

SPRING-BENNER-WALKER JOINT AUTHORITY

REGULAR MEETING

May 11, 2020

ATTENDANCE:

AUTHORITY MEMBERS:

Spring	Toby Dashner Joseph Galbraith Gregg Heny Chris McMurtrie
Benner	Dan Hoffman Willis Houser, Jr.
Walker	Dennis McDowell Joseph Swanderski

GUESTS: None present

EXECUTIVE DIRECTOR: N. Warren Miller

EMPLOYEES: Kelly Gill & Tasha Dutton

CALL TO ORDER:

The May 11, 2020, Regular Meeting of the Spring-Benner-Walker Joint Authority was called to order at 7:00 P.M. by Dennis McDowell, Chairman. Mr. McDowell thanked everyone for attending and stated that the meeting would be recorded for transcription purposes.

ROLL CALL:

Joseph Swanderski, Secretary, took Roll Call, recording eight members present. Mr. Book was excused from the meeting. Mr. McDowell, 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. McDowell, Chairman, led the Board members and Employees in the Pledge of Allegiance.

Thank You – Mr. McDowell took a moment to share a thank you card the Authority received from a local Girl Scout, Maura Sharer, of Troop 40034.

APPROVAL OF MEETING MINUTES:

Mr. McDowell asked the Board if there were any questions and/or changes to the April 27, 2020 meeting minutes as presented. **Mr. Galbraith moved, seconded by Mr. Houser to approve the Minutes of the April 27, 2020 Regular Meeting as presented.** 8 ayes, 0 nays, 1 absent. **The motion carried.**

CORRESPONDENCE:

Precision Acoustic Devices (Blatek Industries, Inc.) - We received a letter from Michael Pratt of Keller Engineers requesting a letter of intent to provide sewer service for Precision Acoustic Devices located at Lot #28R in the Penn Eagle Industrial Park. The estimated EDUs requested for this project is 32.02 EDUs. Our force main crosses this parcel of land and will need to be marked prior to construction.

Penn Eagle Pump Station (#9) – Mr. Miller indicated the capacity at our Penn Eagle Pump Station (#9) was recently reviewed due to upcoming development. The Chamber of Business & Industry of Centre County constructed Pump Station #9 to accommodate 1,200 EDUs and there is approximately 300 EDUs currently being conveyed through it. Mr. Miller indicated the remainder of the Amberleigh Development and a portion of the new Logan Greene Residential Community (former Hartle Property) will flow into the Penn Eagle Pump Station without difficulties. The developer of the future projects will not be required to make upgrades to the pump station at this time due to adequate capacity.

APPROVAL OF PAYMENTS:

Approval of Requisitions:

Revenue Fund Requisition 2020-04 Mr. Heny presented the Board with Revenue Requisition #2020-04 in the amount of \$400,917.82. Mr. Heny indicated a significant portion of this requisition was to Bellefonte Borough. Mr. Hoffman asked if the two (2) payments to the Centre County Prothonotary to satisfy Municipal Liens were due to the customers paying on their delinquent accounts. Mrs. Dutton indicated Mr. Hoffman was correct and that there were two (2) Municipal Liens per property. Mr. McDowell asked if Bellefonte Borough was providing adequate information to the Authority when Mrs. Gill requests additional information pertaining to the quarterly bills. Mrs. Gill stated she will submit a Right-to-Know request to the Borough if necessary, which has been working well for her. **Mr. Swanderski moved, seconded by Mr. Hoffman to approve Revenue Requisition 2020-04 payable to SBWJA in the amount of 400,917.82.** 8 ayes, 0 nays, 1 absent. **The motion carried.**

GUESTS: There were no guests present for the meeting.

SYSTEM OVERVIEW REPORT:

April 2020 System Overview – Mr. W. Miller reviewed the April 2020 System Overview with the Board.

In-Home Inspections - There were 10 in-home inspections completed in the month of April. Mr. Miller indicated the number of in-home inspections were decreased due to Pennsylvania not allowing real estate transactions during the COVID-19 pandemic. One of these included a re-inspection of a property that was previously documented as having a leaking sewer lateral in 2019 and has been paying an infiltration and inflow surcharge. Our staff noted a floor drain was reconnected to the sewer, which we resealed. We also noted significant problems with a private grinder on Valley View Road that was repaired by the seller.

Sewer Permits and/or Lateral Inspections - Our maintenance department completed one (1) new sewer lateral inspection in April. The office staff received one (1) sewer permit application in the amount of 1.00 EDU and issued the permit.

System Maintenance – The maintenance staff performed routine cleaning of the wet wells and we had our flow meters that enter Bellefonte's Treatment plant calibrated. There was no video work scheduled for the month of April.

Benner Township Water Authority – We connected one (1) new customer to the Benner Township Water Authority.

Inter – Municipal Work – Our personnel jetted approximately 400 feet of sewer main for Centre Hall Potter Sewer Authority to remove grit. We also collected waste oil from Benner Township.

Call Outs/ PA One Calls – There was a call out to 657 N. Pennsylvania Avenue due to a build-up of grease in their grinder and we re-set the generator at the Benner Commerce Pump Station (#16) on 04/04/2020. There was also a call out to mark an emergency PA One Call at 638 N. Harrison Road on 04/23/2020 due to a gas leak. Mr. Miller ended the report with a total of 49 PA One Calls being located in April.

