

Minutes of the June 17, 2024 Montclair Public Library Board of Trustees Meeting

The 2191st meeting of the Montclair Public Library Board of Trustees was held on Monday, June 17, 2024 at 7:00 p.m. in accordance with New Jersey Law.

The meeting was called to order by President JoAnn McCullough at 7:10 p.m.

Open Meetings Act:

President JoAnn McCullough announced that the meeting was in compliance with the Open Meetings Act. Notice of this meeting was posted on the Library website, in the Library, at the Municipal Building and advertised in the Star Ledger. Notice of the change of venue to a Hybrid meeting was posted on the library website.

Roll Call:

Board Members Present: JoAnn McCullough, Presiding, Diana Lunin, Andrew Silver, Geoffrey Borshof and Tamar Campbell

Board Members Absent: Theodore Graham Brian Clarkson, Damen G. Cooper and Lilian Ferguson

Library Staff Present: Director Janet Torsney, Assistant Director Selwa Shamy, Recording Secretary Linda Welch, Facilities & Security Supervisor Timothy Flowers

Approval of Minutes:

The Minutes of the May 20, 2024 Regular Meeting stood approved. Geoffrey Borshof made the motion and JoAnn McCullough seconded. The motion was carried unanimously.

The Minutes of the June 5, 2024 Special Session stood approved. Geoffrey Borshof made the motion and JoAnn McCullough seconded. The motion was carried unanimously.

Presidents' Report:

JoAnn McCullough reported that at the Special Session of the Board of Trustees on June 5, 2024 the Board of Trustees, Support Groups and Senior Library staff met with the candidate for Library Director Radwa Ali.

Treasurer's Report:

Lisa Connell presented the Treasurer's Report:

Geoffrey Borshof moved for the adoption of Resolution #24-26 Approving the Bills and Payables Between the May 20, 2024 and June 17, 2024 Board of Trustees Meetings be approved and the itemized summary be made part of the minutes and JoAnn McCullough seconded. The motion was carried unanimously.

Andrew Silver moved for the adoption of Resolution #24-27 Pre-Approving the Bills and Payables Due Between the June 17, 2024 and July 15, 2024 Board of Trustees Meetings be approved and the itemized summary be made part of the minutes and Diana Lunin seconded. The motion was carried unanimously.

Thamar Campbell moved for the adoption of Resolution #24-28 Approving the May 2024 Bank Reconciliation Statements and Geoffrey Borshof seconded. The motion was carried unanimously.

Reports from Support Organizations:

Report from The MPL Foundation - Gina Chung Fortt Board Updates

At the Foundation's Board meeting on June 6, the last of our current Board year, we said goodbye to two members who are cycling off – Seo Hee Koh and Kishore Krishnan. Gina Chung Fortt is stepping down as Board Chair after two years of service, but will stay on as Vice-Chair in a role shared with Emily Hagen. We are delighted to welcome Sheila Boyd as the new Chair of the Foundation Board.

Annual Report

Please enjoy a copy of the 2023 Annual Report (also available on the Foundation website in the "About Us" section.) With a "refresh" spearheaded by Kelly Ziek and beautifully designed by Andy Ng, it is a piece that celebrates the many wonderful programs and people of MPL. Read it and pass it on to a friend!

Advocacy and Communications

Members of the Advocacy and Communications committee reached out individually to members of the Town Council in the lead-up to the June 11 vote on the budget. Following Janet's advice, messaging focused on the many achievements and successes of the library over the past two years, thanks in part to their support. We urged them to continue that legacy of support in the 2024 budget cycle. We were all heartened to receive the news on July 12 that the budget had passed with the \$515,000 in ancillary support intact.

Development

The Foundation will be on hand at the launch of the library's Summer Reading program on June 25. We are also delighted an event with Foundation Board member and author Henry Neff will take place at the Library on June 27 to launch his first novel for adults, "*The Witchstone*."

And don't miss a fond fundraising farewell to Janet in the form of a Karaoke Night at Tierney's on Thursday, July 25! Tickets are available on the Foundation website under "Events."

Gala plans for 2025 are underway. Stay tuned for a save-the-date in another few weeks.

