BROWNSVILLE
PUBLIC UTILITIES BOARD

Date: July 19, 2022
To: All Vendors
Subject: Addendum #1

REFERENCE: P054-22 Cyber Liability Insurance

This Addendum forms part of the contract and clarifies, corrects or modifies original proposal document.

Question 1: Need remediation steps taken by BPUB from 3/6/2022 cyber event.

Answer 1: High level summary of steps taken by BPUB after cyber incident in March.

1. Next-Gen Anti-virus purchased and rolled out
2. Monitored managed threat hunting service purchased to detect and protect against abnormal client behavior or current vulnerabilities in our environment
3. Unit 42-services contracted to assist with incident response and remediation
4. MFA (Multi-Factor authentication)- DUO installed and rolled out.
5. External Firewall replacement and upgrade
6. Exagrid-backup solution to protect backups against Ransomware attacks
7. Backblaze – Backup solution uploading data daily to the cloud
8. Working on Encryption of all mobile devices – in progress
    a. Estimated time of completion approximately August 8, 2022.

Question 2: Need update on the status of the 3/6/2022 cyber claim and which direction it is headed

Answer 2: The claim has been resolved pending final invoices and insurance carrier closure. Per the adjuster - This claim was recently “closed” by breach counsel and the forensics team, meaning that all work is complete. It was determined that the Insured does not have any continuing notification obligations, and thus costs, beyond those known, are expected to be limited to any trailing invoices from counsel and/or the forensics team. To date, there has been approximately $49,235 paid in expenses, and $96,618.68 in reimbursement to the Insured.

Question 3: Need copy of cyber incident response plan.

Answer 3: Attached is the Computer Security Incident Response plan.

Question 4: Need to know the expiring cyber premium. Need copy of expiring cyber policy form.

Answer 4: BPUB does not believe release of the requested information is necessary for prospective bidders to offer a proposal in response to this RFP solicitation. Please refer to the 2022 BPUB Cyber Coverage Specifications provided as exhibits.

Question 5: Is current carrier offering renewal terms?

Answer 5: BPUB issued an RFP for Cyber Insurance in July 2019 and awarded a contract that went into effect October 1, 2019. The original contract for Cyber Insurance was for one year with two additional one-year options. BPUB exercised the first and second options. The current contract for Cyber Insurance is now in effect until October 1, 2022. BPUB has no reason to believe the current carrier will not offer a renewal quote for Cyber Insurance as part of this RFP process.

Question 6: What were the remediation steps for social engineering claim in 2019-20 policy period.

Answer 6: Brownsville PUB added a multi-step Direct Deposit Verification Form and Procedure that requires review and approval by Accounting staff, the Treasury & Accounting Support Services Manager, the Director of Finance and the Chief Financial Officer. Forms are attached.

Question 7: Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form? Y or N

a. If "Yes", provide the approximate number of unique records: Paper records: Electronic records:

Answer 7: Yes, electronic records for approximately 60,000 customers and 600 employees.

Question 8: Do you collect, store, host, process, control, use or share any biometric information or data, such as fingerprints, voiceprints, facial, hand, iris or retinal scans, DNA, or any other biological, physical or behavioral characteristics that can be used to uniquely identify a person? Y or N

a. If "Yes", have you reviewed your policies relating to the collection, storage and destruction of such information or data with a qualified attorney and confirmed compliance with applicable federal, state, local and foreign laws? Y or N

Answer 8: No

Question 9: IT Director name, contact information and IT security designations.

a. How many IT personnel are on your team?
b. How many are dedicated to IT security?

Answer 9: Eddy Hernandez, Director of Customer Service and IT
ehernandez@brownsville-pub.com
956.983.6130

a) 18
b) 2

Question 10: Is your network security outsourced or managed internally? If outsourced please explain.

Answer 10: Managed internally with external threat hunting monitored - 24x7.

Question 11: Do you tag external emails to alert employees that the message originated from outside the organization? Y or N

Answer 11: No

Question 12: Have you implemented any of the following to protect against phishing messages? SPF, DKIM or DMARC?

