



Town of Belleair

901 Ponce de Leon Blvd.
Belleair, FL 33756

Meeting Agenda Finance Board

Thursday, August 17, 2017

4:00 PM

Town Hall

Welcome. We are glad to have you join us. If you wish to speak, please wait to be recognized, then step to the podium and state your name and address. We also ask that you please turn-off all cell phones.

ROLL CALL

CITIZENS COMMENTS

(Discussion of items not on the agenda. Each speaker will be allowed 3 minutes to speak.)

APPROVAL OF MINUTES

[17-0173](#) Approval of July 20, 2017 Meeting Minutes

Attachments: [Minutes-July 20, 2017](#)

GENERAL AGENDA

[17-0136](#) Discussion of cybersecurity framework published by AICPA

Attachments: [Cyber Security Framework06092017](#)
[draft cyber security notes](#)

[17-0181](#) Discussion of 2017-2018 Annual Budget

Attachments: [FB0817Budget.pdf](#)

OTHER BUSINESS

STAFF REPORT

COMMISSION ADVISOR REPORT

ADJOURNMENT

ANY PERSON WITH A DISABILITY REQUIRING REASONABLE ACCOMMODATIONS IN ORDER TO PARTICIPATE IN THIS MEETING, SHOULD CALL (727) 588-3769 OR FAX A WRITTEN REQUEST TO (727) 588-3767.



Legislation Details (With Text)

File #: 17-0173 **Version:** 1 **Name:**

Type: Minutes **Status:** Minutes Approval

File created: 8/3/2017 **In control:** Finance Board

On agenda: 8/17/2017 **Final action:**

Title: Approval of July 20, 2017 Meeting Minutes

Sponsors:

Indexes:

Code sections:

Attachments: [Minutes-July 20, 2017](#)

Date	Ver.	Action By	Action	Result
------	------	-----------	--------	--------



Town of Belleair

901 Ponce de Leon Blvd.
Belleair, FL 33756

Meeting Minutes Finance Board

Thursday, July 20, 2017

4:00 PM

Town Hall

Welcome. We are glad to have you join us. If you wish to speak, please wait to be recognized, then step to the podium and state your name and address. We also ask that you please turn-off all cell phones.

Meeting called to order at 4:00 PM with Chairman Olson presiding.

ROLL CALL

Present 6 - Chairman Tom Olson, Vice Chairman Dan Hartshorne, Ernest Whittle, John Prevas, Kevin Piccarreto, and John Hail
Absent 1 - Mary Griffith

Elected Officials Present: Mayor Gary Katica, Deputy Mayor Karla Rettstatt, Commissioner Tom Shelly.

Staff Members Present: JP Murphy, Ashley Bernal, Keith Bodeker, Cathy DeKarz, Doug Speta

CITIZENS COMMENTS

No comments to be heard.

APPROVAL OF MINUTES

[17-0140](#) Approval of June 15, 2017 Meeting Minutes

Mr. Whittel moved approval; seconded by Mr. Prevas.

Aye: 6 - Chairman Olson, Vice Chairman Hartshorne, Whittle, Prevas, Piccarreto, and Hail

Absent: 1 - Griffith

GENERAL AGENDA

[17-0142](#) Election of Officers

Mr. Prevas moved to nominate Tom Olson for Chairman; seconded by Mr. Whittle.

Aye: 6 - Chairman Olson, Vice Chairman Hartshorne, Whittle, Prevas, Piccarreto, and Hail

Absent: 1 - Griffith

Mr. Prevas nominated Dan Hartshorne as Vice Chairman; seconded by Mr. Whittle.

Aye: 6 - Chairman Olson, Vice Chairman Hartshorne, Whittle, Prevas, Piccarreto, and Hail

Absent: 1 - Griffith

[17-0169](#)

Presentation by ABM regarding energy, mechanical and capital savings program.
(Energy Performance Contracting)

JP Murphy-Town Manager-Staff evaluating energy savings and looking for efficiencies; value in looking into prior to beginning budget year for potential savings.

Rob Duncan-ABM Solutions-Presentation identified national trends relating to small cities; company specializes in cost savings related to facility operation and maintenance; photos of areas where upgrades would be beneficial were presented.

Mr. Prevas questioned current staff resources; Mr Murphy stated there are no dedicated building facilities staff.

Mr. Duncan addressed questions regarding continued savings over the years; guaranteed savings required by state statute; will assist with RFP process for financing.

Discussions ensued regarding financing; 15 year contract; options to take on project without financing; contacting other cities in contract with ABM; value of having a single vendor to eliminate delays.

Dan Kline-Vice President and General Manager of ABM operations in central Florida-Provided information on company; primarily a service company; engineer, install and manage projects. Addressed questions from the board related to assistance after installation and other clients.

Discussions ensued regarding savings guarantee; new technologies; guarantee protection of funding source; minimal staff impact as most is outsourced currently; length of contract and savings as well as knowing contingencies.