StoryWalks

The Library and Foundation are partnering with the Judy Weston Garden for a StoryWalk

festival this summer. With a ribbon cutting on August 1 at the Wally Choice Community Center, and kick-off events in two other parks on August 3, the StoryWalks are a wonderful way to bring more visibility to literacy needs in our community, and to provide fun and accessible opportunities for families to engage in reading over the summer.

Montclair Library Friends: *Ed Robin*

The Montclair Library Friends and Friends of the Bellevue Avenue Library met with Janet to present her with a token of their esteem.

The board was shown a preliminary draft of the overview of the courtyard that include the original plans and the new proposed plans.

Friends of Bellevue Avenue Library, Inc.: *Ilmar Vanderer*

Ilmar expressed his appreciation to *Gina Chung Fortt* and wished her well in her future endeavors.

The next book sale is scheduled for September.

The Friends are working on a Summer Concert series for July and August
He is looking forward to the Bellevue Avenue Branch Trivia night on June 21.
Ilmar stated that he enjoyed the Buzz Aldrin School Art Exhibit Reception.

Library Report:

Assistant Director Report: *Selwa Shamy*

Building & Safety

- HVAC: Due to a low performing chiller in need of new parts, the Youth Services department had to close for three days in late May and June; three staff left early on various days while others called out due to the heat.
- HVAC: Repairs to the air handler and chiller have been completed but it's hard to tell if the building is any cooler.
- Elevator: from May 13 thru most of the day on June 7, the elevator was out of service. It only ran for five days before breaking down again. Original issues included a non-functioning motor, a leak spilling gallons of oil, and a bad electronics board. The total cost so far is \$17,550. The elevator was serviced again on 6/14, the speed was increased and a clunking sound is being caused by pistons which need to be adjusted.
 - CONSEQUENCES OF ELEVATOR OUT OF SERVICE
 - Shelving on the 2nd and 3rd floor was suspended.
 - Youth Services programs held on the 3rd floor were relocated to the 1st floor.
 - Caregivers wanting to still visit the 3rd floor left strollers on the 1st floor and carried their little ones up three flights of stairs.
 - Some staff were reassigned to the first floor due to the stairs being a hardship.
 - A staff workstation relocation project and a materials relocation project were suspended.

Programming

- Adrienne Burke has been running a monthly book group for over 18 years mostly focusing on Black authors. From the fall of 2023 through the summer, nine authors will have virtually visited the group.
- Below are the list of authors and titles:
 - Jabari Asim – Yonder
 - Suzette D. Harrison – Dust Bowl Orphans & Her Name is Ona Judge
 - Catherine Adel West – Saving Ruby King & The Two Lives of Sara
 - James E. Laws – Patriarch
 - Preslaysa Williams – Low Country Bride
 - James W. Jennings – Wings of Red
 - Yasmin Angoe – Her Name is Knight
 - Mary Monroe – Mrs. Wiggin (July 2024)
- The Summer Reading Kickoff will take place at the Main Library on June 25.

Outreach

- African-American Heritage Parade and Festival, 6/1: Library staff and members of Friends of Bellevue Ave. decorated a float where staff and Friends sat on the float greeting parade watchers; there were over 100 interactions at the festival.
- Montclair Pride, 6/8: library staff had a very popular button making activity, staff had over 650 interactions.

Schools

- Buzz Aldrin art students, under the direction of Lauren Cirrito, have been working on a mural at the Branch for two semesters. The result is a festival underwater scene that spans from the wall going down the stairs continuing across Kid's Place. A reception to congratulate the students took place on June 12 when over 50 people attended (photo in packet)

Library Director Report: Janet Torsney:

The Library has stabilized and grown substantially since I came back in February 2022. Here is a snapshot:

Budget

	2022	2023	2024	Increase
	\$3,642,898	\$ 4,333,169	\$ 4,679,097	28%

Library use

	2022	2023	Increase
Door count	114,113	169,476	48%

Program attendance/children	5,952	13,362	124%
Program attendance/adult	2,751	3,754	36%

services			
Enrollments/adult school	4,426	5,706	30%

Community hosted events	110	431	291%
Community hosted attendance	2,480	10,758	334%