Answer 12: Yes, DMARC & DKIM

Question 13: Do you use Office 365? Y or N

a. If yes, do you use the Office 365 advanced threat protection add-on? Y or N

Answer 13: No

Question 14: Do you use a cloud provider to store data or host applications? Y or N

a. If yes, provide the name of the cloud provider:
b. Do you use MFA to secure all could provider service (AWS, Azure, Google, etc.)? Y or N
c. Do you encrypt all sensitive and confidential information stored on your organizations systems and networks?

Answer 14: Yes

a) Backblaze (cloud backup storage provider)
b) No
c) Encrypted at rest

Question 15: Who is your MFA provider (AuthO, Duo, LastPass, Okta, OneLogin, etc.)?

a. What type of MFA (Mobile OTP, Physical Key, Push-based auth, Cert-based, etc.)?

Answer 15: DUO

a) Mobile, physical key & push

Question 16: Do you enforce application whitelisting/blacklinting? Y or N

Answer 16: Yes

Question 17: Is EDR deployed on 100% of endpoints? Y or N

a. If no, please explain:

Answer 17: Yes- Palo Alto Cortex

Question 18: Can user access the network with their own devices ("Bring your own devise")? Y or N

a. If Yes, is EDR required to be installed on these devices? Y or N

Answer 18: Yes

a) No

Question 19: Do you use MFA to protect all local and remote access to privileged user accounts? Y or N

Answer 19: Yes

Question 20: Do you manage privileged accounts using privileged account management software (PAM – cyberark, beyontrust, etc.)? Y or N

a. If yes, please provide provider name:
b. If yes, is access protected by MFA?

Answer 20: Yes

a) ManageEngine – ADManagerPlus
b) No

Question 21: Do you actively monitor all administrator access for unusual behavior patterns? Y or N

a. If yes, please provide the name of the monitoring tool:

Answer 21: Yes

a) Palo Alto Cortex XDR – threat hunting monitoring – 24x7

Question 22: Do you roll out a hardened baseline configuration across severs, laptops, desktops, and managed mobile devices? Y or N

Answer 22: No

Question 23: Do you record and track all software and hardware assets deployed across your organization? Y or N

a. If yes, provide the name of the tool used for this purpose (if any):

Answer 23: Yes

a) ManageEngine Desktop Central and also in-house IT asset inventory

Question 24: Do non-IT users have local administration rights on their laptop/desktop? Y or N

Answer 24: No

Question 25: How frequently do you install critical and high severity patches across your enterprise (1-3 days, 4-7 days, 8-30 days, 1 month or longer)?

Answer 25: 8-30 days, 1-3 days on-demand response to highly critical patches

Question 26: Do you have any end of life or end of support software? Y or N

a. If yes, is it segregated from the rest of the network? Y or N

Answer 26: Yes

a) No

Question 27: Do you use a protective DNS service (PDNS) (Xscaler, Quad9, Open NDS or other public section PDNS to block access to known malicious websites? Y or N

a. If yes, provide the name of the DNS provider:

Answer 27: Yes

a) Umbrella – Open DNS

Question 28: Do you use endpoint application isolation and containment technology on all endpoints? Y or N

a. If yes, what provider do you use (Apozy Authentic8, bitdefender, cigloo, etc):

Answer 28: Yes

a) Palo Alto – Managed threat hunting services

Question 29: Can users run Microsoft office macro enabled document on their system by default? Y or N

Answer 29: Yes

Question 30: Do you implement PowerShell best practices as outlined in the Environment Recommendations by Microsoft? Y or N

Answer 30: N/A

Question 31: Do you utilize a security information and event management system (SIEM)? Y or N

Answer 31: No

Question 32: Do you utilize a security operations center (SOC)? Y or N

a. If yes, is your SOC monitored 24hours a day, 7 days a week? Y or N
b. If yes, who is the provider (insightVM/Rapid7, Nessus, Qualys, etc.):
c. If yes, what is your patching cadence (1-3 days, 4-7 days, 8-30 days, 1 month or longer, etc.):

Answer 32: Yes

a) Yes
b) Palo Alto networks – Managed threat hunting and Unit42 services
c) 8-30 days, 1-3 days on-demand response to highly critical patches

