PARK DISTRICT OF OAK PARK
Committee of the Whole Meeting
John Hedges Administrative Center
218 Madison Street, Oak Park, Illinois 60302

Thursday, October 5, 2023, 7:30pm

AGENDA

I. **Call to Order/Roll Call**

II. **Public Comment**
Each person is limited to three minutes. The Board may set a limit on the total amount of time allocated to public comments.

III. **Administration and Finance Committee** – Commissioner Wick
A. Longfellow Master Plan Review Update
B. Disaster Recovery Policy*
C. 2024 Committee & Board Meeting Calendar*

IV. **Parks and Planning Committee** – Commissioner Worley-Hood
A. ADA Transition Plan Review Update*

V. **Recreation and Facility Program Committee** – Commissioner Lentz

VI. **New Business**

VII. **Closed Session**

VIII. **Adjournment**

* Indicates information attached.
** Indicates information to be provided before or at the meeting.
Update/Presentation indicates verbal report provided at meeting no materials attached.

The Park District of Oak Park welcomes the opportunity to assist residents and visitors with disabilities. If you need special accommodations for this meeting, please call (708) 725-2017 or via email at Edith.Wood@pdop.org.

In partnership with the community, we enrich lives by providing meaningful experiences through programs, parks, and facilities.

Disaster Recovery Policy

Park District of Oak Park
218 Madison Street ▪ Oak Park, Illinois 60302 ▪ ph: (708) 725-2000 ▪ fx: (708) 383-5702 ▪ www.pdop.org

PARK DISTRICT of OAK PARK

Memo

To: David Wick, Chair, Administration and Finance Committee
Board of Park Commissioners

From: Mitch Bowlin, Finance Director

CC: Jan Arnold, Executive Director

Date: September 28, 2023

Re: Disaster Recovery Policy

Statement

Staff are presenting this Disaster Recovery Policy to the Board as a matter of industry best practice and in order to maintain Cyber Liability Coverage through PDRMA.

Discussion

As cyber attacks continue to increase in frequency and severity it is prudent for the District to consider a Disaster Recovery Policy. This policy can also be thought of as a business continuity plan in order to maintain operations during a data breach while protecting both the District's systems and its customers.

The District has many safeguards in place to prevent such a breach (above and beyond what PDRMA recommends), but it is still important to have a plan and policy in place just in case an event were to happen. This policy has been developed from a template provided from PDRMA with minor modifications to better suit the Park District of Oak Park.

Recommendation

Staff recommends the Park Board review and approve the Disaster Recovery Policy.

Attachment: Disaster Recovery Policy

Disaster Recovery Policy

Introduction

The Park District of Oak Park has adopted this Disaster Recovery Policy. The goal of this plan is to outline the key recovery steps to be performed during and after a disruption to return to normal operations as soon as possible.

Scope of Policy

The scope of this disaster recovery plan addresses technical recovery only in the event of a significant disruption. All personnel of Park District of Oak Park must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce. The disaster recovery plan should be tested annually to maintain its integrity.

Considerations

- A disaster may occur at any time, not necessarily during work
- The Park District should establish and implement processes and procedures for responding effectively to emergencies or other occurrences (fire, vandalism, system failure, and natural disaster, etc.) that damage systems containing PII / sensitive data
- Systems that contain PII / sensitive data can be affected or destroyed in many ways, such as:
    - Flooding
    - Fire
    - Loss of power
    - Acts of God: Tornado, tsunami or hurricane
    - Hackers
    - Unauthorized access or malicious activity

Policy Statement

It is the policy of The Park District of Oak Park to establish and implement processes and procedures to create and maintain retrievable exact copies of PII / sensitive data.

Assembling Breach Response Team

Assembling a breach response team is an integral part of breach preparation. The members of a breach response team should be identified, each bringing their own skills to the group. In the event of a breach the team will work together to address the situations and take appropriate actions based on the circumstances. The individuals selected and identified below should be made aware and agree to accept the responsibilities that come with this position. The composition of this group may depend on the size of the organization, but each critical role should be identified to the best of the organization's ability. (An alternative Breach Response Team template is available in Appendix A)

Team Leader – The team leader will be responsible for the oversight of the group. These responsibilities include but are not limited to; developing and overall coordination with the team, updating breach response procedures as necessary and ensuring the team stays on track for timely response.

Name: Jan Arnold Email: jan.arnold@pdop.org Phone:708-725-2020

Information Technology – A representative from the Information Technology (IT) department should be selected to oversee the technology aspects associated with a breach. This includes but is not limited to; initial breach investigation, mitigation of ongoing harm and implementation of new technologies that can prevent future occurrences.