Outreach events	61	99	62%
Outreach contacts	2,480	4,316	74%

Circulation (BCCLS)	4	247,49	9	289,96	17%
Digital materials		91,676		98,446	7%
Museum passes		388		591	52%
Hotspots		580		825	42%

Programs and Partnerships

- Hosted the Weston Toast to the Teachers on June 10. More than 120 teachers, families and supporters attended. So much library love!
- We were very happy to be the gathering point for NAACP's Unity Walk on June 9, which was attended by 35 people including the Mayor-elect and several of the Council-elects. Thanks to Nola for being the liaison.
- Montclair Reads *Best We Could Do* ended on May 15. Between February and May, 14 partners worked with us on 49 events attended by 1,768 people.
- Planning for Partners for Health (PfH) /MPL *Poverty, by America* event continues. PfH is providing 113 books to local book clubs. The September 12 OBOM program will be preceded by a workshop with local individuals and organizations working on poverty and homeless
- Launch event for Walk Read Montclair, which we are doing in conjunction with the Judy Weston Garden at Watchung Park, is set for August 1 at 2pm at Wally Choice/Glenfield. The author of *Fab Cab*, the book that will be in the park, will be on hand along with local officials and kids from the Grassroots Camp. *Fab Cab* is a decodable book informed by the MPS Science of Reading.
- Future OBOM programs include Chasing Hop/Kristoff (9/25), Woman of Interest/O'Neill (10/5), Locker Room Talk/Ludke (10/16), How to Baby/Finck (fall), Never Far From Home/Jackson (11/16)

Buildings

- Senator Booker recommended that the Senate Subcommittee on Transportation, Housing and Urban Development (THUD) fund our request for \$500,000. Fingers crossed

- Worked with architect on BAB water infiltration report and QPA on bid packet
- Opened insurance claim for elevator work (about \$18,000)
- Plan to submit HVAC repairs to township for possible reimbursement
- Working with landscape architect on plan for restoring BAB courtyard
- Updated priorities list

Technology

- Met with Garden State JIF about cybersecurity.
- Implementing multi-factor authentication (a JIF requirement) and installation of switches funded by e-rate delayed by Township tech staff

Policies

- Created cybersecurity policies with guidance from Garden State JIF
- Revised Compensatory Time and Work from Home policies and clarified Work from Home agreements
- Working on new financial management and control policies as requested by auditor

Meetings

- Met with the Township Manager about HVAC, parking, network issues, budget, solar power and the cyberattack letter sent to staff.
- Attended Township Manager's presentation of budget
- Attended approval of Township budget

Miscellaneous

- Coordinated process and interviews for Search Committee
- Recorded episode of Watchung Booksellers podcast
- Attended opening of Judy Weston Garden
- Attended Brooklyn Public Library workshop on early literacy
- I'll be out the week of June 24

Timothy Flowers, Head of Facilities and Security

Tim presented an overview of the Maintenance and Security Department

- He discussed the HVAC issues and Elevator problems at the Main Library
- The water intrusion issue at the Bellevue Avenue Branch
- The Maintenance Department has taken over cleaning both branches.
- Kenny Williams is being promoted to full time in July
- There are 2 part-time employees working with Tim.
- Tim expressed his appreciation to Ed robin for the new security cameras

Old Business:

Personnel Committee Report - Andrew Silver

Radwa Ali, has been unanimously chosen as the new library director and will start on July 22, 2024.

New Business:

Revised Policies - Diana Lunin

Compensatory Time And Working From Home Policies (Work-14)

This policy applies to full-time employees of the Library. The full-time workweek is 35 hours/week with either a 30-minute or one hour unpaid meal break (see Pay-2). For example, a common schedule is 10 a.m. - 6 p.m. with a one-hour meal break. If an employee's approved duties exceed those hours, they are entitled to compensatory time.

Regulations

1. The supervisor must approve the employee's additional hours in advance.
2. The employee and supervisor should establish agreement on the number of compensatory hours and when they can be taken within a week.
 1. Events that exceed regular work hours and the compensatory time should be noted on the departmental calendars.
3. Compensatory hours must be taken within a month unless the Director or Assistant Director has approved an exception. Otherwise, those hours are forfeit.

