

Planning Committee Minutes
Wednesday, March 9, 2022
via zoom/telephone/in person

MEMBERS PRESENT: Shirley Copes, Paula Freedman, Steve Hodgens, Darryl "DJ" Williams
MEMBERS EXCUSED: None
MEMBERS ABSENT: Elizabeth Hakanson
STAFF PRESENT: Carolyn D. Brown, Todd M. Goehle

CALL TO ORDER:

The March 9, 2022 Planning Committee meeting called to order at 4:47 PM by the Committee Chair Shirley Copes. It was noted for the record that a quorum was present.

DJ Williams attended the meeting as part of his New Board Member orientation.

APPROVAL OF PREVIOUS MINUTES

Steve Hodgens moved the motion to approve the February 2022 minutes. It was seconded by DJ Williams and unanimously approved.

PRESENTATION

Strategic Plan Goal 3 Update: IT Assessment

On 9 March 2022, Community Engagement Director Todd Goehle provided an update to the Planning Committee about the Progress made towards Strategic Plan Priority 3: Strengthen Information Technology (IT) and Facilities to support agency operations. Mr. Goehle also provided an overview of the IT Assessment pursued and finalized by FoxPointe Solutions for PEACE, Inc.

GRANT SUMMARY REPORT:

Current Grant Summary report was distributed to the Committee in the meeting packets for their review.

Executive Director Carolyn Brown and Community Engagement Director Todd Goehle provided a monthly grants overview and discussed a recently awarded "Aging-in-Place Home Modification" Pilot Program within the agency's Department of Energy and Housing Services.

OLD BUSINESS: None

NEW BUSINESS:

HR Director Catherine Green Harris announced her plans to retire effective December 2022. A committee of staff will be formed to begin the search for a replacement.

PEACE, Inc. was highlighted in a Press Conference with County Executive Ryan McMahon regarding new funding aimed at repairs to homes of senior citizens.

OTHER: None

ADJOURNMENT

Paula Freedman moved a motion to adjourn the March 9, 2022 Planning Committee meeting. It was seconded by Steve Hodgins and unanimously approved. The meeting adjourned at 5:27 PM.

PEACE, Inc. Recent Grant Applications 2/22/2022

<u>Funding Source</u>	<u>Project</u>	<u>Program</u>	<u>Submission Date</u>	<u>Request Amount</u>	<u>Status</u>	<u>Award Date</u>	<u>Award Amount</u>	<u>FY Submitted</u>	<u>Lead Writer/Submitter</u>
The Davies Foundation	BBBS	BBBS	BBBS 2/4/2022	Amount decided by the Davies Foundation	Pending				Todd Arnold - BBBS Volunteer (employees of the Davies Company submit applications to the Foundation for organization's of their choice).
			BBBS 2/1/2022	\$7,500	Not Awarded	1/9/2022			
The John Ben Snow Foundation & Memorial Trust	BBBS School-Based Programs		BBBS 1/3/2021	\$10,000	Awarded	1/3/2021	\$10,000		John Bruzdinski
Summit Federal Credit Union	Community and School Based Programs		SSFRC 12/17/2021	\$82,676	Pending				Jerry Barker
Onondaga County Save the Rain Program	Southside Revitalization Project		BBBS 12/15/2021	\$15,000	Awarded	12/14/2021	\$15,000		Todd Goehle
Department of Children and Family Services Renewal	BBBS School-Based Mentoring, Onondaga County		BBBS 12/1/2021	\$5,000	Awarded	12/29/2021	\$5,000		Lucy Totino
Oswego County Youth Bureau BS Oswego County/Central Square		Head Start / Early Head Start Baldwinville, Genesee, James St, Jordan Elbridge, LaFayette, Liverpool, Merrick, Sumner	BBBS 11/19/2021	\$540,800	Awarded	11/22/2021	\$540,800		Rebecca Heberle
New York Office of Children and Family Services	Head Start Stabilization								
City of Syracuse CDBG	Dunk Your Junk	Family Services	11/12/2021	\$71,637.04	Pending				Lucy Totino
Inspire Brands/Arby's - Utica Branch	BBBS Salaries	BBBS	11/8/2021	\$2,000.00	Awarded	11/28/2021	\$2,000		Todd Goehle
Inspire Brands/Arby's - Syracuse Branch	BBBS Holiday Event	BBBS	11/8/2021	\$27,800	Awarded	12/17/2021	\$27,800		Todd Goehle
CO-OP Fund (EITC Funders Network, Community Foundation Opportunity Network, and CFLeads)	EITC Tax Recruitment and Enrollment	EITC	10/1/2021	\$96,500	Awarded	10/21/2021	\$100,000		Todd Goehle

PEACE, Inc. Recent Grant Applications 2/22/2022

OCFS and Onondaga County	Gun Violence Funding	Family Services / BBBS	9/27/2021	\$20,835	Awarded	9/27/2021	\$20,835	Carolyn Brown
Fatherhood Connection, Inc.	Fatherhood Initiative	Family Services	9/24/2021	\$8,000	Awarded	9/24/2021	\$8,000	Carolyn Brown
National Grid	BBBS Corporate Mentorship Program	BBBS	9/8/2021	\$13,000	Pending			Todd Goehle
United Way	Free Tax Program	Free Tax Program	9/3/2021	120,000.00	Awarded	11/1/2021	\$110,000	Todd Goehle
United Way	BBBS	BBBS	9/3/2021	16,150.00	Awarded	11/1/2021	\$16,000	Todd Goehle
OPWDD	Project Connections	ESFRC	8/29/2021	\$73,238	Awarded	8/18/2021	\$73,238	Mary Beth Welch, Nancy Turo
NYSOFA (Magineirelli)	Senior Meals, Trips	Foster Grandparents, Eastwood Community Center, Senior Nutrition	8/27/2021	\$20,000	Awarded	7/23/2021	\$20,000	Lucy Totino
SCSD	SCSD Alternative Classroom	ESFRC	8/23/2021	\$65,000	Awarded	Waiting for Contract	\$65,000	Mary Beth Welch, Nancy Turo
BNY Mellon	BBBS Corporate Mentorship Program	BBBS	7/16/2021	\$25,000	Awarded	9/1/2021	\$20,000	Todd Goehle
Mother Cabrini Health Foundation	Southside Revitalization Project	SSFRC	5/20/2021	\$75,000	Not Awarded	12/10/2021		Todd Goehle
Housing and Urban Development	Aging in Place Program	Weatherization	5/18/2021	\$500,000	Not Awarded	8/1/2021		Todd Goehle
St. Augustine's Roman Catholic Church	CWFRFC Food Pantry	CWFRFC	5/3/2021	\$700	Awarded	5/3/2021	\$700.00	Mary Beth Welch
Syracuse HOPE/United Way	Let Me Be Great, Dunk Your Junk, Additional Summer Funds	ESFRC	5/1/2021	\$75,000.32	Awarded	7/19/2021	149,933 Total	Carolyn Brown, Nancy Turo
CNY Food Bank	2021-2022 HPNAP	CWFRFC	4/30/2021	Amount Decided by CNY Food Bank	Awarded	6/25/2021	\$14,660	Mary Beth Welch, Meg Tamilio
CNY Food Bank	2021-2022 HPNAP	ESFRC	4/30/2021	Amount Decided by CNY Food Bank	Awarded	6/25/2021	\$15,542	Mary Beth Welch, Meg Tamilio
CNY Food Bank	2021-2022 HPNAP	SSFRC	4/30/2021	Amount Decided by CNY Food Bank	Awarded	6/25/2021	\$14,790	Mary Beth Welch, Meg Tamilio

