Subscriptions	10140200.517100	$28,215

Purchasing the appliances and contracting for the service will result in an expenditure of $162,657 including tax and shipping. This first year cost includes the hardware, setup, professional services and storage fees.

Ongoing annual maintenance including the storage fees for both IT and PD will be budgeted each year for a total of $80,960. This expenditure will be budgeted in IT Repairs & Maintenance - 10124100.600200. Staff is requesting City Council approval for an increase in this amount up to 15% over the prior year's cost, subject to the approval of the City Manager.

ATTACHMENTS

1. Zones, Inc. Partner Letter

RECOMMENDED MOTIONS

That the City Council:

1. Approve an agreement with Iron Mountain, Inc., through Zones, Inc. as the account reseller, in an amount not-to-exceed $162,657 for the first year, for associated hardware, setup, professional services and storage fees, and an amount not-to-exceed $80,960 for the second year for ongoing annual maintenance; and

2. Approve three optional one-year extensions for annual maintenance in amounts not-to-exceed the prior year's cost by more than 15%, subject to the approval of the City Manager; and

3. Authorize the City Attorney to prepare any required documents; and

4. Authorize the City Manager to execute the agreements on behalf of the City.