Working From Home

Based on changes in the manner of working generally, due to specific needs necessitated by the personal circumstances of individual employees and due to wider communal circumstances, such as a pandemic or other health emergency, Montclair Public Library recognizes the need and appropriateness of allowing some employees to work remotely/telework from a location outside of the physical structure of the Library.

Regulations

1. Applicability
 - A. This policy applies to full and part-time employees of the Library. Employees may be assigned to telework or may submit a request to telework, which must be approved by the Library Director.
2. Definitions
 - A. For purposes of this policy, "working remotely" and "telework" both shall mean the practice of working from home or alternative locations outside of the Library through the use of technology, which enables the employee to access necessary materials and perform essential job functions.
3. Eligibility

To qualify to work remotely, an employee:

 - A. Should have a demonstrated ability to work well with minimal supervision, have a thorough knowledge and understanding of their job tasks and operations, have a history of reliable and responsible accomplishment of work duties, and have demonstrated an ability to establish priorities and manage their time; and
 - B. Must hold a position, for which the duties are conducive to being performed remotely, as determined by the Director or their designee, and the employee must have:
 1. Access to a desktop or laptop computer or tablet during all required working hours (although in some circumstances, the Library may permit an employee to borrow the required equipment from the Library, subject to

availability and need, and the approval of the Director),

2. Internet access (although in some circumstances, the Library may permit an employee to borrow a portable Internet hot spot device, subject to availability and need, and the approval of the Director),

3. Remote access to the materials and resources they will need to perform their job duties,

4. Childcare or elder care assistance during working hours, if applicable

5. A dedicated phone, which may be a cell phone, and a willingness to share personal contact information with the Library.

Note that while working remotely, each employee will be responsible for all associated costs and expenses, including payment for Internet access, cell phones, and other equipment. Employees wishing to use office supplies and materials from the Library must get prior approval from the Director.

Geoffrey Borshof moved to approve the Compensatory Time and Working from Home Policies (Work-14) and Andrew Silver seconded. The motion was approved unanimously.

Cybersecurity Policies as Required by Garden State JIF

Business Continuity and Disaster Recovery Policy

1.0 Purpose

This document defines policy directive on business continuity activities, including business continuity and disaster recovery planning for all the critical business processes and service activities undertaken by for its business/customers in order to:

- Effectively manage any incident that may cause a business disruption to
- Provide continuity of critical business processes and services managed by
- Minimize the potential impact that any business disruption would have on and its reputation.

2.0 Scope

This policy applies to all people, processes and systems required to maintain normal business operations and to recover from disruptions.

3.0 Definitions

Business Impact Analysis (BIA) predicts the consequences of disrupting a business function and process and gathers information needed to develop recovery strategies. Business Continuity Plan (BCP) is concerned with keeping business operations running, perhaps in another location, or by using alternative tools and processes following a disruption. Disaster Recovery Plan (DRP) is concerned with restoring normal business operations after a disaster.

4.0 Policy

All internal departments, processes or any independent client business elements that are considered critical and whose extended loss would have a significant impact on shall have a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for its operations within an agreed strategy. management shall regularly assess the impact of potential

disasters on business operations as part of the periodic BIA exercise. Management shall designate respective department heads responsible for maintaining a minimum acceptable standard of service in disaster situations.

In addition, all management personnel and employees shall be made aware of the BCPs and DRPs and their roles and responsibilities in achieving the defined continuity and recovery objectives. The BCPs and DRPs shall be tested and reviewed at regular intervals to ensure they remain relevant. Contracts with third-party suppliers that provide critical services to shall include:

- Communication and understanding of the relevant plans for the respective supplier's role.
- Adequate contingency or recovery strategies over the lifecycle of the product and service.

4.1 Roles and Responsibilities

The organization should ensure that roles and responsibilities have been assigned for:

- Providing guidance and oversight for the management of business continuity and disaster recovery activities as well as improvements.
- Managing all areas of the BIA, BCP and DRP and understanding the business.
- Updating management on BCP and DRP readiness.
- Managing and improving BCP testing exercises by monitoring schedules, reviewing assessment results and maintaining records.
- Training and educating the relevant individuals with necessary information on the organization's policies and procedures on business continuity and disaster activities.
- Coordinating and managing the BCP and DRP, including communication to relevant stakeholders in an actual or potential disaster.