Question 33: Do you use a data backup solution? Y or N

a. If yes, what best describes your data backup solutions?
   i. Backups are kept locally but separate from your network?
   ii. Backups are kept in a dedicated cloud backup service?
   iii. You use a cloud-syncing service (dropbox, ondrive, sharepoint, etc.?):
   iv. Are you backups encrypted? Y or N
   v. Do you have immutable backups? Y or N
   vi. Are your backups secured with different access credentials from other administrator credentials? Y or N
   vii. Do you utilize MFA for both internal and external access to your backups? Y or N
   viii. Do you test the successful restoration and recovery of key server configurations and data from backups in the last 6 months? Y or N
   ix. Are you able to test the integrity of backups prior to restoration to ensure that they are free of malware? Y or N
   x. Estimated amount of time it will take to restore essential functions using backups in the event of a widespread malware or ransomware attack

within your network (0-24 hours, 1-3 days, 4-6 days, 1 week or longer, etc.)?

Answer 33: Yes

a) We currently use Veaam as the backup engine. Backups are kept in two locations using Exagrid appliances. Backups are then sent to a cloud backup site hosted by Backblaze. We also backup and replicate critical systems every 15 mins using Purestorage to local and remote location.

   i. Yes
   ii. Yes
   iii. Yes, Backblaze
   iv. Yes
   v. Yes
   vi. Yes
   vii. Yes
   viii. Yes
   ix. No
   x. 0-24hrs

Question 34: Do any of the following employees at your company complete social engineering training:

a. Employees with financial or accounting responsibilities? Y or N
b. Employees without financial or accounting responsibilities? Y or N
c. If yes, does your social engineering training include phishing simulations? Y or N

Answer 34:

a) Yes
b) Yes
c) Yes

Question 35: Does your organization send and/or receive wire transfers? Y or N

a. If yes, does it include a wire request document form? Y or N
b. If yes, is there a protocol for obtaining proper written authorization for wire transfers? Y or N
c. If yes, is a separation of authority part of the protocol? Y or N
d. If yes, is a protocol for confirming all payment of funds transfer instructions/requests from a new vendor, client or customer via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer <u>before</u> the payment or funds transfer instruction/ request was received? Y or N
e. If yes, is a protocol for confirming any vendor, client or customer account information change requests (including requests to change bank account numbers, contact information or mailing addresses) via direct call to that vendor, client or customer using only the telephone number provided by the vendor, client or customer <u>before</u> the change request was received? Y or N

Answer 35: Yes

a) Yes
b) Yes
c) Yes
d) Yes
e) Yes

Question 36: In the past 3 years, has the entity received any complaints or written demands or been a subject in litigation involving matters of privacy injury, breach of private information, network security, defamation, content infringement, identity theft, denial of service attacks, computer virus infections, theft of information, damage to third party networks or the ability of third parties to rely on the entities network? Y or N

Answer 36: No

Question 37: In the past 3 years, been the subject of any government action, investigation or other proceedings regarding any alleged violation of privacy law or regulation? Y or N

Answer 37: No

Question 38: In the past 3 years, notified customers, clients or any third party of any security breach or privacy breach? Y or N

Answer 38: No

Question 39: In the past 3 years, received any cyber extortion demand or threat? Y or N

Answer 39: Yes

Question 40: In the past 3 years, sustained any unscheduled network outage or interruption for any reason? Y or N

Answer 40: No

Question 41: In the past 3 years, sustained any property damage or business interruption losses as a result of a cyber-attach? Y or N

Answer 41: No, please refer to Loss History Reports provided as Exhibits.

Question 42: Do you or any other person or organization proposed have knowledge of any security breach, privacy breach, privacy-related event or incident or allegations of breach of privacy that may give rise to a claim? Y or N

Answer 42: No

Question 43: In the past 3 years, has any service provider with access to network or computer systems sustained an unscheduled network outage or interruption lasting longer than 4 hours? Y or N

a. If yes, did the entity experience an interruption in business as a result of such outage or interruption? Y or N

Answer 43: No

The signature of the company agent, for the acknowledgement of this addendum, shall be required.
Complete information below and return via e-mail to: dsolitaire@brownsville-pub.com.