EXECUTIVE DIRECTOR'S REPORT:

Act 537 Plan Special Study – The Benner Township Supervisors are proposing to have the Act 537 Plan Special Study on the agenda for discussion at their June 1, 2020 meeting. It was noted that the residents involved will receive a postcard invitation from Benner Township informing them of the meeting and they will be asked to RSVP so the Township can comply with social distancing. Our Authority will request the Phase I Archaeological Survey be completed if the Benner Township Supervisors approve the Act 537 Plan Special Study.

Village of Nittany Glen Phase IV – A new suction lift pump station will be constructed along Filmore Road to accommodate the Village of Nittany Glen Phase IV. The developer, Berks Homes, will be required to construct the pump station to our specifications, at their cost, and will then dedicate the pump station to our Authority. Mr. Miller is currently working with Chad Stafford of Penn Terra Engineering to establish the requirements of the new pump station.

Bellefonte Borough's Capital Project – Mrs. Gill contacted Mr. Stewart of Bellefonte Borough regarding Mr. Book's question from our April 27, 2020 Board meeting pertaining to Bellefonte Borough's capital project at their wastewater treatment plant being closed out. Mr. Stewart indicated G.M. McCrossin had sent Bellefonte Borough Authority a notice in late February that stated they are taking legal action against the Bellefonte Borough Authority. There has been no additional contact between G.M. McCrossin and Bellefonte Borough Authority since February.

SOLICITOR'S REPORT: Mr. Mix was excused from the meeting.

ENGINEER'S REPORT: Mr. Johnson was excused from the meeting.

OLD BUSINESS:

COVID-19 – Mr. Heny asked if the Authority staff was back to their regular schedule. Mr. Miller indicated the Authority personnel returned to the normal work schedule on May 4, 2020.

Maintenance Laborer/Maintenance Crew Leader – Mr. Swanderski asked what our status was for hiring new employees. Mr. Miller indicated he would like to promote a Maintenance Crew Leader from within and then he would proceed with hiring one (1) or two (2) laborers. At a recent staff meeting the maintenance personnel were asked to provide Mr. Miller or Mrs. Gill with a letter of interest if they would like to be considered for the Maintenance Crew Leader position. Mrs. Gill indicated the Maintenance Laborer position was advertised with CareerLink, PA Rural Water Association, Central PA Water Quality Association, PA Water Environment Association and with the Lock Haven Express; however, we only received six (6) applications with a limited skill set.

NEW BUSINESS:

Identity Theft Prevention Program – Mr. McDowell 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. It was noted there were no changes to the Identity Program Compliance Model. This Program is updated and approved on a yearly basis. **Mr. Heny moved, seconded by Mr. Hoffman to approve the Identity Theft Prevention Program as presented for discussion and made a part of these official Minutes.** 8 ayes, 0 nays, 1 absent. **The motion carried.**

2019 Audit – Mrs. Gill stated that Baker Tilly Virchow Krause, LLC has been working remotely on our audit due to the COVID-19 pandemic and they have expressed their willingness to present the 2019 audit to the Board virtually, if the Board so desires. Mr. Heny stated he didn't feel this was necessary as long as they are available by telephone to answer any questions that may arise. Mrs. Gill indicated Christine Zoerner will provide the Board with a hard copy of the 2019 audit for the 6/8/2020 meeting.

SBWJA Board Packets – Mr. McDowell asked if anyone would have objections to eliminating Board Packets being delivered to the homes of the Board members. Mr. McDowell stated a hard copy could be provided the night of the meeting. No changes will be made to the distribution of Board Packets at this time.

COMMITTEE REPORTS:

Personnel & Community Relations Committee: Mr. Hoffman had nothing to report.

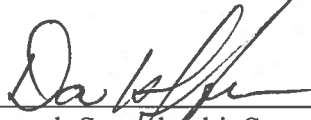
Facilities Committee: Mr. Book was absent. Mr. Houser had nothing to report.

Financial Committee: Mr. Heny had nothing to report.

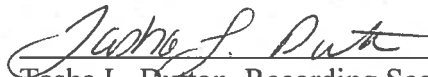
ADJOURNMENT:

Mr. Dashner moved, seconded by Mr. Houser to adjourn the meeting at 7:20 p.m. 8 ayes, 0 nays, 1 absent. The motion carried.

Respectfully submitted,



Joseph Swanderski, Secretary
Dan Hoffmann, Asst.



Tasha L. Dutton, 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

May 11, 2020

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. <u>Dennis McDowell, Chairman</u> | 7. <u>Brian Book</u> |
| 2. <u>Joseph Galbraith, Vice Chairman</u> | 8. <u>Toby Dashner</u> |
| 3. <u>Gregg Heny, Treasurer</u> | 9. <u>Willis Houser, Jr.</u> |
| 4. <u>Chris McMurtrie, Assistant Treasurer</u> | |
| 5. <u>Joseph Swanderski, Secretary</u> | |
| 6. <u>Dan Hoffman, Assistant Secretary</u> | |

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

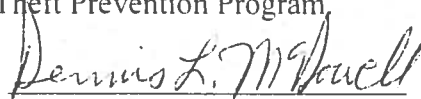
Personal Information Security Procedures

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

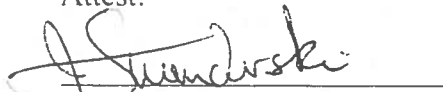
1. Files containing personally identifiable information are kept in a locked file cabinet except when an employee is working on the file
2. Employees will not leave sensitive papers out on their desks when they are away from their work stations.
3. No visitor will be given any entry codes or allowed 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 May 11, 2020 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: 05/11/2020

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.
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.