4.2 Business Impact Analysis

Shall define a formal process to determine the criticality of a given process, business units and the impact on business, if they are not operational in case of a disaster, which may be an internal or external event. The output of this activity should be used to determine business continuity priorities and requirements. At a minimum, the following should be considered in the BIA exercise:

- Maximum tolerable business downtime
- Operational disruption and productivity
- Financial consideration
- Regulatory requirements
- Contractual obligations
- Organizational reputation

4.3 Business Continuity Planning

Business continuity planning shall be documented and approved by management for processes and business units (as applicable) that are identified as critical in the BIA. The BCP shall include the activities to be performed in various scenarios in case of incident/disaster which can occur due to internal or external events. The BCP shall consist of activities to be followed to protect personnel and assets following a disaster and resume services quickly. A BCP involves the following:

- Strategies to ensure the safety of personnel
- Analysis of potential threats
- Alternate strategies to continue business operations (alternate site of operations) in a defined time frame
- A list of the primary tasks required to continue the operations along with assigned responsibilities (recovery team)
- Easy to locate management contact information
- Explanation of where personnel should go if there is a disastrous event
- Information on data backups and organization site backup
- Communication strategies
- Buy-in from everyone in the organization

4.4 Disaster Recovery Planning

Shall develop and establish a Disaster Recovery Plan (DRP) that addresses the step-by-step process of recovering and reinstating the business operations to a pre-disaster state, including assessing the damage, estimating recovery costs, working with insurance companies, monitoring the progress of the recovery process and transitioning the management of the business operations from the recovery team back to the regular managers. A dedicated disaster recovery functional team shall be established for the management and implementation of the DRP.

4.5 Exercising or Testing

Performs regular database restores to ensure database backup validity and periodically tests application server backups to ensure we can recover from an application server failure. Periodic tests shall be performed by designated personnel authorized by management to test the execution of business continuity and disaster recovery plans. When possible, the testing involves collaboration with critical third parties to ensure vendor-dependent services and/or system(s) can be recovered to meet Recovery Time Objective (RTO) and Recovery Point Objective (RPO). The test results shall indicate whether the test was successful or requires corrective actions. In addition, BCP and DRPs shall be updated based on the results of the tests performed and lessons learned.

Diana Lunin moved to approve the Business Continuity and Disaster Recovery (CBY-1) and Andrew Silver seconded. The motion was approved unanimously.

Cybersecurity 2

Acceptable Use of Technology Policy

1. Overview

Effective security is a team effort involving the participation and support of every Montclair Public Library (MPL) employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at MPL. These rules are in place to protect the employee and MPL. Inappropriate use exposes MPL to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Library business or interact with internal networks and business systems, whether owned or leased by MPL, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at MPL and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with MP policies and

standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2.

This policy applies to employees, contractors, consultants, temporaries, and other workers at MPL, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by MPL.

4. Policy

4.1 General Use and Ownership

4.1.1 MPL proprietary information stored on electronic and computing devices whether owned or leased by MPL, the employee or a third party, remains the sole property of MPL. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard*.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of MPL proprietary information.

4.1.3 You may access, use or share MPL proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within MPL may monitor equipment, systems and network traffic at any time, per InfoSec's *Audit Policy*.

4.1.6 MPL reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security & Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.

4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. The screen must be locked or log off when the device is unattended.

4.2.4 Postings by employees from a MPL email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of MPL, unless posting is in the course of business duties.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, as they may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of MPL authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing MPL-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by MPL.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which MPL or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting MPL business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a MPL computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any MPL account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honey nets, or similar technology on the MPL network.
15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
Providing information about, or lists of MPL employees to parties outside MPL.
17. Providing information about, or lists of, MPL employees to parties outside MPL.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within MPL's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by MPL or connected via MPL's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.2 Blogging and Social Media

1. Blogging by employees, whether using MPL's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of MPL's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate MPL's policy, is not detrimental to MPL's best interests, and does not interfere with an employee's regular work duties. Blogging from MPL's systems is also subject to monitoring.
2. MPL's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by MPL's Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of MPL and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by MPL's *Non-Discrimination and Anti-Harassment* policy.
4. Employees may also not attribute personal statements, opinions or beliefs to MPL when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of MPL. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, MPL's trademarks, logos and any other MPL intellectual property may also not be used in connection with any blogging activity

5. Policy Compliance

5.1 Compliance Measurement

Compliance to this policy will be measured through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved in advance.