Mr. Murphy commented on measurement and verification period; Mr. Duncan provided comments regarding continued reporting and evaluation.

Recommendation to the Commission to proceed with the contract with AMB.

Mr. Prevas moved to recommend; seconded by Mr. Whittle.

Aye: 6 - Chairman Olson, Vice Chairman Hartshorne, Whittle, Prevas, Piccarreto, and Hail

Absent: 1 - Griffith

17-0168

Discussion of 2017-2018 Fiscal year budget

Mr. Murphy introduced Doug Speta-Assistant Finance Director; Mr. Speta spoke briefly to the board. Cathy DeKarz-Management Analyst and Ashley Bernal were also introduced to the board.

Mr. Murphy discussed past practice of interfund transfers; one time dollars to be spent on one time expenses; golf course revenue funds go away; proposes not spending sale proceeds until after November election.

Discussion ensued regarding upcoming election; ability to do longer term forecasting afterwards; plan two expenditures are set as projected.

Mr. Murphy addressed questions regarding potential uses of funds from golf course; commented further on fund transfers and single one time purchases.

Mr. Murphy provided summary of revenues and related increases; discussed expenditures and capital equipment replacements; commented on salaries and shift differential relating to fully staffed police department; addressed questions related to building permitting and inspections;

Mr. Olson requested an organizational chart for the next meeting to identify departments and responsibilities; commented on budget control regarding departmental changes.

Comments made regarding police being fully staffed; FOP is union and contracts are three years; future increases should be minor.

Mr. Piccarreto left the meeting at 5:37 PM

Mr. Murphy continued summary of budget; highlighted key points in each department in the general fund; stated next step is for Commission to set MMP; available for questions.

OTHER BUSINESS

No other business.

COMMISSION ADVISOR REPORT

Mayor Katica commented on ABM presentation and guarantee.

Board comments were made regarding guarantee and potential contingencies; Mr. Murphy will provided contract from Temple Terrace for reveiw.

ADJOURNMENT

No further business; meeting adjourned in due form at 5:55 PM.

APPROVED:

Chairman



Legislation Details (With Text)

File #: 17-0136 **Version:** 1 **Name:**
Type: Discussion Items **Status:** Agenda Ready
File created: 6/13/2017 **In control:** Finance Board
On agenda: 8/17/2017 **Final action:**
Title: Discussion of cybersecurity framework published by AICPA
Sponsors:
Indexes:
Code sections:
Attachments: [Cyber Security Framework06092017](#)
[draft cyber security notes](#)

Date	Ver.	Action By	Action	Result
------	------	-----------	--------	--------

Summary

To: Finance Board
From: Stefan Massol, Director of Support Services
Date: 8/17/2017

Subject:

Discussion of Cybersecurity Framework published by AICPA

Summary:

Staff is developing a cybersecurity framework and risk assessment tool using guidance published by the Association of International Certified Professional Accountants (AICPA).

Previous Board Action: None.

Background/Problem Discussion: Provided is a draft overview of the topics that have been identified for the cybersecurity framework and risk assessment tool. Staff is requesting any additional areas of emphasis that the board believes should be included in the final version. The final version will include the overall framework as well as a risk assessment questionnaire, which collectively will be used by town staff to complete a cybersecurity risk management report. Relevant computer use policies will also be included in the cybersecurity risk management report, as well as statistical information pertaining to the technological resources and needs of the town.

Expenditure Challenges: None.

Financial Implications: None.

Recommendation: None, this item is for discussion purposes only.

Proposed Motion: None, this item is for discussion purposes only.



Association
of International
Certified Professional
Accountants®

Illustrative cybersecurity risk management report

Note to readers:

Although the AICPA Guide Reporting on an Entity's Cybersecurity Risk Management Program and Controls describes the components of a cybersecurity risk management report and the information to be included therein, it does not mandate specific formats for most of the information to be presented. Entity management and the practitioner may organize and present the required information in a variety of formats.

The format of the illustrative cybersecurity risk management report presented in this nonauthoritative document is included for illustrative purposes only. The illustrative cybersecurity risk management report contains all the required components of such a report, including (a) management's assertion, (b) the accountant's report, and (c) the description of the entity's cybersecurity risk management program.

CONTENTS

Section 1—Assertion of the Management of XYZ Manufacturing

Section 2—Independent Accountant's Report

Section 3—XYZ Manufacturing's Description of Its Cybersecurity Risk Management Program

Section 1—Assertion of the Management of XYZ Manufacturing

Introduction

We have prepared the attached XYZ Manufacturing's Description of its Cybersecurity Risk Management Program throughout the period January 1, 20X1, to December 31, 20X1, (description) based on the criteria for a description of an entity's cybersecurity risk management program identified in the AICPA *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* (description criteria). An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented. We have established XYZ Manufacturing's cybersecurity objectives, which are presented on page XX of the description. We have also identified the risks that would prevent those objectives from being achieved and have designed, implemented, and operated controls to address those risks.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in an entity's cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Assertion

We assert that the description throughout the period January 1, 20X1, to December 31, 20X1, is presented in accordance with the description criteria. We have performed an evaluation of the effectiveness of the controls included within the cybersecurity risk management program throughout the period January 1, 20X1, to December 31, 20X1, using the criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) (control criteria). Based on this evaluation, we assert that the controls were effective throughout the period January 1, 20X1, to December 31, 20X1, to achieve the entity's cybersecurity objectives based on the control criteria.

