

SPRING-BENNER-WALKER JOINT AUTHORITY

REGULAR MEETING

April 13, 2015

ATTENDANCE:

AUTHORITY MEMBERS:	Spring	Joseph Galbraith Gregg Heny Dondi Smeltzer
	Benner	Dan Hoffman William Hughes Timothy Miller
	Walker	Ted Onufrak

GUESTS: None

EXECUTIVE DIRECTOR: N. Warren Miller

CONSULTING SOLICITOR: Robert Mix, Esq.

EMPLOYEES: Kelly Gill

CALL TO ORDER:

The April 13, 2015, Regular Meeting of the Spring-Benner-Walker Joint Authority was called to order at 7:00 P.M. by Timothy Miller, Chairman. Mr. T. Miller thanked everyone for attending and stated that the meeting would be recorded for transcription.

ROLL CALL:

William Hughes, Secretary, took Roll Call, recording seven members present. Mr. McDowell and Mr. Scott were absent. Mr. T. Miller, Chairman, noted that with a quorum present, the Spring-Benner-Walker Joint Authority was permitted to conduct business under the laws of Pennsylvania.

PLEDGE OF ALLEGIANCE:

Mr. T. Miller, Chairman, led the Board members and Employees in the Pledge of Allegiance.

APPROVAL OF MEETING MINUTES:

Mr. T. Miller asked the Board if there were any questions and/or changes to the March 23, 2015 meeting minutes as presented. **Mr. Galbraith moved, seconded by Mr. Heny to approve the Minutes of the March 23, 2015 Regular Meeting as presented. 7 ayes, 0 nays, 2 absent. The motion carried.**

CORRESPONDENCE:

Bellefonte Class of 2015 Parent Group – We received a request for contribution from the Bellefonte Class of 2015 Parent Group for the “All Night Party”.

Mr. Onufrak indicated that at his place of employment the employees use any proceeds from their soda fund to assist with these types of contributions to benefit an employee’s child.

Bellefonte Borough’s Annual Chapter 94 Report – Mr. W. Miller informed the Board that we recently received a copy of Bellefonte Borough’s 2014 Chapter 94 Report. A copy of the report will be forwarded to our Authority Engineers for their review and comment.

APPROVAL OF PAYMENTS:

Approval of Requisitions:

Revenue Fund Requisition 2012-52 – Mr. Onufrak presented the Board with Revenue Requisition 2012-52. **Mr. Hughes moved, seconded by Mr. Heny to approve Revenue Requisition 2012-52 payable to SBWJA in the amount of \$69,156.21.**

Mr. Galbraith referenced the payment to Knisely Shredding and suggested the Authority may want to consider hosting a community event for the next time shredding is completed. Mr. Galbraith stated that Titan Credit Union held a similar event at Restek and it was greatly appreciated by the surrounding community. The Authority could invite its customers to have items shredded at no cost to them. Mr. W. Miller appreciated the suggestion and indicated it will likely be a long time before the Authority would have another shredding event, but will offer this in the future. 7 ayes, 0 nays, 2 absent. **The motion carried.**

GUESTS: There were no Guests present for the meeting.

EXECUTIVE DIRECTOR'S REPORT:

Lost Customer Payment – Mr. W. Miller informed the Board that a former employee lost/misplaced a customer payment that was hand delivered to our office in March. The Authority became aware of the lost payment when penalties were assessed and Mrs. Gill recalls seeing the customer make the payment. The customer was contacted and immediately wanted to stop payment on the check, but wasn't happy about the additional fees that would be assessed to complete this task.

Mr. W. Miller informed the Board that he recommended the customer wait until mid-April to see if the lost check would somehow clear the bank. At that time, the customer will be asked to issue a new check and if for some reason the original check would ever clear his bank account, our Authority will credit his sewer account for the amount of the check, \$65.00. The Board was receptive to Mr. W. Miller's suggestion.

Mr. Heny referenced the Identity Theft Prevention Program that was located in the Board packets for approval later in the meeting and asked if this type of situation was addressed in the program. Mr. W. Miller stated no, lost payments aren't referenced in the program. Mr. Heny then asked if the Authority staff knew what kind of personal information was on the check; however, none of the current staff were in contact with the customer regarding the mishap and were unaware of the details surrounding the lost payment.