PEACE, Inc. Recent Grant Applications 2/22/2022

CNY Food Bank	2021-2022 HPNAP	WSFRC	4/30/2021	Amount Decided by CNY Food Bank	Awarded	6/25/2021	\$15,232	Mary Beth Welch, Meg Tamilio
Onondaga County Office of the Aging	EISEP- 3 Year Contract	Senior Supports	4/23/2021	Amount Decided by Onondaga County	Awarded	6/17/2021	\$171,000	Beth O'Hara
Onondaga County Office of the Aging	NAP- 3 Year Contract	Senior Supports	4/23/2021	Amount Decided by Onondaga County	Awarded	6/17/2021	\$130,000	Beth O'Hara
Onondaga County Save the Rain Program	Weatherization Driveway Installation	Department of Energy and Housing	3/1/2021	\$176,034	Awarded	10/5/2021	\$176,034	Jerry Barker
ARISE Food Insecurities Distribution	Not determined yet which senior program will use these funds	Agencywide	2/22/2021	\$27,000	Awarded	2/22/2021	\$27,000	NA Misc check was mailed to the Agency
Housing Visions	Housing Visions/ESFRC Housing Eviction/Rental Relief Program	FRC	2/1/2021	\$23,088	Awarded	2/1/2021	\$23,088	Mary Beth Welch, Todd Goehle, Nancy Turo
Jon Ben Snow Foundation	BBBS School-Based Mentoring Program	BBBS	1/31/2021	\$7,500.00	Awarded	9/9/2021	\$7,500	Todd Goehle
Romano Automart	Romano Automart Holiday Hope/FRC Toilettry Program	FRC	12/1/2020	\$2,500	Awarded	12/8/2020	\$2,500	Todd Goehle
Vera House	Vera House/FRC Elder Abuse Outreach	FRC	12/1/2020	\$24,172	Awarded	4/29/2021	\$24,172	Mary Beth Welch
Onondaga County Youth Bureau	BBBS School-Based Mentoring, Onondaga County	BBBS	12/1/2020	\$15,000	Awarded	1/4/2021	\$15,000	Todd Goehle
Oswego County Youth Bureau	BBBS School-Based Mentoring, Oswego County	BBBS	12/1/2020	\$6,000.00	Awarded	3/11/2021	\$6,000	Todd Goehle
Charter Communication (Spectrum)	BBBS laptop giveaway, Nutrition Basic Needs Distribution	BBBS, Senior Nutrition	10/28/2020	\$5,000	Awarded	10/28/2020	\$5,000	Carolyn Brown
CNYCC	Partner MY5 Rebase Payment Part 1	Agencywide	10/15/2020	121,181	Accepted	10/15/2020	\$121,181	Nancy Turo, Carolyn Brown, Todd Goehle
CNYCC	VBP_4_ Imp2	Agencywide	10/13/2020	\$80,241	Accepted	10/13/2020	\$80,241	Nancy Turo, Carolyn Brown, Todd Goehle
BNYMellon	Corporate-Based Mentorship Program	BBBS	9/30/2020	\$25,000	Accepted	9/30/2020	\$25,000	Todd Goehle
Arby's Foundation	Additional Budgetary funds for BBBS Holiday Party	BBBS	9/15/2020	\$5,000	Awarded	10/29/2020	12,550	Todd Goehle
United Way	Free Tax Program	Free Tax Program	8/31/2020	136,289.00	Awarded	11/5/2020	\$110,000	Todd Goehle
United Way	BBBS	BBBS	8/31/2020	16,150.00	Awarded	11/5/2020	16,150	Todd Goehle

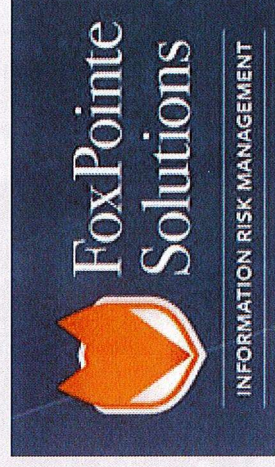


PEACE, Inc.

Information Technology Operations, and Cybersecurity Risk A Findings Report

Prepared by:

**FoxPointe Solutions, a Division of The Bonadio Group
March 2, 2022 for the 2021 Calendar Year**



Contents

Confidentiality Statement.....	
Introduction.....	
Overall Risk Ranking.....	
Effective Controls and Processes Observation	
IT Satisfaction Survey.....	
Pandemic Planning.....	
Laws, Regulations, and Standards Compliance General Observation	
General IT Department Observations and Recommendations.....	
Strategic Plan Documents.....	
Key Operational Findings and Recommendations.....	
Risk Assessment, Operations Findings and Recommendations.....	
Full Risk Assessment Matrix	
NIST Cybersecurity Framework Matrix	
Finalize the Documentation.....	
Periodic Review and Updates to the Risk Assessment.....	
Conclusion.....	
Appendix: General Key Regulatory Control Information.....	
Appendix: NIST CSF-HIPAA Crosswalk.....	
Appendix: Determining Compliance Level.....	
Appendix: HIPAA Security Risk Assessment.....	
Appendix: The Cybersecurity and Infrastructure Security Agency on Ransomware.....	
Appendix: Industry General Observations.....	
Appendix: Risk Analysis Requirements under the Security Rule.....	
Appendix: Enterprise Risk Assessment Scope and Process.....	
Appendix: IT Satisfaction Survey Results.....	
Appendix: Acronyms and Definitions.....	