Section 2—Independent Accountant 's Report

To Management of XYZ Manufacturing:

Scope

We have examined the accompanying XYZ Manufacturing's Description of its Cybersecurity Risk Management Program throughout the period January 1, 20X1, to December 31, 20X1, (description) based on the description criteria noted below. We have also examined the effectiveness of the controls within that program to achieve the entity's cybersecurity objectives based on the control criteria noted below.

The criteria used to prepare the description are the AICPA's *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* (description criteria); the criteria used to evaluate whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives are the criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) (control criteria).

An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that were not prevented.

Entity's Responsibilities

XYZ Manufacturing's management is responsible for the following:

- Establishing the entity's cybersecurity objectives, which are presented on page XX of the description.
- Designing, implementing, and operating the cybersecurity risk management program, including the controls within that program, to achieve the entity's cybersecurity objectives
- Preparing the accompanying description of the entity's cybersecurity risk management program
- Providing an assertion about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether controls within the cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives.

When preparing its assertion titled *Assertion of the Management of XYZ Manufacturing*, management is responsible for (a) selecting, and identifying in its assertion, the description criteria and the control criteria and (b) having a reasonable basis for its assertion about whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives by performing an assessment of the effectiveness of those controls based on the control criteria. The description of the entity's cybersecurity risk management program and management's assertion accompany this report.

Accountant's Responsibilities

Our responsibility is to express an opinion, based on our examination, about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls within the program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

Our examination included

- obtaining an understanding of the entity's cybersecurity objectives and its cybersecurity risk management program;
- assessing the risks that the description was not presented in accordance with the description criteria and that the controls within that program were not effective; and
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria and whether the controls were effective.

Our examination also included performing such other procedures as we considered necessary in the circumstances. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in a cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects,

- the description of XYZ Manufacturing's cybersecurity risk management program throughout the period January 1, 20X1, to December 31, 20X1, is presented in accordance with the description criteria and
- the controls within that program were effective throughout the period January 1, 20X1, to December 31, 20X1, to achieve the entity's cybersecurity objectives based on the control criteria.

Baker, Jones, and Eagle, CPAs
Athens, Georgia March 1, 20X2

Section 3—XYZ Manufacturing's Description of its Cybersecurity Risk Management Program

Note to readers: *The following illustrative description of an entity's cybersecurity risk management program, which is based on the operations of a hypothetical company, illustrates how a company might prepare and present a description of its cybersecurity risk management program in accordance with the description criteria. The description criteria have been included within the presentation for illustrative purposes.*

Nature of Business and Operations

DC1: The nature of the entity's business and operations, including the principal products or services the entity sells or provides and the methods by which they are distributed

XYZ Manufacturing (XYZ or the Company) is a leading manufacturer, distributor, and retailer of reproduction consumer products and objects from various historical periods, with an emphasis on classical Greece, ancient Rome, and medieval Europe. The Company's products allow consumers to emulate a non-contemporary lifestyle in one or more facets of their lives. Merchandise is provided across a broad range of categories including kitchen and dining, furniture, bedding and bath, lighting solutions, and arts, crafts, and sewing. The Company operates through three key segments: manufacturing (30 percent of revenue), online retail (40 percent of revenue), and wholesale (30 percent of revenue). XYZ's online retail and wholesale operations offer products manufactured by the Company and sourced under contract from other manufacturers. Online retail also offers products sourced from other wholesalers.

The Company serves its primary markets of North America and Europe from its headquarters in Athens, Georgia, and Rome, Italy, respectively, and has major operating facilities throughout the U.S. and Europe. Manufacturing is located in Shanghai, China. In 2015, the Company entered into a joint venture with UVW Trading of Hong Kong to expand into Asian markets, where the Company's products hold strong appeal from a novelty perspective. Distribution is provided by commercial carriers.