I hereby acknowledge receipt of this addendum.

Company: ____

Agent Name: ____

Agent Signature: _______________________________________

Address: ____

City: ___________________ **State:** ___________________ **Zip:**________

Phone #:___________________**E-mail address:**____________________________

If you have any further questions about the Proposal, call 956-983-6366.

Diane Solitaire
BY: Diane Solitaire
Purchasing

BROWNSVILLE PUBLIC UTILITIES BOARD	Computer Security Incident Response	Department	Information Technology
		Procedure Number	ITH-1501-P
		Effective Date	10/30/2020
		Revision Number	N/A
		Final Approver	Executive Management

1.0 Purpose

The purpose of this procedure is to establish a protocol to guide a response to a computer incident or event impacting Brownsville Public Utilities Board (BPUB) computing equipment, data, or networks.

2.0 Scope

This procedure applies to all BPUB employees, contractors, consultants, vendors, and temporary employees, including all personnel affiliated with third parties that use BPUB systems. This procedure applies to all information technology equipment and assets that are owned or leased by BPUB and other information equipment that may be used to access BPUB systems within the company firewall.

3.0 Definitions

3.1 Administrator – The default user account that by default has access to all commands and files on a Microsoft operating system.

3.2 Computer Security Incident – is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

3.3 Data destruction - Is the process of destroying data stored on tapes, hard disks and other forms of electronic media so that it is completely unreadable and cannot be access or used for unauthorized purposes.

3.4 Root – is the user name or account that by default has access to all commands and files on a Linux or Unix-like operating system.

3.5 Web Server – Is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form web pages to users.

4.0 Roles and Responsibilities

4.1 Executive Management ensures implementation of this procedure.
4.2 Senior Management ensures compliance with this procedure.

4.3 Middle Management enforces this procedure.

4.4 All employees, contractors, consultants, vendors, and temporary employees, including any third party using BPUBs network must follow this procedure.

5.0 Procedures

5.1 Incident Reporting

5.1.1 All computer security incidents, including suspicious events, shall be reported immediately (orally or via e-mail) to the Information Technology (IT) Department and/or by the department supervisor of the employee who witnessed/identified the breach.

5.2 Escalation

5.2.1 The IT manager and/or department supervisor needs to determine the criticality of the incident. If the incident is something that will have serious impact, the IT Director will be notified and briefed on the incident.

5.2.2 The IT Director will determine if other agencies, departments, or personnel need to become involved in resolution of the incident. Only the Communications and Public Relations Department will speak to the press about the incident.

5.3 Mitigation and Containment

5.3.1 Any system, network, or security administrator who observes an intruder on Brownsville Public Utilities Board (BPUB) network or system should take appropriate action to terminate the intruder’s access.

5.3.2 Affected systems, such as those infected with malicious code or systems accessed by an intruder should be isolated/disconnected from the network until the extent of the damage can be assessed by the IT department. Any discovered vulnerabilities in the network or system will be rectified by appropriate means as soon as possible.

5.4 Eradication and Restoration

5.4.1 The extent of damage must be determined and course of action planned and communicated to the appropriate parties.

5.5 Information Dissemination

5.5.1 Any public release of information concerning a computer security incident shall be coordinated through the Communications and Public Relations Department.

5.5.2 The IT Director shall manage the dissemination of the incident information to other participants, such as law enforcement or other incident response agencies.

5.6 Ongoing Reporting

5.6.1 After the initial oral or e-mail report is filed, and if the incident has been determined to be a significant event, subsequent reports shall be provided to the IT Director and appropriate managers.

5.6.2 Incidents such as individual workstations infected with malware are considered minor events and need not be followed up with a written report.

5.6.3 The incident reports shall be submitted within 24 hours of the incident.

5.6.4 An agency may be required to provide reports sooner in accordance with more stringent regulations (e.g., Social Security Administration and Internal Revenue Service.)