Confidentiality Statement

THE ENCLOSED MATERIAL IS PROPRIETARY AND CONFIDENTIAL INFORMATION AND IS THE PROPERTY OF PEACE, INC.

The enclosed material may not be disclosed, reproduced, or used in any manner whatsoever, other than by the addressee and the addressee's authorized employees or representatives, for the purpose of evaluation of its contents, solely for the limited internal business purpose for which it is being transmitted to the addressee. Any trademarks used are the property of their respective owners. *document and all others referenced within this document contain highly sensitive and confidential information that should be communicated to internal and external parties only with extreme care.* and any of the referenced documents are proprietary, confidential information regarding the technologies, systems, and security operations and protections at PEACE, Inc. (PEACE) as completely confidential and protected as such.

This report and all deliverables from FoxPointe Solutions (FoxPointe) are intended solely for PEACE for its internal use and benefit and are not intended to nor may they be used for any other purpose. Our assessment was a point in time assessment and was an assessment of the controls in operation at the first day of fieldwork. The information contained within the report are meant to provide reasonable but not absolute findings or recommendations or assurances. FoxPointe accepts no liability or responsibility to any Third Party who gains access to a data loss or breach.

The output from the work efforts, documentation, reports, and findings surrounding this engagement are the property of PEACE, and PEACE may disclose those findings, programs and assessment documentation, testing applications, and internal workpapers for this engagement are the property of FoxPointe Solutions and constitute FoxPointe Solutions' copyrighted data. Any reproduction of the supplied documentation must be approved in writing by FoxPointe.

PEACE agreed that FoxPointe was not required to undertake any task or function that FoxPointe determined would impair its independence and PEACE did not request FoxPointe to perform any task or function that would impair its independence. Our work was limited to the specific procedures and analysis described herein and was based only on the information made available during our reviews. Accordingly, changes to the findings outlined in this report.

The services contemplated within the context of this engagement included the concepts of sample-based and risk-based assessments. Accordingly, these services do not include a system, nor do they include a detailed examination of all transactions. Therefore, they cannot be relied upon to disclose all errors or fraud that may exist. These services do not include a statement of opinion. PEACE was responsible for ensuring that all information provided to us was accurate and complete in all material respects, contained no material omissions, and that the information was reliable. PEACE assumed responsibility for obtaining all third-party consents required to enable us to access, assess, or use any third-party products necessary for the performance of the engagement. A lack of recommendation does not imply that PEACE may skip or otherwise not implement any needed controls or other changes. Senior Management (with the support of the Officers) may opt to apply controls that have been chosen independently of our recommendations to mitigate the areas of possible risks identified in this report. It should be the responsibility of the organization or entity and the regulatory and enforcement authority.

Introduction

During the months of May through July 2021, FoxPointe performed an IT Operations, Cybersecurity, Regulatory Compliance, and General Risk Assessment review surrounding cybersecurity business practices and IT general controls. That assessment was performed on data and information supplied by PEACE, via document reviews and policy and to the precautions set by PEACE based on the COVID-19 pandemic, all work was performed remotely, and our observations and recommendations reflect that level of work by PEACE on its information technology, information systems, cybersecurity, physical, technical, and administrative controls at PEACE covering covered sensitive, confidential

In general, we assessed implemented controls and:

- Documents, technologies, people, processes, implementation levels, training, management reporting, policies, cyber protection tools, etc.
- IT Operational programs, policies, processes
- Processes supporting PEACE's current cybersecurity risk assessment compliance requirements
- Vendor management and outsourced managed service providers (MSP/Cloud/TSP) assurance programs
- The protection and use of non-public (NPI/PII), confidential, and other protected data in any form (physical, electronic, and verbal)

Our work was conducted through off-site testing, key Management and stakeholder interviews, and reviews of PEACE's supplied controls, documents, and reports. The physical, administrative, and technical landscape (internal and external) and data supplied by PEACE. We assessed the cybersecurity controls, general user and application management, and other controls in place designed to meet PEACE's requirements for cybersecurity, privacy, confidentiality, availability, integrity, user access, processing information that PEACE controls.

Our work was limited to the specific procedures and analysis described herein and was based only on the information made available during our reviews. Accordingly, changes to the findings outlined in this report. Our reporting is intended to provide guidance in the application of reasonable and actionable threat mitigation recommendations, which assess cybersecurity needs and reduce the possible adverse effect on internal and external impermissible disclosures, un-approved or unknown access to data, information security laws in the overall IT/IS infrastructure.

Use of Subject Matter Experts

The consultants and subject matter experts used for the project included personnel from FoxPointe who have certifications in and actively practice within information including but not limited to:

- CISA – Information Systems Audit and Control Association Certified Information Systems Auditor
- CCSFP – Certified Assessor for the HITRUST Common Security Framework
- CTPRP – Certified Third-Party Risk Professional
- CISSP - Certified Information Systems Security Professional

The risk assessment was undertaken with the following key understandings:

- PEACE is an organization with considerable NPI to protect.
- PEACE stores, processes, and transmits protected NPI consisting of electronic and physical data for residents and individuals of New York State.
- PEACE's cybersecurity environment has a large footprint consistent with an entity equivalent in both size and function to PEACE.
- PEACE currently has other regulatory requirements with which it is complying or needs to comply, such as NY General Business Law 899-aa and 899-bb, HIPAA, etc.
- PEACE is not aware of any reportable data breaches during the assessment period.

Core Assessment Processes

FoxPointe used guidance from regulatory references and control programs and data assurance standards to assess the controls in place at PEACE and to customize the R include, at minimum, the regulations, processes, and assessment guidelines detailed by the following:

- | | |
|--|--|
| <ul style="list-style-type: none">▪ Information Systems Audit and Control Association (ISACA)▪ Certified Information Systems Auditor (CISA) procedures, standards, and guidance▪ NIST SP800-30r1▪ NIST SP800-53r4 | <ul style="list-style-type: none">▪ NIST CSF (Cybersecurity Framework)▪ NY General Business Law 899-aa and 899-bb▪ COBIT/COSO Controls Maturity▪ HIPAA/HITECH |
|--|--|

The referenced processes, controls, documents, and data can be supplied upon request.