Nature of Information at Risk

DC2: The principal types of sensitive information created, collected, transmitted, used, or stored by the entity

The Company creates, obtains, distributes, uses, and stores a wide variety of information in its operations. In addition to information common to the operation of entities similar to XYZ, such as regulatory compliance information and personnel records, the Company uses the following information:

- Financial information, which is used for both internal and external reporting purposes. Internal financial information and external financial information, prior to publication, is considered confidential and is treated as insider information.
- Confidential sales information, including customer lists, confidential wholesale pricing information, and order information
- Payment card information used in online retail and wholesale transactions, including cardholder names and card numbers. This information may be retained for customer convenience on XYZ systems for ease of ordering
- Online retail customer profile information used to provide customers with a personalized lifestyle experience
- Confidential product information including product specifications, new design ideas, and branding strategies

- Proprietary information provided by business partners, including manufacturing data, sales and pricing information, and licensed designs
- Confidential employee information

Cybersecurity Risk Management Program Objectives (Cybersecurity Objectives)

DC3: The entity's principal cybersecurity risk management program objectives (cybersecurity objectives) related to availability, confidentiality, integrity of data, and integrity of processing

Under the direction of the XYZ board of directors, management establishes the objectives of the Company. Based on these objectives, management also establishes specific objectives for its cybersecurity risk management program. Because substantially all Company operations involve the use of IT, the Company makes no distinction between information security and cybersecurity.

XYZ Manufacturing's cybersecurity objectives are the following:

Availability

Enabling timely, reliable, and continuous access to and use of information and systems to support operations and to

- provide
 - online retail store availability 24-hours a day year-round
 - customer experiences related to system response and dropped transactions meeting benchmarks established by management
 - manufacturing system availability during scheduled shifts
 - timely information from the enterprise resource planning (ERP) system to suppliers and management to support decision making
 - wholesale online, field sales support, and customer service center systems availability as committed
 - accurate product availability and delivery information
- support the delivery of products to customers as committed
- comply with applicable laws and regulations
- safeguard assets

Confidentiality

Protecting information from unauthorized access and disclosure, including means for protecting proprietary information and personal information subject to privacy requirements, to safeguard

- employee and customer information, including credit card information, in accordance with laws, regulations, and card brand requirements
- confidential corporate data related to sales and financial reporting
- confidential business transactions related to the information of business partners and others
- the intellectual property of the Company, its business partners, and others

Integrity of Data

Guarding against improper capture, modification or destruction of information to support

- the preparation of reliable
 - financial and nonfinancial information for external reporting purposes
 - information for internal use
- nonrepudiation and authenticity of transactions from online systems
- the completeness, accuracy, and timeliness of manufacturing, delivery of goods, and information processing

- management, in holding employees, vendor and business partner employees, and customers accountable for their actions
- the storage, processing, and disclosure of information, including personal and third-party information

Integrity of Processing

Guarding against improper use, modification, or destruction of systems in order to support

- the accuracy, completeness, and reliability of product delivery and transaction processing
- the manufacture of goods to product specifications
- the efficient operation of production
- the safeguarding of the life and health of employees in production facilities

Guarding against the improper use or misuse of processing capabilities that that could be used to impair the security or operations of external parties

DC4: The process for establishing, maintaining, and approving cybersecurity objectives to support the achievement of the entity's objectives

The Company's board of directors, with the support of management and outside resources engaged by the board, reviews and updates its formal business strategy annually. Based on that strategy, management and the board annually establish or update the Company's overall business objectives, including objectives over operations, compliance, and reporting. At the completion of this process, the overall objectives are approved.

Upon approval of the Company's business strategy and overall objectives, management uses a top-down approach to establish or update specific business objectives for business units and functions, including information technology, within the organization. This process includes budgeting resources and establishing metrics for the achievement of the objectives. At the completion of this process, the specific business objectives and the budget is submitted to the board for approval.

As part of the development of specific business objectives, the chief information security officer (CISO) updates the Company's cybersecurity objectives with the objectives of the business units and other functional areas. These cybersecurity objectives are then approved by the Company's executive management, including the CEO, COO, CFO, chief risk officer (CRO), general counsel (GC), and the CIO.

The Company's cybersecurity risk management program is based on specifications set forth in the National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity" (NIST cybersecurity framework) and International Standardization Organization and International Electrotechnical Commission (ISO/IEC) standards. The Company's portfolio of security controls is based on ISO/IEC controls and, for systems containing cardholder information, the Payment Card Industry Data Security Standards.

Factors that have a Significant Effect on Inherent Cybersecurity Risks

DC5: Factors that have a significant effect on the entity's inherent cybersecurity risks, including the (1) characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity; (2) organizational and user characteristics; and (3) environmental, technological, organizational and other changes during the period covered by the description at the entity and its environment

Technologies, connection types, service providers, and delivery channels. The Company uses the following technologies, connection types, service providers, and delivery channels:

- An integrated ERP system is used to manage manufacturing, wholesale, and retail operations. The ERP system is interfaced with the manufacturing, wholesale, and online retail systems to provide an integrated IT environment.
- Online retail operations are supported by a software-as-a-service (SaaS) cloud provider. The integrated solution provided permits the Company to design and maintain its retail site in an effective and efficient manner. Online wholesale operations are supported through a third-party system that interfaces with the ERP system. The system is hosted on a network of virtual servers hosted in XYZ's primary data center.
- Wholesale call center services are outsourced with the call center's systems interfaced with the ERP system to facilitate ordering and problem resolution. The interface with the call center is over a virtual network connection. Custom-developed software is used to interface the call center system to the ERP interface.
- Field sales automation is provided through the use of company-owned tablet devices running third-party software customized for the Company. Tablets access the ERP system through a virtual private network (VPN) system.
- Manufacturing is controlled through a network of midrange systems running widely used manufacturing system software. This software is modified and maintained by Company IT personnel.
- All connectivity to external users occurs through defined access points managed by routers.
- Routers are also used to segment the network within the Company.
- Transmissions to vendors and other third parties are sent through defined channels.