5.6.5 A general report to the IT Director and IT Security Administrators should contain the following:

5.6.5.1 Point of Contact
5.6.5.2 Affected systems and locations
5.6.5.3 System description, including hardware, operating system, and application software.
5.6.5.4 Type of information processed.
5.6.5.5 Incident description.
5.6.5.6 Incident resolution status.
5.6.5.7 Damage assessment, including any data loss or corruption.
5.6.5.8 Organizations contacted.
5.6.5.9 Corrective actions taken along with lessons learned.
5.6.5.10 Notifications to entities affected.

5.6.6 A follow-up report shall be submitted upon resolution by those directly involved in addressing the incident.

5.7 Review

5.7.1 After the initial reporting and/or notification, the IT manager, department/agency managers and IT Director reviews and reassess the level impact that the incident created.

6.0 References

Not Applicable

7.0 Approvals

Role	Name and Title of Approver	Approval Signature	Date Approved
Procedure Writer	Rolando Chacon IT Cyber Security Administrator		
Records Management	Nancy Tello Enterprise Content, Records, and Policies Manager		
Middle Management	Sergio Martinez IT Area Manager		
Senior Management	Eddy Hernandez IT Director		
Executive Management	Leandro Garcia Chief Financial Officer		

8.0 History

Effective Date	Revision Number	Final Approver	Description of Change
10/30/2020	N/A	Executive Management	Created Procedure

9.0 Appendix

Not Applicable

BROWNSVILLE
PUBLIC UTILITIES BOARD

Direct Deposit Authorization Form

Dear Vendor,

The Brownsville Public Utilities Board (BPUB) is pleased to provide our vendors with the opportunity to receive payments directly through an Automated Clearing House (ACH). The ACH is an automated process that permits funds to be directly transferred to your financial institution. ACH will alleviate lost checks in the mail, potential mail fraud, and also expedite your payments upon payment terms. Whenever you enroll in ACH, the email address you provide below is automatically setup to receive electronic notifications when BPUB processes an ACH payment for you. If you are interested in this payment option please complete the information requested in this form and fax or mail back as indicated below. All fields are required.

□ New Application □ Request Change □ Request Cancellation

Vendor Information

Business Name: ____________________

Tax ID Number: ____________________

Remit to Address: ____________________

City: ____________________ State: __________ Zip Code: __________

Bank Information

Bank Name: ____________________

Bank Routing (ABA) Number (9 digit number): ____________________

Bank Account Number: ____________________

Please enclose one of the following for verification:

□ Voided Check

□ Specification form from bank

Check One:

□ Checking Account

□ Savings Account

Authorization

I, ____________________, as an authorized signer for ____________________
do hereby authorize the BPUB to deposit payments by ACH directly into the above specified bank account and request payment notification to be sent to the recipient e-mail address below.

____
Authorized Signature

____
Title

____
Date Telephone Number

____
Electronic Notification E-Mail Address

Mail to:
Brownsville Public Utilities Board Attn: Finance Department
P.O. Box 3270 Brownsville, TX 78523-3270
Email to: APinvoices@brownsville-pub.com

E-mail invoices to: APinvoices @brownsville-pub.com

BROWNSVILLE
PUBLIC UTILITIES BOARD

Direct Deposit Verification Form

The following checklist will be used to reduce the risk of impostor fraud in the Accounts Payable Department. All steps must be completed within three (3) business days and payments to the vendor are not authorized until step 4 "Management Review and Concurrence" is complete.

1. ***Verify the Request***
   a. Watch for red flags
      i. Follow up with the requestor.

   b. For requested changes, the Accountant and AP Clerks will compare the details (i.e., names, titles, e-mail address, fax/telephone number, signature, etc.) between the old and new Direct Deposit Authorization Form and look for any anomalies. Accountant completes section. Accountant and AP clerk initials.

   Anomalies Yes □ No □ If yes, contact Manager for further instructions.

   Findings: ____

   Accountant Initials: ____________ AP Clerk Initials ____________

   c. Verify by calling the vendor
      i. AP Clerks will contact vendor by a telephone call using Banner contact information and perform a verification with the individual who signed the Direct Deposit Authorization Form. Signer may designate an authorized individual to perform verification. AP Clerk will explain in notes and include name/title of the individual performing verification.