PEACE Involvement

FoxPointe met virtually with key members of PEACE's Management Team and other personnel. They included:

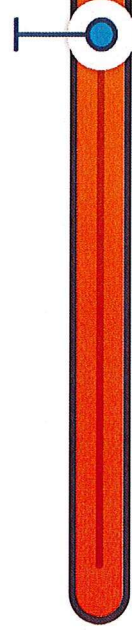
Todd Goehle, Planning and Community Engagement Manager	Chris Thompson, Information Technology Director	Holly Hastings, Child Development
Kathleen O'Brien, Chief Financial Officer	Jerry Barker, Facilities Manager	Tammi Hatch, Head Start Health (
Joseph O'Hara, Executive Director	Mary Beth Welch, Family Services Director	Melissa Farrar, Head Start Data A
Catherine Green Harris, Human Resources Director	Linda Parker, Baldwinville Site Supervisor	Stephanie Bingham, Westside Fam
Carolyn Brown, Deputy Director	Nancy Turo, Controller	Randy LaManche, Food Services L
Rollin Mincher, Eastwood Community Center Program Manager	Becky Heberle, Early Head Start and Head Start Director	Kim Barone, Head Start Associate

Overall Risk Ranking

This was the first assessment of this level of detail and testing performed for PEACE, and all findings and observations need to be assessed in that light. The graphic below in time that the assessment was completed in July 2021. No other periods or dates are represented. All circumstances and changes both internally and externally to regulat and administrative, technical, and physical environment will likely expose PEACE to multiple new areas of risk. Those new risks, along with any changes to PEACE's ris communicated to all needed stakeholders and Management at all phases of the cybersecurity compliance activities in any future endeavor or assessment taking into considera

PEACE Assessment Risk Summary Rankings – Overall Risk Rank

2021



High Risk

It is understood that when utilizing information systems and technology, there is no such thing as no risk. As illustrated by the graphic above, PEACE's overall risk posture Risk ratings were assessed as a qualitative test and have included cybersecurity control items that were implemented and operating effectively at the time of the assessment and severity of any risks surrounding the controls that may need enhancements. The services performed did not exploit the potential risks found (e.g., capturing a cell ph access database on it to trigger the incident response plan to assess outcome).

Generally, the overall rating is tempered with the fact that PEACE has several well-functioning controls, but also that the level of the severity of the enhancements needed is significantly increase the overall cybersecurity risk posture (remember, this is not a statement of regulatory compliance, as that is an area wherein FoxPointe consultants may be taken into consideration is that high or severe-risk items may only affect a small portion of the departments assessed (e.g., encryption is a high-risk area, but the overall identified). As a result of the assessment, we have noted areas where PEACE's ongoing efforts may need enhancements in order to meet the expectations of the control requirements of applicable laws, regulations, and standards affecting PEACE. All controls assessed, as well as remediation comments, are detailed within this report.

Additional Observation

Security Awareness and Education

As a result of interviews with staff members including Program personnel and Senior Management, it was determined that while some PEACE personnel maintain a height on an individual level; however, a full and comprehensive Agency-wide information security awareness training program is not currently in place. Security awareness training of employees, but procedural requirements to ensure that all Agency staff are required to attend and complete regular security awareness training is not in place.

Recommendation

The Agency should continue its efforts to develop and maintain a culture of heightened information security awareness through an updated information security PEACE should ensure that Senior Management is included in the information security awareness training program to support the "Tone at The Top" mentality. D should be an active part of the "C" suite roles and responsibilities for key governance requirements across the entire organization. As PEACE works to maintain awareness throughout the entire Agency, an information security awareness training program needs to be implemented that focuses on the relevant security awaren

1. Phishing Awareness – Phishing should be a training focus due to the increase in both the frequency and sophistication of these types of attacks in recent years
2. Removable Media – Employees need to continue to understand the risks in using removable media, as well as acceptable uses and Agency policies regarding the
3. Passwords – Employees need to be continuously educated on how to select sufficiently strong passwords, and how to properly protect passwords to limit the ri
4. Physical Storage – The proper storage requirements for paper records, including guidance on not storing passwords in easily accessible areas should be part of t
5. Mobile Devices – With the continued use of mobile devices, education on mobile device security risks needs to be included in addition to acknowledgement of
6. Remote Work – Within the training program, Agency staff need to be educated on remote work best practices and be encouraged to effectively manage risks w
7. Public Internet – Employees need to be educated on the safe use of public Wi-Fi and the common signs to spot a potential scam, therein increasing overall Ager
8. Social Media and Internet Use – Employees should be educated on preventing the spread of Agency information to reduce the risk of the leverage that hackers c
9. Email Use – Education on requirements for the secure use of email accounts needs to be included in the training program to ensure that users are consistently a
10. Home Office Security – Due to the increase use of remote workforce and use of personal devices, employees should be educated on risks of not securing device

Effective Controls and Processes Observation

Within every assessment, it is highly desirable to identify and communicate the areas that have been recognized as being effectively implemented and controlled. P effective processes and controls, the overall threat posture in all areas assessed would be significantly negatively impacted. Our review identified the following as n operating effectively; they are also seen as highly desirable repeatable practices and processes that need to be continued as they are seen as meeting or exceeding industry expectations to reduce the risks to data and overall threat posture of the systems and data under the control of PEACE.

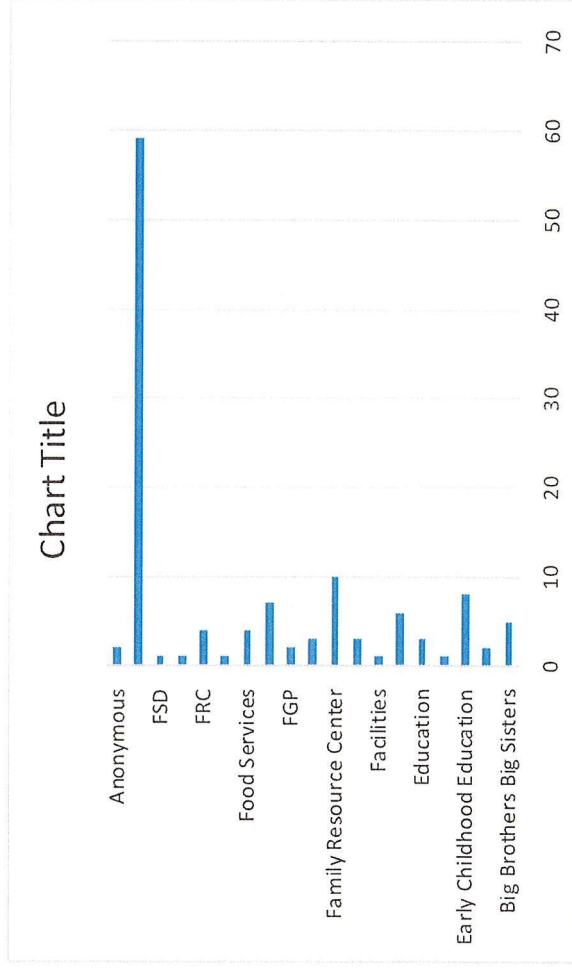
As part of the PEACE infrastructure, PEACE:

- ✓ Has a cybersecurity focus that crosses all departments and infrastructure.
- ✓ Recognizes and communicates that effective and repeated information security training is a core threat mitigation requirement.
- ✓ Engages experts to independently assess threats and controls measuring PEACE's current overall data security and privacy environment.
- ✓ Enforces a limit of three failed login attempts and users are then locked out for 30 minutes as a result.
- ✓ Documents and retains all maintenance work orders electronically.
- ✓ Escorts all visitors in sensitive areas at PEACE facilities including areas with network infrastructure.
- ✓ Properly stores information system media in secure areas that are accessible by authorized personnel only.
- ✓ Configures its main data center with tested emergency power units.
- ✓ Documents confidentiality requirements and usage restrictions for Agency assets and information throughout the Employee Handbook and other PEACE policies.
- ✓ Performs background checks (including drug tests, reference checks, state and federal registry checks and fingerprinting) on all employees prior to employment deployment.
- ✓ Follows a progressive discipline procedure with documented forms and notices that are given to employees as necessary.
- ✓ Documents sanction statements within Agency policies including the Standards of Conduct and the Employee Handbook.
- ✓ Security systems and controls protect the Agency against DOS (Denial-of-Service) attacks.
- ✓ Utilizes an industry recognized and centrally managed antivirus solution for endpoint protection.
- ✓ Utilizes numerous filtering tools and controls to minimize the amount of spam messages delivered to the end user.
- ✓ Documents explicit authorizations and approvals for remote access to the network.
- ✓ Encrypts all remote access connections.
- ✓ Enforces a 30-minute remote session timeout for inactive remote access connections.

IT Satisfaction Survey

The following information and charting are a synopsis taken from the IT Satisfaction Survey. The full results and all comments are attached in the appendices.

Q1: Which department do you work in?

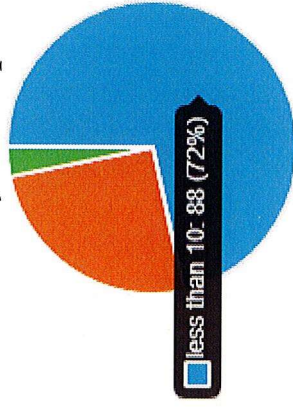


Q2: Please rank how well IT keeps the IT systems it provides up and running.

The following is an analysis of responses grouped into the following categories:

- 9-10 Very Satisfied: 61
- 7-8 Satisfied: 38
- 5-6 Needs Improvement: 16
- 1-4 Not satisfied: 8

Q3: How many IT requests have you had in the last 12 months?



The following is an analysis of responses grouped into the following categories:

- Less than 10: 88
- More than 10, less than 25: 31
- More than 25: 4

Q4: How satisfied were you with the time it took IT to respond to your last IT request?

8.11

Average Number

The following is an analysis of responses grouped into the following categories:

- 9-10 Very Satisfied: 61
- 7-8 Satisfied: 39
- 5-6 Needs Improvement: 13
- 1-4 Not satisfied: 10

Q5: Overall, how would you rank IT for support?

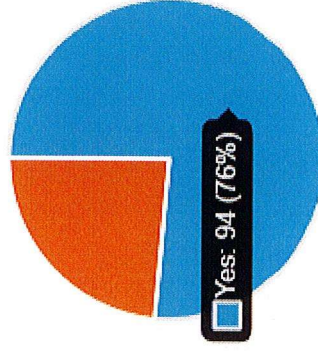
8.15

Average Number

The following is an analysis of responses grouped into the following categories:

- 9-10 Very Satisfied: 67
- 7-8 Satisfied: 34
- 5-6 Needs Improvement: 13
- 1-4 Not satisfied: 9

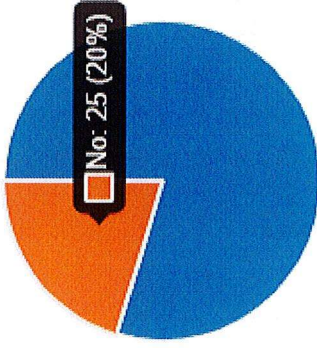
Q6: Do you use a mobile device (phone, tablet, laptop) to perform work functions (e.g., read and intranet/applications, etc.)?



The following is an analysis of responses grouped into the following categories:

- Yes: 94
- No: 39

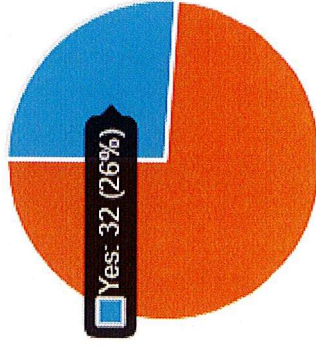
Q7: Do IT and the current systems in place meet your business and operational requirements?



The following is an analysis of responses grouped into the following categories:

- Yes: 98
- No: 25

Q8: Do you ever download applications to use on your device (laptop, cellphone, tablet)?



The following is an analysis of responses grouped into the following categories:

- Yes: 32
- No: 91

Q9: Which application(s) do you use the most?

The following is a synopsis of “like” (office applications include email, word, excel, adobe, etc.) or core (EMR/EHR, Finance, HR, etc.) applications; please note that individuals, and as such, the totals do not match the full population:

- Office Applications: 105
- Core Applications: 27
- Other (N/A, etc.): 17

Key Comments: Please note that the following comments are a sample of those shared that may be adding operational or data risks to the organization. These comments are our recommendations and suggestions.

- *I use my own laptop, not a company laptop.*
- *When working offsite I use texting and calling most. No specific applications.*
- *Online database, Microsoft Office. lots of Google products – I heavily use Google Drive, Calendar, and Sites, Microsoft 365, I got 365 so I can share with outside the agency.*
- *Dropbox*

Q10: How often do you have to perform any manual work-arounds to get your job done?

The following is an analysis of responses grouped into the following categories. Please note that there were multiple responses from some individuals, and as such, the total

- Never: 63
- Infrequent: 27
- Regularly: 14
- Almost Daily: 20

Key Comments: Please note that the following comments are a sample of those shared that may be adding operational or data risks to the organization. These comments are our recommendations and suggestions.