Name: Noventech Inc, Email: Support@Noventech.com Phone: 630-595-5200

Human Resources/PR/Outreach – An individual should be identified to lead the efforts in the communication department. Breaches, depending on size, will often involve notification steps where affected individuals or appropriate government entities are informed of the incident and the remediation steps taken by the organization. This individual will be tasked with producing and sending notifications along with responding to questions or issues raised by affected individuals.

Name: Jan Arnold Email: jan.arnold@pdop.org Phone:708-725-2020

Legal Counsel – A representative from a legal team is a strong recommendation for a breach response team. Ideally this should be someone knowledgeable and experienced in these situations who can provide guidance from a legal perspective surrounding the actions taken by the team.

Name: Caitlyn Culbertson Email: caitlyn.culbertson@elrodfriedman.com Phone: 312-528-5206

Outside Vendors – Any outside or third-party vendors who may play a role in assisting with a breach should be identified. This could be data forensics companies, law enforcement or data breach resolution companies. If the breach had occurred within a 3rd party system, a representative from that team could play an important role as well.

	Name	Phone Number	Emergency Phone Number	Email Address
Team Leader	Jan Arnold	708-725-2020	708-725-2020	Jan.arnold@pdop.org
IT Provider	Noventech Inc,	630-595-5200	630-595-5200	support@noventech.com
PR/Outreach	Jill Allread Public Communications, Inc	312-848-3768	312-848-3768	jallread@pcipr.com
Legal Counsel	Caitlyn Culbertson Elrod Friedman	312-528-5206	312-528-5206	Caitlyn.culbertson@elrod.friedman.com

System and Application Criticality

The Park District of Oak Park provides several critical systems to service its business needs. It is important to note that this DRP attempts to classify and categorize the many systems and applications supported by client name for the purpose of offering a tiered approach to the restoration of the services and systems in the event of a disaster. If a disaster does occur, the systems and applications will be restored in tier order as follows:

- Tier A –The system is critically fundamental to the operation of the business and must be restored immediately (less than 4 hours – time can be changed to fit business need).
- Tier B – The system is important to the daily business operations but may be out of service for 1 business day and up to 3 business days in case of a serious catastrophe. (Time can be changed to fit business need)
- Tier C – The system is not required for daily business operations and can run successfully for an extended period (3 business day or more) without the system being available. (Time can be changed to fit business need)

What are the critical components of our network?

System / Application	Function	Consequences of Disruption	Workarounds / Alternatives	Primary Contact	Priority Tier
List name of system or application	Describe the function or purpose of the system.	Explain what would happen if the system was unavailable.	List any other method that would allow your business to continue to access the data or use the system during a disruption.	List the primary contact for the listed system.	Assign a priority tier (A, B, or C) based on the definition.
Fortinet	Enables users to VPN into the office. Directs all internet traffic to all the locations.	Internet is out to all the district and file access is extremely limited.	Users can store any data locally for the time being.	Noventech	A
Dell R640 8GK8743	Server host for half of the VM's	Documents and half network resources will be down.	Restore server to other host for priority servers.	Noventech	A
R640 GCK8743	Server host for half of the VM's	Documents and half network resources will be down.	Restore server to other host for priority servers.	Noventech	A
PDOP-APPS02	SmartFusion Host server	Smart Fusion is unassessiable.	No workaround server would need to be restored.	Noventech	C

PDDOP-Data	Data server	User would not have access to network drives.	User would be able to use internet resources and any local files.	Noventech	A
PDOP-DC	Domain controller/ DNS Host/DHCP for networks across the network/ Software repository	Logins could be affected but unlikely as other domain controllers are on the network.	Logins could be affected but unlikely as other domain controllers are on the network	Noventech	C
PDOP-JHACDC1	Domain controller/ DNS Host/DHCP for phone networks across the network	Logins could be affected but unlikely as other domain controllers are on the network	Logins could be affected but unlikely as other domain controllers are on the network	Noventech	C
PDOP-MGNT01	Runs scheduled reports to collect data for Survey gizmo.	Data would be out of date.	Server would need to be restored for collections to continue.	Noventech	C
PDOP-Proxy	Proxy server to assist with Veeam backups	Backups would not run as efficiently	Create a new proxy.	Noventech	C
PDOP-SQL01	Hosts data for Smart Fusion mPower and a few different PDOP sites.	Site will be offline and data unassailable.	Server would need to be restored	Noventech	B
RCRC-DC	Spare DC for Failover	Users would not be affected.	Backup DC's would handle all responsibility.	Noventech	C
Baracuda Spam filter	Filters emails before end users receive them.	Email would not come in.	Route traffic through 365 .	Noventech	B
Archiver	Archives all emails	Email would still come in but throw errors to admin account.	Device would need to get backup and running	Noventech	B
Synology-NAS	Where Local backups are stored	Backups will not be able to complete	Backups can be retrieved from cloud copy.	Noventech	A

APC Battery Backups	Power would be lost for all IT devices	Network and server access would be lost due to power outage	Replacement batteries would need to purchased. We have small spares where we can route power to critical items.	Noventech	A
Aruba Switches	Internet connectivity would be lost at 218	Users can still use local PC to work on word documents	Grab an old switch and upload config files.	Noventech	A

Incident Response Plan

This section discusses the steps to be taken during an incident.