Organizational and user characteristics. The Company's IT function is headed by a chief information officer (CIO) and is divided into application services, technology services, and information security. The Company uses a centralized organizational model to support company applications and technology. The online retail and call center vendor relationships are managed by designated personnel in technology services reporting to the chief technology officer (CTO). The information security group is headed by the CISO and consists of security architecture and technical support, application security, and security operations center personnel. Security operations center personnel are primarily responsible for user administration, second-level security support, security event monitoring, and security incident response and management.

Users of the system primarily consist of the following:

- Consumers whose access is restricted to the online retail system provided by the vendor.
- Wholesale customers whose employees have access to catalog information, order status, order functionality, and account functionality through the internet module of the wholesale system. Customer personnel are assigned user IDs via a master customer account that is also used to administer the accounts. Customer personnel accounts are assigned defined roles established by the Company.
- UVW personnel whose access is similar to wholesale customer access.
- Call center service organization personnel, who access the wholesale system through assigned user accounts that are restricted to a defined call center role.
- All XYZ employees, who are assigned unique user IDs that grant them default company access and email access, with the exception of manufacturing line personnel in Shanghai who are not granted access.

- Product vendors, who are granted limited access to the ERP system to pick up purchase orders and inquire about the status of invoices. This access is provided through a module of the ERP system through a vendor account and password.

Although IT assets are located in all countries of operation, the Company does not deem any countries to be of higher risk than others.

Environmental, technological, organizational, and other changes during the period. In December of 20XX, the Company added manufacturing operations in Shanghai, China, through the acquisition of an established brass foundry. At the time of acquisition, the foundry ran its business operations using off-the-shelf software on a local area network. The Company completed migration of all foundry data processes to the ERP system in March of the current year.

The Company is in the process of finishing its new manufacturing facility and upgrading manufacturing and foundry equipment as part of a modernization program. As part of this program, it is modernizing foundry floor equipment, replacing existing manual equipment with new equipment that uses leading industrial control systems. These systems will be integrated with the ERP system to enhance production operations and reporting. The new facility is expected to be operational by November. The process for adding new system components related to this change is subject to the cybersecurity risk management program and controls over those components are implemented as part of the change management process.

DC6: For security incidents that (1) were identified during the 12-month period preceding the period end date of management's description and (2) resulted in a significant impairment of the entity's achievement of its cybersecurity objectives, disclosure of the following: (a) nature of the incident; (b) timing surrounding the incident; and (c) extent (or effect) of these incidents and their disposition

XYZ utilizes a number of both manual and automated security monitoring capabilities to identify security events that occur in the environment. During the period under assessment, the Company experienced an incident that resulted in a compromise of sensitive data from a SQL injection attack on a web application. The attack was detected approximately 66 hours after the event and was remediated within 5 days of detection. XYZ Manufacturing incurred costs related to the notification of and credit monitoring for affected parties (commercial customer information and personally identifiable information of retail customers), as well as fees associated with the retention of outside cybersecurity expertise to conduct forensic investigation of the affected systems and, later, an independent evaluation of security measures to ensure that remediation actions were sufficient to address the identified threats. The incident was fully resolved and remediated, and XYZ has made the necessary adjustments to its systems and processes, as well as to the affected service provider systems and processes, to reduce the likelihood that similar incidents could reoccur.

Cybersecurity Risk Governance Structure

DC7: The process for establishing, maintaining, and communicating integrity and ethical values to support the functioning of the cybersecurity risk management program

Management sets the organizational tone through policies, a code of ethics, a commitment to hiring competent employees, and the development of reward structures that promote an effective internal control and governance structure. The board of directors meets quarterly with members of executive management to review financial and operational performance, including the entity's cybersecurity risk management program.

Employees are required to sign the employee handbook upon hire, acknowledging their acceptance and adherence to the Company's policies and code of conduct. Such policies and the code of conduct have been designed to promote integrity and ethical values throughout the workplace. The information security policy includes information about the following:

- Information privacy, confidentiality, and acceptable use
- Electronic communications
- Data management
- Disclosure

DC8: The process for board oversight of the entity's cybersecurity risk management program

The XYZ board of directors includes various outside directors with industry knowledge and experience including one board member who is a former IT director of an S&P 100 company with 15 plus years of experience in IT and cybersecurity and serves as the board's subject matter expert on cybersecurity matters. Additionally, the XYZ CISO joins the quarterly board meeting to present an overview of the Company's cybersecurity risk management program, including activities of the entity's risk governance committee. Feedback and action items are provided by the board, which is actively engaged in overseeing this key business risk.