- *Frequently. Will use my personal phone since often sites that may be needed are blocked*
- *I'll work at home and then send my work to my email*
- *Accessing certain Internet pages sometimes is prohibited, then I would use my personal cell phone. Sometime the firewalls will prevent a document from being emailed to me*
- *Not often, only when the system is down. Usually when the internet is down, but we are able to work around most of some things.*
- *I've learned to avoid getting myself into anything that I know I won't support.*
- *Use my personal laptop for meetings since I don't have a microphone or camera on my office laptop*
- *Use my cell phone internet access*

Q11: Regarding the systems, support, and network, what have been, and/or are, your biggest (most significant)

The following is an analysis of responses grouped into the following categories:

- No challenges: 64
- System speed/connectivity: 28
- IT controls are too restrictive: 16
- Response to IT problems is slow, condescending, or ineffective: 15

Key Comments: Please note that the following comments are a sample of those shared that may be adding operational or data risks to the organization. These comments are our recommendations and suggestions.

- *Some lack of knowledge*
- *IT doesn't always check to make sure we have access to everything we should have access to*
- *Sharing Information / Data*
- *Google Docs does not work*
- *Multi-agency communication is becoming necessary to collaborate across agencies and in partnerships, this is a critical concern that prevents me from doing my job properly*
- *Questions answered in a condescending way / in a way that staff can understand it, or a "no" answer*
- *Unreliable Internet*
- *Use personal tablet because I do not have a camera on my desktop*
- *Unneeded controls to meet laws / regulations*
- *The biggest challenge with this is how our Google Drive isn't available to work with outside organizations / individuals.*
- *Use of "made up" Gmail account to be able to work on a team and share files*
- *Being bulldozed whenever a question is raised*
- *Lack of instruction offered to teach employees*

Q12: What one thing could IT do to make it easier for you to work?

The following is an analysis of responses grouped into the following categories:

- Nothing, problems are solved upon request: 70
- Faster and more reliable computers and internet: 12
- Loosen IT controls: 25
- Be more responsive, provide tips, be more understanding and less condescending: 16

Key Comments: Please note that the following comments are a sample of those shared that may be adding operational or data risks to the organization. These comments are our recommendations and suggestions.

- *Listen to what we need*

- *There seems to be an argument for everything*
- *More responsive to IT issues we may be encountering - often times no one available to answer our calls*
- *More training on a variety of IT topics*
- *Every staff member I have interacted with in IT has been very friendly and easy to communicate with*
- *IT has to remote in to install updates*
- *Bandwidth is painfully slow.*
- *Offer staff training for employees who need to learn simple basic computer skills.*
- *I save items to my desktop for access*

Q13: What are the two or three most important services IT Services provides you?

The following is an analysis of responses grouped into the following categories:

- No feedback provided: 12
- Quick to resolve issues: 64
- Uptime including internet, email, remote access, and phone: 15
- Training and technological support: 32

Key Comments: Please note that the following comments are a sample of those shared that may be adding operational or data risks to the organization. These comments are our recommendations and suggestions.

- *When I call, they do get right on the issue and are helpful to me trying to figure out my issue / problem*
- *Responding to questions or concerns promptly.*
- *Great customer service.*
- *They are very responsive to calls and quick to resolve issues.*

Q14: Is there anything else you would like to comment on?

The following is an analysis of responses grouped into the following categories:

- No: 67
- IT support is excellent: 20
- IT support is good, some improvements are needed: 23
- IT Staff are not always friendly, many improvements are needed and controls are too robust: 13

Key Comments: Please note that the following comments are a sample of those shared that may be adding operational or data risks to the organization. These comments are our recommendations and suggestions.

- *I think our IT department goes above and beyond in meeting the requests of the agency they serve*

- *Perhaps a better training system for them may better support our needs*
- *Sometimes made to feel like their questions are stupid*
- *A number of staff have shared with me that they are reluctant to reach out to IT.*
- *Lack of budget is often cited as to why a concern cannot be addressed*
- *Staff need reliable internet both remotely and onsite*
- *Community needs reliable Wi-Fi access at agency sites*
- *The IT department needs to grow in size, scope, and functionality to keep up with the agency needs and changes in technology to help the agency succeed.*
- *IT does a lot of strange things*
- *I don't have time to complete a training; I barely have time to complete this survey*

Pandemic Planning

PEACE has had to respond to an unplanned pandemic in COVID 19. That response, while coordinated and still in process, was not based on a written response plan. PEAC and restoration focused on recovery from information system outages. While most recovery and continuity plans generally address these types of geographical or man-made given to pandemics planning, as pandemics themselves pose an entirely different threat to an organization. While other disasters often only impact a limited number of individuals how pandemics interrupt business processes at all levels. Pandemic planning likewise requires organizations to anticipate alternative arrangements and fallbacks for all business embedded below.

	Natural Disaster		Pandemic	
	Local to Regional	National to Global	Months	People
Impact	Days to Weeks	People	Illness (Decreased Performance, Sick Days)	Weeks to Months
Duration	Infrastructure (Physical/ Logical), Data			
Target	Business Disruption			
Threat	None			
Warning				



Pandemic_Influenza
_Template.pdf

Laws, Regulations, and Standards Compliance General Observation

Compliance with the myriad of data security and privacy laws, regulations, and contractual standards is a **CRITICAL** risk area. Based on our review, the needed controls are required to be in place to meet the rules below were not as complete as expected. The following cybersecurity rules, laws, and standards have been identified as a set of compliance actions and controls:

- General Business Law 899-aa and 899-bb (SHIELD Act)
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM)
- Title iii of the Americans with Disabilities Act
- Payment Card Industry Data Security Standard
- HIPAA and HITECH Acts

Our observations and recommendations noted in this and all FoxPointe reports will assist PEACE Inc. regarding their compliance efforts; however, ongoing assessments of required to maintain compliance.

SHIELD Act Compliance

The SHIELD Act is an expansion of breach notification requirements and private information definitions of already existing New York State data privacy and security laws. The previous definition of "private information" that is required to be secured was expanded on by the SHIELD Act to include Social Security number, driver's license number and biometric information along with usernames and passwords and even email addresses that can be used to access an account. As part of this assessment, FoxPointe assessed core control subset of NIST Special Publication 800-53r4, and provided observations and recommendations that if implemented, would help provide real-world compliance represents suggested information security strategies to assist in ensuring SHIELD Act compliance. Some strategies listed may already be implemented (partially or in full) as c

- Implementation of a strict IT security plan that bans BYOD (Bring Your Own Device) options.
- Implementation of secure remote work requirements, such as allowing the use of virtual private network connections only.
- Implementation of a next generation firewall in combination with automated security protocols that detect, isolate and analyze threats in real time (such as intrusion c
- Implementation of a comprehensive security awareness training program (see detailed recommendations on page 3, as well as the Security Awareness Training secti
- Ensure that senior management personnel are included in and complete Agency-wide information security awareness training program requirements.
- Require all third-party vendors to uphold the Agency's IT security standards (see detailed recommendations within the Third Party Personnel section of the assessm
- Implementing encryption for all Agency emails end-to-end and create a policy prohibiting sending personal information through an unencrypted email.
- Perform ongoing risk assessments at an Agency-defined frequency.
- Implement a consistent policy for destroying paper and electronic documents containing protected information.