Benner Pike Sewer Extension – The Benner Township Supervisors have indicated they were unaware of the five properties along Benner Pike not being connected to the public sewer and they would see no problems with connecting these properties to the public sewer. Mr. W. Miller explained to the Board that these five properties are located between Valentine Hill Road and the Benner Pike, across from the former Mansun Bus Depot.

This would involve the construction of a low pressure sewer main that would run in the front of the properties along the Benner Pike and would be conveyed to the 4" force main just before it crosses the Benner Pike, near the Penn State Federal Credit Union. Each property would have a grinder pump that would be purchased and maintained by our Authority.

Discussion was then held regarding the estimated costs for the minor sewer extension. **Mr. Galbraith moved, seconded by Mr. Hughes to move forward with the possibility of providing public sewer to the five properties along Benner Pike. 7 ayes, 0 nays, 2 absent. The motion carried.** Mr. W. Miller indicated the next step will be contacting the affected property owners to inquire about their interest and opinions in connecting to public sewer.

Suction Hose for Vactor Truck – Mr. W. Miller informed the Board he would like to purchase 4” suction hose for the Vactor Truck to assist with cleaning the individual grinder pumps on our Authority’s system. Mr. W. Miller believes we will need about 200’ of hose, which will cost around \$3,000. The Board didn’t have any issues with the purchase of the suction hose.

Bellefonte Borough – Mr. W. Miller indicated that he has not heard anything further from Ralph Stewart regarding an upcoming meeting with Bellefonte Borough Authority regarding their proposed Wastewater Treatment Plant upgrades.

Nittany Valley Joint Recreational Authority – Mr. W. Miller informed the Board that he was recently approached by Michael Bonchack of the Nittany Valley Joint Recreational Authority (NVJRA) asking for our assistance to help locate leaks at the Kepler Pool. The pool is currently empty, which makes it very difficult to locate any leaks. Mr. W. Miller indicated that once the Kepler pool has been filled, Mr. Bonchack will be contacting our Authority for further assistance with leak detection. Mr. Heny asked if we were charging the NVJRA for our time and Mr. W. Miller stated no, we are simply helping another Authority in our area.

EXECUTIVE SESSION – Mr. T. Miller recessed the Board for an Executive Session at 7:30 p.m. to discuss personnel issues and potential litigation. The meeting reconvened at 7:49 p.m.

SOLICITOR’S REPORT: Mr. Mix had nothing to report.

OLD BUSINESS:

Board Contact Information – Mr. Heny referenced discussions at prior board meetings regarding the grievance policy in the employee handbook and asked if employees were provided with Board member contact information such as phone numbers, email addresses and the list of committee members. Mr. Hoffman indicated that proper protocol would involve the employee contacting their direct supervisor and if the issue isn’t resolved to the employee’s satisfaction, the employee can ask the Executive Director to contact the Board members of that particular committee. Mr. Mix stated that there has been a lot of informal conversation back and forth between Board members and employees; however, proper procedures need to be followed, which starts with following the approved organizational chart.

Exit Interview – Mr. Smeltzer referenced an email from Ted Onufrak that was circulated among Board members regarding an Exit Interview being held at the termination of employment and indicated he would like to see this procedure added to our Authority's handbook. Mr. W. Miller stated that the Exit Interview is being added to the Personnel Handbook along with other changes which will be provided at a future meeting. Mr. W. Miller indicated the changes are being made for clarification purposes, which wasn't an issue until the past year.