The risk governance committee was established to coordinate the risk assessment and management efforts of the entity and its units. The committee, which is chaired by the CRO and consists of the CISO, CCO, external specialists, and IT and business line personnel, ensures that (a) cybersecurity risks arising from both internal and external sources are identified and evaluated, (b) controls are properly designed and implemented to address all areas as appropriate, and (c) controls operate effectively to achieve the entity's cybersecurity objectives. Areas evaluated include systems development, computer operations, program changes, and access to programs and data.

As part of the CISO's quarterly presentations, the results of the XYZ information security team's program assessments are presented and discussed, as well as any corrective action needed as a result of the assessments. The presentations also include summaries of the Company's vendor and business partner oversight program. Under the program, Company personnel perform an annual review of vendor and business partner relationships to evaluate whether the Company is in compliance with industry standards and best practices.

DC9: Established cybersecurity accountability and reporting lines

Under the direction of the risk governance committee, the CISO is responsible for overseeing the cybersecurity risk management program and executing the entity's strategy and other decisions agreed upon by executive management and the board of directors. The CISO reports administratively to the CIO, with an escalation point to the CEO. The CISO presents a quarterly cybersecurity update to the board of directors to report on the state of the entity's cybersecurity risk management program.

The CISO also chairs the information security committee. The information security team, which consists of representatives from all departments in XYZ, is a centralized team of cybersecurity practitioners, subject matter experts, and IT personnel who support the information security operations of the organization (such as systems administrators, software engineers, network engineers, and security analysts). The duties, responsibilities, and hierarchy of employees on the information security team are defined in a role matrix and form the foundation of the entity's cybersecurity risk management program. The information security committee defines and approves the strategy, policies, and standards underlying the entity's cybersecurity risk management program. The results of the annual risk assessment, periodic internal audits, and quarterly external independent assessments are provided to the CISO and the information security committee throughout the year in order to continuously adapt the program to align with new and emerging threats and potential vulnerabilities. The activities of the information security committee are overseen by the risk governance committee.

Alongside the CISO is the CTO, who also reports administratively to the CIO but with an escalation point to the CEO. The CTO is responsible for managing the technology and resources that support the internal operations of the company. This includes overseeing policy and processes regarding relationships with vendors and business partners that may contribute to the cybersecurity risk management program. These

policies and processes are administered through the vendor and business partner oversight program discussed in a later section.

DC10: The process used to hire and develop competent individuals and contractors and to hold those individuals accountable for their cybersecurity responsibilities

Applicants with a role in the cybersecurity risk management program are hired based on their ability to satisfy the job duties and responsibilities of the position and fulfill the goals and expectations of the entity. They are evaluated on their level of education, the merits of their past experience, a positive performance history, and knowledge of relevant cybersecurity controls and processes. Before employment, all applicants must also pass a thorough background check.

Upon hiring, employees are required to sign the employee handbook, acknowledging their acceptance and adherence to the Company's policies and any associated confidentiality and nondisclosure agreements.

Upon hiring and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective cybersecurity risk management program. Employees with job responsibilities that fall directly within the cybersecurity risk management program (such as IT personnel, IT management, and internal auditors) have minimum training and continuing education requirements each year.

Employees in the cybersecurity risk management program are encouraged to maintain an active role in relevant cybersecurity information sharing forums, special interest groups, and professional associations to stay up to date on new and emerging cybersecurity risks that may impact the entity or its operating environment.

Contractors are required to follow the same onboarding process as employees and are subject to the same background checks and security awareness training requirements as employees. Employees' and contractors' compliance with security awareness training requirements is monitored on a semiannual basis by human resources.

XYZ has established an entity-wide hierarchy and reporting structure that is codified within an organizational chart maintained on the corporate intranet by human resources. XYZ has prepared a role matrix for employees and managers who have roles within the cybersecurity risk management program. The role matrix defines key job duties and responsibilities in the context of the overall program. Additional information security responsibilities and practices for certain roles within the entity are described in the Company's information security policy and the employee handbook.

All employees go through an annual performance review cycle. At the beginning of each calendar year, employees and their immediate supervisors establish goals and expectations for their job performance over the upcoming year based on the job duties and responsibilities described in the role matrix.

Employees then receive a mid-year and year-end performance review from their supervisors that assesses the employees' performance against the agreed-upon goals and expectations. Based on the results of their performance review, employees receive merit increases in compensation and are eligible for bonuses and promotion, respective of their seniority, experience, and position within the organization. Employees whose performance is not in alignment with established goals and expectations for job performance, or who are not fulfilling their job responsibilities, may be referred to human resources by their supervisor to develop a performance enhancement plan.