1. The person who discovers the incident will contact the IT provider Noventech, Inc.

2. If the person discovering the incident is a member of the IT department, proceed to step 5.

3. If the person discovering the incident is not a member of IT, they will contact the IT Provider:

Noventech Inc,
450 E. 22nd Street, Suite 140
630-595-5200
Support@noventech.com
Ticket system: https://portal.beaconapp.io

4. When contacting IT, the caller is to provide:

- The name of the caller.
- Time of the call.
- Contact information about the caller.
- The nature of the incident.
- What equipment or persons were involved?
- Location of equipment or persons involved.
- How the incident was detected.
- When was the event first noticed?
- What have you done before contacting IT?

5. The IT staff member who receives the call (or discovers the incident) will:

- Refer to their contact list for both management personnel and incident response members to be contacted.

- The staff member will contact the incident response manager using Teams, email, and phone messages. While ensuring other appropriate and backup personnel and designated managers are contacted.
- The staff member will log the information received in the same format as the previous step.

6. a. The incident response manager and IT department will begin to triage the incident by gathering and logging:
    - Is the equipment affected business-critical?
    - What is the severity of the potential impact?
    - What is the targeted system's name, the operating system, IP address, and device location?
    - IP address and any information about the origin of the attack.

   b. Contacted members of the response team will meet or discuss the situation over the telephone or Teams and determine a response strategy.
    - Is the incident real or perceived?
    - Is the incident still in progress?
    - What data or property is threatened, and how critical is it?
    - What is the impact on the business should the attack succeed? Minimal, serious, or critical?
    - What system or systems are targeted, and where are they located physically and on the network?
    - Is the incident inside the trusted network?
    - Is the response urgent?
    - Can the incident be quickly contained?
    - Will the response alert the attacker and do we care?
    - What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

7. The incident will be categorized into the highest appropriate level of one of the following categories:

- Category one - A threat to sensitive data
- Category two - A threat to computer systems
- Category three - A disruption of services

8. Team members will establish and follow one of the following procedures basing their response to the incident assessment:

- Malware response procedure
- Spyware response procedure.
- Virus response procedure
- System failure procedure
- Active intrusion response procedure - Is critical data at risk?
- Inactive Intrusion response procedure
- System abuse procedure
- Property theft response procedure
- Website denial of service response procedure

- Database or file denial of service response procedure

The team may create additional procedures which are not foreseen in this document. In that case, the team must document what was done and later establish a process for the incident.

9. Team members will:

- Use cybersecurity and forensic techniques to remediate.
- Review system logs, looking for gaps in logs.
- Review intrusion detection logs.
- Interview witnesses and the incident victim to determine how the incident was caused.

Only authorized personnel should perform interviews or examine the evidence, and the authorized personnel may vary by situation and facility.

10. Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.

11. Upon management approval, implement recommended changes.

12. IT Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:

- Re-install the affected system(s) from scratch and restore backup data if necessary.

Preserve evidence before doing this.

- Restore Servers by performing full VM restore
- Make users change passwords if passwords have been sniffed\compromised.
- Be sure the system has been hardened by turning off or uninstalling unused services.
- Be sure the system is fully patched.
- Be sure real-time virus protection and intrusion detection is running.
- Be sure the system logs the correct events to the proper level.

13. Full Incident Documentation—the following shall be documented:

- How the incident was discovered.
- The category of the incident.
- How the incident occurred, whether through email, firewall, etc.
- Where the attack came from, logging IP addresses, and other related information about the attacker.
- What was the response plan was.
- What was done in response?
- Whether the response was adequate.

14. Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence if necessary to complete prosecution and beyond in case of an appeal.

15. Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.

16. Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

17. Review response and update policies—plan and take preventative steps so the intrusion can't happen again.

- Consider whether an additional policy could have prevented the intrusion.
- Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
- Was the incident response appropriate? How could it be improved?
- Was every appropriate party informed promptly?
- Were the incident-response procedures detailed, and did they cover the entire situation? How can they be improved?
- Have changes been made to prevent a re-infection? For example, have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
- Have changes been made to prevent a new and similar infection?
- Should any security policies be updated?
- What lessons have been learned from this experience?

