PARK DISTRICT OF OAK PARK

Records Management Manual

Park District of Oak Park
218 Madison St
Oak Park, Illinois 60302

Last Review:
February 23, 2015

SECTION 2: RECORDS RETENTION AND STORAGE

Most records have active and inactive stages in their lifecycle.

Active Records

Paper records are usually retained within the department until they are no longer considered active. In most cases, a record must be referred to more than six times per year to be considered active. When activity drops, departments should determine which records are eligible for transfer to the storage trailer by periodically (every 6 to 12 months) reviewing the Records Schedule.

Inactive Records

When records are seldom referred to, their continued on-site retention becomes impractical. For this reason, the Park District has the option for inactive records to be stored in an off-site storage facility until retention requirements have been met. By storing inactive records off-site, costs associated with storing the same records within prime office space are reduced.

The Park District also has the option of using a vendor for records storage, retrieval, destruction and microfilming services. A record stored at an off-site facility remains available to the department until the recommended legal retention period has been met.

Records Disaster Mitigation

It is not always possible to prevent an emergency, but the Park District is able to reduce the likelihood that emergencies become disasters by establishing and following effective emergency management practices, even with Park District records.

Possible threats to records include:

- Natural disasters
- Fires
- Floods
- Insect infestations
- Security breaches
- Theft

Prevention is the best insurance against the loss of records and information. The following steps are taken to help reduce the chance that the Park District's records will be lost or damaged.

- The Park District strives to have effective processes for managing all documents and records, regardless of format or medium by reviewing the Records Management Plan among key staff at least every 3 years.
- The Park District's records are stored in a room which is secure, equipped with fire and flood prevention and detection devices, and fitted with locks and alarms.
- Paper records are protected by always being stored in boxes or cabinets in cool, dry, secure locations away from sunlight, windows, water pipes, gas pipes, and at least 6 inches off the floor.

- Electronic records are protected with established, regular back-up and storage procedures.
- Records storage areas (paper and electronic servers) are regularly inspected to ensure they are secure, safe, and free from any sign of deterioration, infestation, or damage.
- Personnel responsible for records management are trained to handle records securely, including adhering to established records classification, cleaning up records according to retention schedules, and protecting sensitive information.
- Extra protection is given to vital and essential records, such as deeds. These records are also saved electronically at a different location than where the original copies are kept in order to increase the probability that one copy will survive if the other is destroyed.
- Eating and drinking while working with records is prohibited.
- Records storage areas are not to be used for surplus storage of other objects.

SECTION 6: DISASTER RECOVERY

Disaster Recovery Plan

The following disaster recovery plan has been established to ensure that the Park District can act quickly and effectively to protect materials from harm, recover any damaged materials, and prevent further risks to records.

In the event of a disaster, the Disaster Records Recovery Team made up of the Executive Director, Designated Records Manager, and IT Manager should follow these key steps:

1. Confirm that all personnel are safe.
2. Ensure that the office is structurally sound and safe before authorizing anyone to return.
3. Access a copy of the Records Management Plan.
4. Confirm that the Park District is operating under emergency conditions.
5. Bring the disaster response team together to confirm and prioritize records recovery operations.
6. Assign immediate responsibilities according to this plan.
7. Establish disaster response site.
8. Secure the records storage site to prevent any future damage, loss, or theft.
9. Restore environmental controls to provide a cool, dry climate.
10. Stabilize the records. In a water disaster recovery effort, speed is of the essence. Wet records must be salvaged within 48 hours of the disaster to avoid costly restoration efforts. Photographic materials, magnetic media and coated paper stock paper deteriorate more quickly and should be given the highest priority. If stabilization is not possible, records should be moved off-site.
11. Document the damage through photographs and other forms of record for use in making a detailed assessment of the damage.
12. Recall, and if necessary, reconstitute, essential records and issue them to appropriate personnel for action.
13. Throw out duplicate, replaceable or disposable materials (including damaged non-records materials) to reduce the volume of materials confronting the recovery team and to remove a source of humidity from the disaster area. Keep an inventory of discards for insurance, replacement, and tracking.
14. As appropriate, arrange to salvage any non-vital records or clean up records systems or storage areas.
15. Records that have been water-damaged or mold-infested should be kept apart from other records for at least six months in a well-ventilated area with good climate control and low humidity.
16. Once the disaster is over and the office is back to normal, review the plan and make changes to improve it for next time.

Electronic Recovery Instructions

Restoration of servers, Virtual Machines, files and brick-level email is done by utilizing Veeam software on PDOP-VCS01. Administrative client allows the restoration of 14 previous snapshots (two weeks) of all servers.

File recovery details are as follows:

Files

Files are stored on file server (PDOP-DC01) in directories \\PDOP-DC01\e$\PDOP-Production.
User directories are stored on file server (PDOP-DC01) in directories \\PDOP-DC01\f$\Home.

Back-ups

Backups of all servers, Virtual Machines and files take place at 10:00PM daily utilizing Veeam software to PDOP-NAS01 (Network Attached Storage Device). An additional backup is run daily utilizing an additional 3GB USB external hard drive. The drive is rotated every two weeks and taken off-site for disaster recovery purposes.

Email

Email is archived on a Barracuda Email Archiver. All email (inbound and outbound) is routed and stored on this device for a period of seven years. Items can be retrieved by accessing an admin portal and performing a search by individual, subject, to, from, date, etc.

Data Replication/Duplication

Plans are underway to duplicate data off-site to one of our remote facilities. All items in PDOP-NAS01 will be replicated daily to an additional NAS device, allowing for VM's (Virtual Machines) to be restored on hardware housed in another remote location.