NEW BUSINESS:

Identity Theft Prevention Program – Mr. T. Miller presented the Identity Theft Prevention Program Compliance Model to the Board for comment. This program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events. This Program is updated and approved on a yearly basis. **Mr. Onufrak moved, seconded by Mr. Smeltzer to approve the Identity Theft Prevention Program as presented for discussion and made a part of these official Minutes.** 7 ayes, 0 nays, 2 absent. **The motion carried.**

The Glen at Paradise Hills West, Agreement of Dedication– We received a signed and notarized Agreement of Dedication for the Glen at Paradise Hills West located in Benner Township, just behind Nature's Cover. Our Authority is also in receipt of a check for the maintenance bond, which will be deposited into an 18 month Certificate of Deposit at Northwest Savings Bank. **Mr. Galbraith moved, seconded by Mr. Hoffman to approve the Agreement of Dedication for the Glen at Paradise Hills West, which includes the opening of the Escrow Account at Northwest Savings for the maintenance bond.** 7 ayes, 0 nays, 2 absent. **The motion carried.**

COMMITTEE REPORTS:

Personnel & Community Relations Committee: Mr. Hoffman indicated the Authority staff is currently working with the Solicitor to provide an amended Personnel Handbook at a future meeting. Mr. T. Miller suggested the draft handbook be distributed to the Personnel Committee before being presented to the entire Board.

Facilities Committee:

Building Expansion – Mr. Hughes asked if the employees have provided any recommendations on the building expansion. Mr. W. Miller stated that earlier today Mr. Royer informed him that a few of the existing windows are barely intact and he would suggest construction of a complete new facility. Mr. W. Miller reminded the Board that the current facility is a pole shed and the Authority is limited to the existing footprint as per Spring Township Planning.

Finance Committee: Mr. Onufrak had nothing to report.

ADJOURNMENT:

Mr. Hoffman moved, seconded by Mr. Galbraith to adjourn the meeting at 8:00 p.m. 7 ayes, 0 nays, 2 absent. The motion carried.

Respectfully submitted,



William Hughes, Secretary



Kelly J. Gill, Recording Secretary

CC: Benner Township _____
Spring Township _____
Walker Township _____

Identity Theft Prevention Program

For

SPRING – BENNER – WALKER JOINT AUTHORITY

170 Irish Hollow Road

Bellefonte, PA 16823

April 13, 2015

Spring – Benner – Walker Joint Authority Identity Theft Prevention Program

This Program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events.

Contact Information:

The Senior Management Person responsible for this program is:

Name: N. Warren Miller

Title: Executive Director

Phone number: 814-355-4778

The Governing Board Members of the Utility are:

1. Timothy Miller, Chairman

7. Dan Hoffman

2. Dennis McDowell, Vice Chairman

8. Joseph Galbraith

3. Ted Onufrak, Treasurer

9. Jason Scott

4. Gregg Heny, Assistant Treasurer

5. William Hughes, Secretary

6. Dondi Smeltzer, Assistant Secretary

Risk Assessment

The Spring Benner Walker Joint Authority has conducted an internal risk assessment to evaluate how at risk the current procedures are at allowing customers to create a fraudulent account and evaluate if current (existing) accounts are being manipulated. This risk assessment evaluated how new accounts were opened and the methods used to access the account information. Using this information the utility was able to identify red flags that were appropriate to prevent identity theft.

- ✓New accounts opened In Person
 - ✓Account information accessed In Person
-

Detection (Red Flags)

The Spring Benner Walker Joint Authority adopts the following red flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

- ✓Fraud or active duty alerts included with consumer reports
- ✓Notice of credit freeze provided by consumer reporting agency
- ✓Notice of address discrepancy provided by consumer reporting agency
- ✓Inconsistent activity patterns indicated by consumer report such as:
 - Recent and significant increase in volume of inquiries
 - Unusual number of recent credit applications
 - A material change in use of credit
 - Accounts closed for cause or abuse
- ✓Identification documents appear to be altered
- ✓Photo and physical description do not match appearance of applicant
- ✓Other information is inconsistent with information provided by applicant
- ✓Other information provided by applicant is inconsistent with information on file.
- ✓Application appears altered or destroyed and reassembled
- ✓Personal information provided by applicant does not match other sources of information (e.g. credit reports, SS# not issued or listed as deceased)
- ✓Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)
- ✓Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager)
- ✓ SS#, address, or telephone # is the same as that of other customer at utility
- ✓Customer fails to provide all information requested
- ✓Personal information provided is inconsistent with information on file for a customer
- ✓Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet
- ✓Identity theft is reported or discovered

Response

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to the senior management official.