5.3 Non-Compliance

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

6. Related Standards, Policies, and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

Diana Lunin moved to approve the Acceptable use of Technology Policy (CBY-2) and Andrew Silver seconded. The motion was approved unanimously.

CYBERSECURITY - 3

Incident Management Policy

1.0 Purpose

The purpose of this policy is to provide guidelines to manage security incidents that threaten the confidentiality, integrity, or availability of information assets.

2.0 Scope

The policy applies to all employees, consultants and contractors of the Montclair Public Library (MPL). This policy is also applicable to all types of incidents (including but not limited to ones defined in this policy) related to information assets such as IT systems/services and related support systems of

3.0 Definitions

Information security event: Any occurrence related to information assets or the environment indicating a possible compromise of policies, failure of controls, or an unmapped situation that can impact security.

Information security incident: Any event that threatens the confidentiality, integrity, or availability of organization systems, applications, data, or networks.

1. Examples of organization systems include, but are not limited to: • Servers • Desktop computers • Laptop computers • Workstations • Mobile devices • Network equipment Examples of security incidents include, but are not limited to: • Unauthorized access • Potential violation of approved policies • Potential data and privacy breach • Intentionally targeted but unsuccessful unauthorized access • Accidental disclosure of confidential data • Infection by malware • Denial-of-Service (DoS) attack • Theft or loss of an organization system or asset • Theft or physical loss of computer equipment • Loss or theft of tablets, smartphones or other mobile

devices • A server known to have sensitive data is accessed or otherwise compromised by an unauthorized party • A firewall accessed by an unauthorized entity • A DDoS (Distributed Denial of Service) attack • The act of violating an explicit or implied security policy • A virus or worm uses open file shares to infect from one to hundreds of desktop computers • An attacker runs an exploit tool to gain access to a server's password file • Any event that affects the availability of our product or service • Any event that compromises the contractual commitments to our clients • Failure of information security controls with a likelihood of disrupting business operations

4.0 Policy

A designated individual shall establish information security incident management within the organization, i.e., overseeing incident management activities, including documentation, response, escalation, resolution, and analysis. should communicate where applicable with its employees, customers and other stakeholders when an incident that impacts them occurs, provide updates during the incident and after the resolution.

As needed, the security incidents would be reported outside of MPL by a designated person nominated by senior management. Users shall not report to or discuss incidents with other users or external persons as this may affect the reputation or hinder the investigation.

Intrusion attempts, security breaches, theft or loss of hardware, suspicion of an incident, or other security related incidents perpetrated against the organization must be reported to the incident management team (see Appendix A for details). All known vulnerabilities, in addition to all suspected or known violations, must be communicated promptly.

The team responding to the incident shall keep notes and use the appropriate chain of custody procedures to ensure that the evidence gathered, both digital and physical, during the security or privacy incident can be used successfully during prosecution, if appropriate. The chain of custody process should answer the following questions:

- What is the evidence? For example, digital information includes the filename, md5 hash, and Hardware information includes serial number, asset ID, hostname, photos, description
- How did you get it? For example: bagged, tagged, or pulled from the desktop
- When was it collected? Date, time
- Who has handled it? Name of person
- Why did that person handle it? Justification on the appropriateness of the individual who handled it • How was it stored? For example: In a secure storage container
- Where was it stored? This includes the information about the physical location in which proof is stored, or information regarding the storage used to keep the forensic image
- How do you transport it? For example: In a sealed static-free bag or a secure storage container

Who has access to the evidence?

This involves developing a check-in/ check-out process. The post-incident analysis must take place, as necessary, to identify the root cause of the incident. All critical servers should be monitored to ensure that users only perform authorized actions and processes. Aspects to be monitored are audit trails, which record exceptions and other relevant events. Audit trails shall be kept for a defined period to assist in investigations and ongoing access-control monitoring. Access to these audit logs shall be restricted to authorized individuals only. Accurate computer system clocks are essential to ensure the accuracy of audit logs, which may be needed for investigations or as evidence in legal or disciplinary cases. Lessons learned from incidents shall be incorporated into risk assessment process for continual improvements.