18. Train staff on incident response

Only IT may need to fully understand the incident response plan. But it is crucial that everyone in the organization understands the importance of the plan. Full employee cooperation with IT can reduce the length of disruptions. In addition, understanding basic security concepts can limit the chances of a significant breach.

PARK DISTRICT of OAK PARK

2024 Committee & Board Meeting Calendar

Park District of Oak Park
218 Madison Street ▪ Oak Park, Illinois 60302 ▪ ph: (708) 725-2000 ▪ fx: (708) 383-5702 ▪ www.pdop.org

PARK DISTRICT of OAK PARK

2024 Committee & Board Meeting Calendar

Committee of the Whole Meeting -
First Thursday of the month (unless noted)
Hedges Administrative Center, 218 Madison
7:30PM (unless noted)

Regular Park Board Meeting -
Third Thursday of the month (unless noted)
Hedges Administrative Center, 218 Madison
7:30PM (unless noted)

- **COW Meeting**
- **Board Meeting**
- **Budget Meeting / Release**
- **Publication Date**
- **Annual Meeting**

January

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

February

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29		

March

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

April

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

May

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

June

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

July

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

August

S	M	T	W	T	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

September

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

October

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

November

S	M	T	W	T	F	S
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

December

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

JANUARY
11 – COW Meeting
18 – Board Meeting
25-27 – IPRA Conference

FEBRUARY
8 – COW Meeting
22 - Board Meeting

MARCH
7 – COW Meeting
21 – Board Meeting

APRIL
4 – COW Meeting
8 – Park District Birthday
18 – Board Meeting

MAY
2 – Annual / COW Meetings
18 – Board Meeting

JUNE
6 – COW Meeting
18 – Board Retreat
20 – Board Meeting

JULY
11 – COW Meeting
18 – Board Meeting

AUGUST
No COW Meeting
15 – Board Meeting

SEPTEMBER
5 – COW Meeting
19 – Board Meeting
26 – Budget Meeting

OCTOBER
3 – COW/Budget Meetings
4 – Release of draft budget to the public (30 days)
8-10 – NRPA Conference
17 – Board Meeting
29 – Publish Notice of Hearing

NOVEMBER
7 – COW Meeting / Tax Levy Hearing
21 – Board Meeting / Budget & Appropriation Hearing / Approval of Budget & Appropriation Ordinance

DECEMBER
5 – COW Meeting
19 – Board Meeting

PARK DISTRICT of OAK PARK

ADA Transition Plan Review

Park District of Oak Park
218 Madison Street ▪ Oak Park, Illinois 60302 ▪ ph: (708) 725-2000 ▪ fx: (708) 383-5702 ▪ www.pdop.org

PARK DISTRICT of OAK PARK

Memo

To: Jake Worley-Hood, Chair, Parks and Planning Committee
Board of Park Commissioners

From: Chris Lindgren, Superintendent of Parks & Planning

CC: Jan Arnold, Executive Director

Date: September 28, 2023

Re: ADA Transition Plan Review

Statement

The review of policy and procedures is being conducted in accordance with the Americans with Disabilities Act (ADA). The ADA requires all public entities to review their policies and procedures to determine if any discriminate against a person with a disability participating in their programming. Under Title II of the Americans with Disabilities Act (ADA), the regulations prohibit public entities, such as Park Districts, from discriminating against or excluding a person from programs, services or activities on the basis of disability. Title II and specifically §35.150 of the ADA addresses the requirements for all levels of state and local governments to develop transition plans to aid in the process of removing accessibility barriers. A transition plan is both a planning tool and public document.

Discussion

In February, 2011, the Park District entered into an agreement with Mark Trieglaff, President, Accessibility Consultation and Training Services, to review all Park District parks and facilities to determine their level of accessibility and to develop an ADA transition plan for the District. The Board reviewed and discussed the plan at its meeting on November 10, 2011, and formally approved it at the 2013 April Regular Board Meeting. Staff have been using and updating the transition plan annually with updates to the Park Board.

Staff engaged Mark Trieglaff in June of 2023 to update our ADA Transition Plan that was 10 years old. This was done to reflect progress over the years and to add in new facilities and capture new code changes. All parks & facilities were reviewed for compliance and incorporated into the new plan.

Recommendation

Staff and Mark Trieglaff of Accessibility Consultation and Training Services will bring the updated ADA transition plan to the Board for consideration and approval at the October 19 Regular Board Meeting.