- ✓Ask applicant for additional documentation
- ✓Notify internal manager: Any utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify the Executive Director.
- ✓Notify law enforcement: The utility will notify the PA State Police at Rockview of any attempted or actual identity theft.
- ✓Do not open the account
- ✓Close the account

Personal Information Security Procedures

The Spring Benner Walker Joint Authority adopts the following security procedures:

1. Files containing personally identifiable information are kept in a locked file cabinet except when an employee is working on the file
2. Employees will not leave sensitive papers out on their desks when they are away from their work stations.
3. No visitor will be given any entry codes or allowed unescorted access to the office.
4. Passwords will not be shared or posted near work stations.

Identity Theft Prevention Program Review and Approval

This plan has been reviewed and adopted by the Utility Board of Directors by motion during the April 13, 2015 meeting. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.


Board Chairman

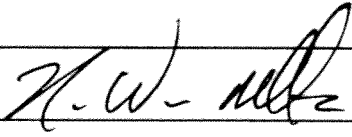
Attest:


Secretary

Name of Senior Management Staff Person: N. Warren Miller

Position: Executive Director

Date: 04/13/2015

Signature: 

A report will be prepared annually and submitted to the above named senior management or governing body to include matter related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

Appendix A
Other Security Procedures

The following suggestions are not part of or required by the Federal Trade Commission's "Identity Theft Red Flags Rule". The following is a list of other security procedures a utility should consider to protect consumer information and to prevent unauthorized access. Implementation of selected actions below according to the unique circumstances of utilities is a good management practice to protect personal consumer data.

1. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets. File cabinets will be stored in a locked room.
2. Only specially identified employees with a legitimate need will have keys to the room and cabinet.
3. Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.
4. Employees will not leave sensitive papers out on their desks when they are away from their workstations.
5. Employees store files when leaving their work areas
6. Employees log off their computers when leaving their work areas
7. Employees lock file cabinets when leaving their work areas
8. Employees lock file room doors when leaving their work areas
9. Access to offsite storage facilities is limited to employees with a legitimate business need.
10. Any sensitive information shipped using outside carriers or contractors will be encrypted
11. Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.
12. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.
13. No visitor will be given any entry codes or allowed unescorted access to the office.
14. Access to sensitive information will be controlled using "strong" passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different. Passwords will be changed at least monthly.
15. Passwords will not be shared or posted near workstations.

16. Password-activated screen savers will be used to lock employee computers after a period of inactivity.
17. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
18. Sensitive consumer data will not be stored on any computer with an Internet connection
19. Sensitive information that is sent to third parties over public networks will be encrypted
20. Sensitive information that is stored on computer network or portable storage devices used by your employees will be encrypted.
21. Email transmissions within your business will be encrypted if they contain personally identifying information.
22. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.
23. When sensitive data is received or transmitted, secure connections will be used
24. Computer passwords will be required.
25. User names and passwords will be different.
26. Passwords will be changed at least monthly.
27. Passwords will not be shared or posted near workstations.
28. Password-activated screen savers will be used to lock employee computers after a period of inactivity.
29. When installing new software, vendor-supplied default passwords are changed.
30. The use of laptops is restricted to those employees who need them to perform their jobs.
31. Laptops are stored in a secure place.
32. Laptop users will not store sensitive information on their laptops.
33. Laptops which contain sensitive data will be encrypted
34. Employees never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.
35. If a laptop must be left in a vehicle, it is locked in a trunk.
36. The computer network will have a firewall where your network connects to the Internet.

37. Any wireless network in use is secured.
38. Maintain central log files of security-related information to monitor activity on your network.
39. Monitor incoming traffic for signs of a data breach.
40. Monitor outgoing traffic for signs of a data breach.
41. Implement a breach response plan.
42. Check references or do background checks before hiring employees who will have access to sensitive data.
43. Access to customer's personal identify information is limited to employees with a "need to know."
44. Procedures exist for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information.
45. Implement a regular schedule of employee training.
46. Employees will be alert to attempts at phone phishing.
47. Employees are required to notify the general manager immediately if there is a potential security breach, such as a lost or stolen laptop.
48. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.
49. Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.
50. Paper records will be shredded before being placed into the trash.
51. Paper shredders will be available at the office, near the photocopier.
52. Any data storage media will be disposed of by shredding, punching holes in, or incineration.