5.0 Roles and Responsibilities

Must establish an Incident Management team that logs, tracks, investigates, resolves and reports incidents in the organization. In the event of an incident or potential breach, or a breach of information, will be responsible for:

- Documentation specific to the incident
- Activities and actions required for escalation
- Notifications and responses
- Corrective actions to remediate causes for a breach
- Any fine, judgment, legal fees and expenses associated with the event
- Measures to bring affected systems, environments, and entities into compliance

5.1 Incident Management Team

All incidents are reported to and managed by the Incident Management Team (IMT). The IMT will determine whether policies and/or processes need to be updated or created, avoid a similar incident in the future and whether additional safeguards are required. The roles and responsibilities of the IMT are listed below (not exhaustive):

Role	Level	Responsibilities	Contact Info
Service/ Help Desk Analyst	Tier 1	Logs and categorizes received incidents, and assigns unresolved incidents received to Tier 2, as appropriate.	
Incident Analyst	Tier 2	Assists users through escalated Tier 1 incidents and are subject matter experts in the support area.	
Incident Analyst or Vendor	Tier 3	Incidents that cannot be resolved by Tier 2 are escalated to this level. Restores a failed IT service as soon as possible and escalates unresolved incidents to external support, such as application or product vendors.	
Incident Coordinator	Not Applicable	Performs administrative tasks required to support process activities and is in charge of assigning incidents within a team. Identifies incidents for review and escalates any process issues to the Incident Manager.	
Incident Manager	Not Applicable	Manages the process of restoring normal service operation as soon as possible in order to minimize the impact on business operations. Serves as the point of contact for all major incidents and communicates with the Incident Process Owner.	
Incident Process Owner	Not Applicable	Accountable for the incident management process and maintains, designs, and improves it as needed to achieve the business' objectives. Communicates incidents to internal and external (where applicable) stakeholders.	

6.0 Reporting an Incident

Any breach of information security policies must be reported as soon as possible. Users should immediately report all incidents pertaining to information security with the below

information at a minimum: • Incident date/time • Type of incident • Description/ incident details • Incident location • Contact details

6.1 Handling an Incident

The designated personnel handling security incidents whether an incident needs to be handed over and dealt with by departmental representatives or the incident needs to be escalated to senior management. *Upon receiving notification, the Information Security team will assess the severity of the incident according to the threshold in the table below: Severity of Incident Criteria Users Affected Violation of Legal/Contractual Obligations Low 1 to 10 No Medium 11 to 50 No High More than 50 Yes* ***The User affected number varies with organizations and is subject to change** (make this a table)* Based on the severity of the incident, the designated individual will decide as to whether an incident needs to be dealt with by departmental representatives, where appropriate, or whether the incident needs to be escalated to senior management. Representatives looking into security breaches will be responsible for updating, amending and modifying the status of incidents. The root cause of the incident must be analyzed to ensure necessary steps are taken to prevent a recurrence.

6.2 Post Mortems

The authorized personnel handling security incidents must schedule and host a post mortem using post-mortem form to ensure an appropriate post mortem is held no later than 72 hours after the incident has been completed. This post mortem must include a cross-functional team with participation from the customer success organization.

The goals of the post mortem at a high level are: • To find a root cause • To prevent recurrence • To understand the level of impact and missed SLA's • To provide the Customer Success team all the information and collateral to communicate with customers, as required.

Contact details for incident reporting

- Incident Category
- Contact Person
- Email Address
- Phone Number

Physical and Environmental IT and Security Data Breach and Privacy General
Emergency
Call 911

Diana Lunin moved to approve the revised Incident Management Policy (CYB-3) and Geoffrey Borshof seconded. The motion was approved unanimously.

Public Comment:

Ilmar Vanderer expressed his appreciation to Janet for her dedication to the library.

Adjournment:

At 8:17 p.m. JoAnn McCullough moved to adjourn the Board of Trustees meeting and Brian Clarkson seconded. The motion was carried unanimously and the meeting was adjourned.