   Vendor Name: ______________________________ Vendor ID: ________________

   Contact Number: _________________Contact Person: _________________________

Verified Banking Information	Verification
Bank Name	□
Bank Routing Number	□
Bank Account Number	□

   AP Clerk Signature: ______________________Verification Date ____________

   Notes: ____

   ____

   ____

   Accountant Enters Dates of Previous Direct Deposit Changes :

2. ***Implement Dual Custody***
   a. AP Clerks will verify payment changes with requestor before initiating a request.

   b. Accountant will verify that the EIN is the same on file. If not, Purchasing will contact vendor directly to obtain a new W-9 form.

      EIN: ________________ Verified Y/N: _____
      Notes: ____

   c. Accountant will confirm if banking information has been verified before entering information in Banner. Voided check will be used to enter banking information in Banner. Quality Reviewer will verify correct banking information in Banner.

      Accountant Signature: ____________________Entered Date: _________________

      Quality Review By: __________________Quality Review Date: _______________

      Print Banner banking information and attach as supporting documentation.

3. ***Monitor BPUB's accounts***
   a. Accountants and Treasury and Accounting Support Services Manager will monitor bank accounts daily.

4. ***Management Review and Concurrence***
   a. Treasury and Accounting Support Services Manager will review all documents and ensure all proper steps outlined above were conducted.

      Signature: ______________________________________ Date: __________
      Treasury & Accounting Support Services Manager

   b. Director of Finance and Chief Financial Officer ensure all proper steps outlined above were conducted.

      Signature: _________________ Signature: _________________
      Director of Finance Chief Financial Officer

      Date: _____________________ Date: _____________________

5. ***Record Keeping***

   a. Accountant will scan these documents to a secure folder for easy reference.

      Initials: _________ Date: _______

   Vendor's Name: ____

Direct Deposit Verification Work Instructions

Impostor fraud occurs when a fraudster impersonates someone you know and trust like a vendor or executive. The impostor contacts you through phone, email, fax, or mail and submits a change to vendor payment instructions. This results in the payment going to the fraudster rather than where we intended.

The attached Direct Deposit Verification form was developed and implemented to reduce BPUB's risk of impostor fraud. This form is required to be completed for every direct deposit verification, whether it is a new Direct Deposit Authorization or a requested change. The steps outlined below will serve as work instructions for the staff affected.

The premise of the form is to follow three steps; 1) verify the request, 2) implement dual custody, and 3) monitor accounts. Please note that step 4 is built in redundancy to ensure the change is appropriately verified and approved. Each step requires an employee's signature acknowledging the completion of the step. Each step is outlined below:

Step 1. Verify the Request

If you receive a request from a vendor or executive to change payment details such as account or invoice information, always make sure the request is authentic.

Always verify information by calling the vendor. If a request seems out of the ordinary, follow up with the requestor, especially if the request is made electronically.

Do not respond directly to the request. For example, if a vendor contacts you by email, confirm by phone. Be sure to only use the contact information on file in Banner. Never use the information provided in the request, as it may also be fraudulent.