If an employee violates any statute of the employee handbook or the Company's policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the Company, whether purposefully or not, the employee is subject to sanctions up to and including termination of employment.

Cybersecurity Risk Assessment Process

DC11: The process for (1) identifying cybersecurity risks and environmental, technological, organizational and other changes that could have a significant effect on the entity's cybersecurity risk management program and (2) assessing the related risks to the achievement of the entity's cybersecurity objectives

XYZ maintains a detailed inventory of all information systems, including manufacturing and industrial control systems. All such assets are assigned ownership by a designated department or team within the entity and prioritized based on the asset's business value and criticality to the organization. Information

and data assets are subject to the data management policy that defines parameters for the ownership, classification, security, storage, and retention of data. Software and hardware assets are subject to the information systems management policy that defines parameters for the acquisition, development, maintenance, security and disposal of information system assets.

On an annual basis, the information security team performs a risk assessment that identifies internal and external cyber threats and vulnerabilities to the organization. Information system assets are analyzed to identify associated threats to those assets and vulnerabilities that may be exploited. The resulting risks are then scored based on their likelihood and potential impact to the organization. The assessment includes consideration of the inherent and residual risks that may reside with external parties and the cybersecurity controls to address those risks. Specific policies and procedures are in place to assess and manage the requisition and engagement of vendors or business partners with consideration for the cyber threats and vulnerabilities such relationships may present.

Results of the risk assessment are evaluated by relevant management against criteria for risk acceptance to identify new or existing protective measures and develop or enhance information security policies and procedures.

Internal audit conducts periodic cybersecurity assessments that include working with process owners and IT support personnel to identify specific security threats and vulnerabilities and to identify how the associated risks are being addressed. Additionally, quarterly vulnerability assessments and penetration tests are performed by an external party to identify specific technical threats and vulnerabilities.

DC12: The process for identifying, assessing, and managing the risks associated with vendors and business partners

XYZ considers the inherent risk of working with vendors and business partners as part of the annual risk assessment performed by the information security team. Internal and external cyber threats and vulnerabilities are identified and assessed based on the likelihood that they could prevent the entity from achieving its cybersecurity objectives. Specific policies and procedures are in place to assess and manage the requisition and engagement of vendors. Consideration is given to the cyber threats and vulnerabilities such relationships may present and whether XYZ's controls reduce such risks to a level consistent with XYZ's cybersecurity objectives and risk acceptance.

XYZ has established a tiering system in which each vendor is assigned a tier (1–3) based upon the inherent risk of the goods and services the vendor provides, the overall operational significance of the vendor to achieving XYZ's business objectives, and the sensitivity of data that resides within the vendor's environment. Business partners are evaluated using the same tiering structure, based on the cybersecurity risk associated with each business partner.

The entity's vendor and business partner oversight program requires that all contracts with vendors or business partners clearly address (a) the size, scope, and nature of services being provided; (b) the hardware, software, and information requirements related to the provision of such services; (c) the responsibilities of each party; (d) the requirements for information security to meet XYZ's standards; (e)

the ability to perform independent audits of the effectiveness of internal control processes; and (f) the requirement to obtain and review a third-party attestation report.

Disclosure of any confidential or personally identifiable information (PII) to a vendor or business partner is provided only on an as-needed basis and only if the vendor or business partner has enacted appropriate information security and privacy controls. All vendors and business partners with access to confidential information are subject to confidentiality and privacy agreements and other contractual confidentiality provisions, which must be signed and acknowledged before access to XYZ's systems and data is granted.

The vendor and business partner oversight team ensures that XYZ and its vendors and business partners stay current with existing contractual obligations, information security and privacy regulations, certification compliance requirements, and industry standards. The vendor and business partner oversight team performs an ongoing annual review of vendor and business partner relationships to (a) reevaluate the services provided and any cybersecurity threats and vulnerabilities arising from the relationship; (b) consider whether the assessed risks are being addressed appropriately by each party's contractual agreements, information security controls and processes; and (c) evaluate whether the entity's vendor and business partner oversight program complies with industry standards and best practices. The review process includes obtaining security questionnaires, conducting personnel interviews, performing walkthroughs, performing site visits, and conducting IT scanning and testing. In addition, when available, the review process may also include obtaining and reviewing third-party attestation reports.

The CISO and the information security team participate in cybersecurity information sharing forums, special interest groups, and professional associations to increase information sharing between knowledgeable parties and to stay up to date on changes in the regulatory, economic, and physical environment in which the Company operates. As an international manufacturer, XYZ Manufacturing maintains communicative relationships with relevant governing and regulatory bodies to stay abreast of changes to laws and regulations that impact the organization as they arise.