General IT Department Observations and Recommendations

This engagement was focused on collecting data and information on the general IT and operational control structures in place, which we are sharing below as observations encompass a general review of the people, processes, and technologies in place and our operational and risk assessment findings and observations provide detailed information internal departments and PEACE senior leaders is included along with the client IT Satisfaction Survey results which may be cross referenced to individual or multiple records.

Based on our inquiries, observations, and testing, from a competency perspective, FoxPointe would assess the current IT personnel as generally capable to support the existing being highly leveraged in reactive support of user/technology functions within the organization (e.g., ensuring that the network is functional, ensuring that email is up applications, securing remote access to the network, and ensuring that servers and infrastructure remain online).

The reactionary environment is severely limiting the ability to align the strategic goals of PEACE with a more effective IT data support and strategic data utilization environment management. Likewise, a highly reactive environment removes the IT team's ability to effectively train and stay abreast of technologies that could be communicated to PEACE and projects to enhance the support of the user and client community.

While it is expected that an IT department should perform those functions, they are only a part of the IT Team's roles. For an organization of its size and complexity, PEACE proactive planning, ongoing testing, and required internal training (e.g., cyber, ERM and IT risk management, business management, etc.) built into the processes used in and subject matter experts on new technologies that are being deployed, be forward-looking to assure "future proofing" (detailed plans for configuration management, integrity, etc.) of the environment, and bring alternatives to the user community for data use and access, etc. Dedicated the necessary amount of planning, resources, test allow for further integration and application of cybersecurity controls (e.g., disaster recovery planning, access control, auditing, etc.) and security tools (e.g., information monitoring, etc.).

This will in all likelihood require some renovation to PEACE's IT support structure, the possibility of outsourcing core and non-core applications and services, a greater use take into account and consider PEACE's overall strategic direction (and its supported operations), regulatory compliance and the proper control and risk management of the environment planning for future technology needs and trends through the use of a multi-year (at least 36 months) rolling horizon IT strategic plan. We would estimate that building a detailed initially and maintaining the plan will take an additional 60 hours per year. It is suggested that whoever is assigned the responsibility for building the plan take the required 1 plan (see the following pages for possible plans).

Please see the IT Strategic Plan supplied in a separate report for additional technological and operational recommendations

INSTRUCTIONS

1 Craft a concise and memorable statement that captures the essence of the strategy. The statement should summarize the key objectives of IT's three-to-five year strategic plan.

2 Identify five to seven metrics that define the IT organization's current and target end state.

3 List the five to seven key IT initiatives required to achieve the end state. The initiatives should be drawn from IT's three-to-five year plan.

4 Document five to seven critical assumptions underpinning the strategy, setting metrics and thresholds where necessary, to indicate when course correction is required as circumstances change.

STATEMENT OF IT STRATEGY

To help achieve company goals of improving profitability and customer loyalty by providing streamlined IT services, the company will implement a series of IT-enabled solutions that enhance the customer experience while reducing operational costs and improving efficiency.

STATE OF INFORMATION TECHNOLOGY IN 20XX

Top Five to Seven Metrics Describing the Initial State

- IT cost as a % of revenue: 3.7%
- Contribution to business process improvement (scale of 1-5): 2.5
- Total value creation from IT-enabled projects: \$3 M
- Number of new innovation ideas that pass innovation committee approval: 0
- Percentage of IT service level targets being met: 85%

Top Five to Seven IT Initiatives

1. Establish a global IT shared services center to reduce overall IT costs.
2. Implement a single ERP system to enhance functionality and improve efficiency of key business processes.
3. Introduce a new tracking system on the customer portal to enable real-time status of shipments (while ensuring compliance with most recent international regulation).
4. Develop an external collaboration portal to enable new idea exchange between IT and its suppliers.
5. Implement ITIL v3 to improve IT service management.

Top Five to Seven Underlying Beliefs and Assumptions

1. The company will achieve nominal revenue growth in 20XX.
2. Our global business operations will remain similar enough to benefit from greater harmonization.
3. There are no plans for acquisitions or divestitures that will affect current company operations.
4. Customers continue to see value-added services as key differentiator when picking shipping solutions.
5. Industry regulation will not change in a dramatic way in the next X years.

STRATEGY ON A PAGE TEMPLATE

STATEMENT OF IT STRATEGY

[Statement]

STATE OF INFORMATION TECHNOLOGY IN [YEAR]

Top Five to Seven Metrics Describing the Initial State

- [Metric] [Current State]
- [Metric] [Current State]
- [Metric] [Current State]
- [Metric] [Current State]
- [Metric] [Current State]
- [Metric] [Current State]
- [Metric] [Current State]

Top Five to Seven IT Initiatives

- 1. [IT Initiative]
- 2. [IT Initiative]
- 3. [IT Initiative]
- 4. [IT Initiative]
- 5. [IT Initiative]
- 6. [IT Initiative]

STATE OF INFO
TECHNOLOGY
Top Five to Se
Describing the

- [Metric] [Target]
- [Metric] [Target]
- [Metric] [Target]
- [Metric] [Target]
- [Metric] [Target]
- [Metric] [Target]
- [Metric] [Target]

Top Five to Seven Underlying Beliefs and Assumptions

- 1. [Assumption]
- 2. [Assumption]
- 3. [Assumption]
- 4. [Assumption]
- 5. [Assumption]

Our review pointed to areas where, based on the outcomes of the testing, it appears that the IT team's skillset, available bandwidth, and appetite for change may not be as robust that may help PEACE and the user base. Likewise, where our testing has identified weaknesses in required systems upgrades, patch management, controls maintenance, regulation has not consistently reacted to risk management and changes, those inactions have allowed potential technological weaknesses to negatively affect PEACE's overall data security.