Step 2. Implement Dual Custody

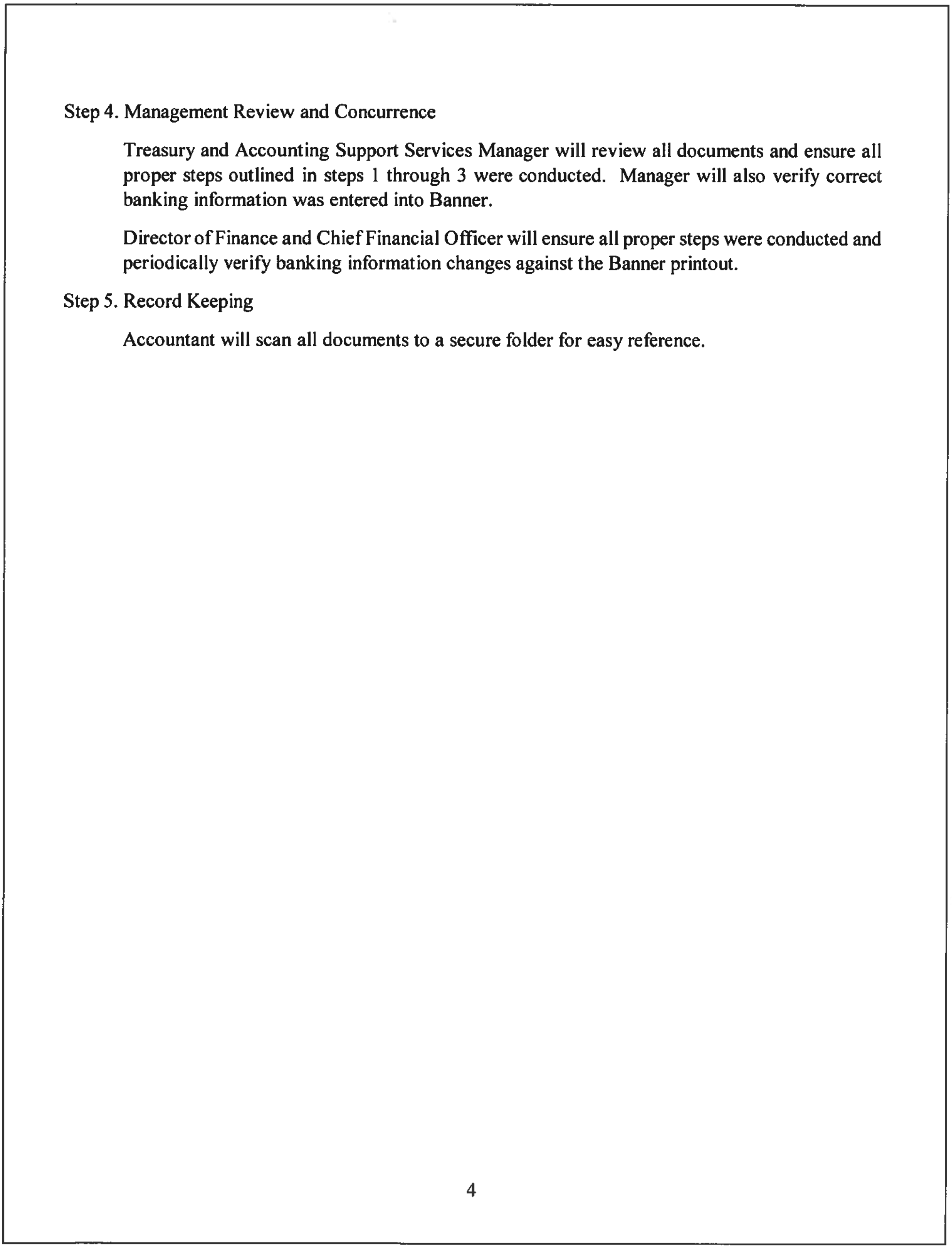
Dual custody requires two users on different computers or mobile devices to initiate and approve online payments and administrative changes. This serves as a second chance to spot a fraudulent payment before it goes out the door. Payments require prior approval by either the Treasury and Accounting Support Services Manager or the Director of Finance.

AP Clerks will verify payment changes with requestor before initiating a request. Pay close attention to the payment details, and note any changes from the information on file in Banner.

The assigned Accountant will verify that the EIN is the same on file and confirm that all banking changes have been verified before updating the banking information in Banner. Once changes are entered into Banner, another employee will conduct a quality review confirming the banking information was entered correctly.

Step 3. Monitor BPUB's Accounts

Accountant and Treasury and Accounting Support Services Manager will monitor bank accounts daily for unusual activity.



Step 4. Management Review and Concurrence

Treasury and Accounting Support Services Manager will review all documents and ensure all proper steps outlined in steps 1 through 3 were conducted. Manager will also verify correct banking information was entered into Banner.

Director of Finance and Chief Financial Officer will ensure all proper steps were conducted and periodically verify banking information changes against the Banner printout.

Step 5. Record Keeping

Accountant will scan all documents to a secure folder for easy reference.