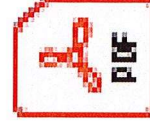
During the interviews, informal discussions, surveys, and other communications, it seems apparent that certain teams have lost faith in the IT Department. But as in almost all of this frustration is bi-directional; the IT group is stretched thin and as additional demands are being made, and it has led to some friction. There should be a re-establishment of good will in the future. We would suggest performing bi-annual satisfaction surveys with the entire workforce (including IT) who are used to drive inclusionary changes and are used to poll the user community for future requests that can be integrated into the strategic planning process and as part of the needed Business Impact Analysis (BIA), which

The PEACE user base has requirements that they have articulated as 'more than just sustained IT support'. They have needs that would leverage different technologies to increase and internally amongst themselves. This type of objective would be very difficult to accomplish if operations, engineering, others, and IT do not all share the same strategic

The PEACE Senior Management Group, as part of its ongoing governance actions, should build an IT Steering Committee (SC) that meets at least monthly. That SC should have strategic responsibilities to assess all ongoing technology needs, build the strategic plan, assess cybersecurity, and risk management, staffing capabilities, vendor management and should consider adding sub-committees who report to the SC for key areas (i.e., cybersecurity, asset refresh, strategic plan drafting, etc.) to lessen the individual efforts for will be the ongoing monitoring of key project and support of the IT over goals both short and long term. A SC charter should be drafted that meets those expectations.

Strategic Plan Documents

Our suggested templated plans are attached for PEACE's use. An additional strategic plan document has been supplied in a separate report.



IT_Strategy_on_a_P
age.pdf



Strategic-Plan-Tem
plate (1).doc.pdf

Key Operational Findings and Recommendations

The following are being communicated as areas where key enhancements in operational controls are required for an effective use of resources, cybersecurity risk program, or allow the controls in place to expose PEACE to potential controllable risks. Management should understand that the following are listed as areas that will require attention a risk areas need to be assessed and remediated as a first priority as they are likely exposing PEACE to unnecessary cyber, regulatory, and other possible data loss risks. The controls that will help minimize the threat to confidential and sensitive data integrity loss, breaches in confidentiality, or unexpected lack of availability at PEACE or its vendor or ineffective controls introduces additional potentials for unknown new or significantly increases existing risks surrounding data loss and the resulting operational, compliance risks.

Laws, Regulations, and Standards

Per inquiry with PEACE, it was communicated that data controlled by laws, regulations, contracts, and standards is stored, processed, or transmitted by the Agency. This various laws, regulations, and standards including HIPAA, the NY State SHIELD Act, and PCI DSS. Through our testing, and per inquiries with PEACE and review of documents may not be fully compliant with those rules. It should be noted that while the Agency has a limited set of established procedures in place with regard to HIPAA, the Agency are detailed in the rest of this report.

Recommendation

PEACE should review accompanying information regarding testing performed by FoxPointe consultants related to HIPAA compliance. Please refer to the tables HIPAA and NY SHIELD Act deficiencies. Additionally, PEACE needs to ensure that upon finalizing its Vendor Management Program documentation, third-party in accordance with HIPAA and the NY SHIELD Act.

Shadow IT and Separation of Duties

Per inquiry with PEACE, it was determined that the IT Department is not involved in the management or administration of PEACE's program management application, myl removed, and changed without IT Department oversight. Additionally, authentication and audit requirements for the system are not known or controlled centrally by the during this risk assessment, a user review was initiated from which 91 user accounts were determined to still be active for previously terminated employees within myHead.

Recommendation

In order to enhance information security and access control management of the myHeadStart system, PEACE needs to put mechanisms in place to ensure that access managed centrally by the IT Department. All access requests (i.e., new, change, removal, etc.) need to be documented and retained centrally. Additionally, PEACE require access to the system are audited to ensure that active access is authorized and follows the principle of least privilege. Procedures and policies that require all program areas at PEACE and the IT Department need to be developed and implemented.

Reporting and Organizational Structure

Per inquiry with PEACE and review of supplied documentation, it was determined that the IT Department reports up through the Human Resources Department. Addition of knowledge and skills in the area of information technology management, the Human Resources Department cannot provide the expected level of oversight of the IT Department of implementing the current reporting line was to build a culture of communication and coordination between the IT Department and the rest of the Agency.

Recommendation

The reporting line between the IT Department and the Human Resources Department should be assessed from an information security perspective. The IT Director's and information security collaboration in order to ensure sufficient oversight of information technology activities and security initiatives.

PCI DSS Requirements

PEACE accepts card payments through Pay Pal, and the Agency does not complete an annual Self-Assessment Questionnaire (SAQ). Additionally, it was communicated that systems, and a PCI DSS gap assessment has not been performed by PEACE.

Recommendation

We would suggest that a PCI DSS gap assessment be completed to confirm that all processing and transactions involving card data are handled in compliance with should plan to complete, at a minimum, a SAQ A for its PayPal transactions. It is further recommended that when accepting card payments at outside events, PEACE being sent over public WIFI.

Organization-Wide Information Security Consciousness

As a result of interviews with staff members including Program personnel and Senior Management, it was determined that while some PEACE personnel maintain a height on an individual level, consistently followed information security protocols (i.e., secure email use, software downloads, information storage, etc.) are not practiced through

Recommendation

The Agency should continue its efforts to develop and maintain a culture of heightened information security awareness through an updated information security PEACE should ensure that Senior Management is included in the information security awareness training program to support the "Tone at The Top" mentality. D should be an active part of the "C" suite roles and responsibilities for key governance requirements across the entire organization.

Internet Connectivity

Throughout the interview process, it was widely communicated that internet connectivity and performance are an issue at PEACE sites. PEACE personnel have expressed with consistent audio and video, and in many cases, calls will disconnect or "drop". In order to address these issues, PEACE has limited and, in some cases, restricted the all personal devices. Additionally, it was communicated that another potential solution being evaluated by PEACE is restricting clients from accessing guest internet at sites, in

Recommendation

PEACE should ensure that staff are able to access the resources they need in order to perform their day-to-day roles and responsibilities effectively and efficiently, the need to utilize personal devices to perform such duties. In order to avoid staff relying on Agency resources for personal use, guest network access should be granted to guest activity (particularly employee activity) should require registration. Additional funding should be considered for a separate Spectrum line dedicated to guest activity therein providing both employees and clients access to the internet for personal use. In doing that, employees should be trained to refrain from using any business resources.

IT Asset Ownership

It was communicated that IT purchases for less than \$5,000.00 are expensed and maintained by the IT Department. IT is therefore responsible for maintaining and inventorying the \$5,000 limit and is required to take a physical inventory of all devices annually. The Finance Department abdicates its responsibility as steward over these resources to the IT Department.

Recommendation

Proper separation of duties requires the Finance Department to be involved in the IT asset inventory control process. Inventory lists should reconcile back to accounting reconciliations at least quarterly to limit the possibility of misplaced, lost, or stolen assets.