Internally, consideration of the entity's cybersecurity risk management program is an integral part of proposed changes to existing business lines or operations, the development or acquisition of new business lines or operations, decisions about doing business in new geographies or markets, and the adoption of new technologies or processes throughout the business. The information security team, led by the CISO, is involved in the decision-making process related to changes that could impact the size, scope, or operational nature of the business. In this capacity, the team may perform ad hoc, focused risk assessments to identify new risks to the organization and associated impacts to be considered during the decision-making process; the team may also reevaluate the design of controls to ensure continued protection.

Additionally, on an annual basis, the information security team performs a full risk assessment that identifies internal and external cyber threats and vulnerabilities to the organization. During the annual risk assessment, the team considers both internal changes to XYZ operational processes (such as new or modified lines of business, new or modified operating procedures, new geographies or markets, new technologies or services used) and external changes (such as new or changing regulatory requirements, industry standards, economic circumstances, emerging risks) that could affect the entity. New controls are designed in response to identified threats and existing controls are assessed to ensure they reflect changes to the size, scope, and operational nature of the business.

Cybersecurity Communications and Quality of Cybersecurity Information

DC13: The process for internally communicating relevant cybersecurity information necessary to support the functioning of the entity's cybersecurity risk management program, including (1) objectives and responsibilities for cybersecurity and (2) thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both

The internal communication of cybersecurity information for employees according to their role in the cybersecurity risk management program is described in the XYZ information security policy, which is available to all employees on the Company intranet. Additionally, the employee handbook identifies certain information security responsibilities and practices, depending on the employee's role within the organization. At the time of hiring, all employees must provide sign-off, acknowledging acceptance of and adherence to the Company's policies.

Upon hiring, and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective cybersecurity risk management program. The training courses are designed to assist employees in identifying and responding to social engineering attacks (phishing, tailgating) and in avoiding inappropriate security practices (for example, writing down passwords or leaving sensitive material unattended). XYZ periodically assesses employees' awareness of corporate policy by attempting to tailgate into buildings, sending simulated phishing emails, and performing desk sweeps, among other tactics. If an employee is found to be violating Company policies, additional training is provided or other disciplinary actions are taken.

Employees with job responsibilities that fall directly within the cybersecurity risk management program (IT personnel, IT management, internal audit, and the like) have additional requirements to complete technical and job-specific training throughout the year. Additionally, those employees who have direct access to customer and employee data (for example, sales, customer service, human resources, IT helpdesk, and finance) will receive specific training around incident management, information handling, and data protection.

Training and other programs related to employee cybersecurity awareness incorporate materials developed internally by XYZ in collaboration with industry- and cybersecurity-focused vendors or business partners. These vendors or business partners provide expertise and tools to develop, perform, track, and test employees' compliance with cybersecurity-awareness policies and standards. XYZ has established a cybersecurity awareness program (CAP) that periodically distributes reminders of information security practices to all employees and sends internal communications to promote security awareness and to provide the latest security news. CAP is also responsible for (a) monitoring cybersecurity risk associated with vendors and business partners who have access to the entity's system; (b) monitoring forums and news sites for information regarding potential breaches; (c) reviewing vendors' and business partners' cybersecurity examination reports on an annual basis; and (d) maintaining ongoing, direct contact with vendors and business partners to address any issues identified.

On an annual basis, XYZ updates the cybersecurity training program and CAP to incorporate changes in the threat landscape and new tactics being executed by threat actors. XYZ also evaluates lessons learned from any previous incidents and incorporates changes into the programs as necessary.

An incident hotline is available to all employees to report information security events they have been involved in or witnessed (such as phishing attacks, malware, lost or stolen devices, and inappropriate information disclosure). XYZ receives a quarterly attestation from the outsourced call center that all hotline personnel have completed XYZ's CAP and are aware of defined policies related to information protection, data handling, and incident response.

The CISO presents a quarterly update to the board of directors to report on the state of the entity's cybersecurity risk management program. During the update, the CISO presents the status of ongoing efforts to develop and maintain the program in response to (a) prior security events at the organization, (b) changes in XYZ's operational procedures, (c) changes to legal and regulatory requirements affecting the organization, (d) results of audits and testing by internal and external parties, and (e) new and emerging cybersecurity risks to the organization.

DC14: The process for communicating with external parties regarding matters affecting the functioning of the entity's cybersecurity risk management program

XYZ has a disclosure policy defining when, by whom, and to what extent external parties are informed of matters relevant to the functioning of XYZ's cybersecurity risk management program. All disclosures to external parties are made in accordance with applicable laws and regulations at the state and federal level. Any such legal requirements are considered in the development and maintenance of the disclosure policy during annual review. Employees are educated on the policies and procedures for reporting and disclosing cybersecurity incidents or events through the XYZ information security policy and XYZ Employee Handbook.

XYZ may become aware of matters affecting the functioning of the entity's cybersecurity risk management program via its existing monitoring processes, as well as via notification by third parties or law enforcement. When such matters arise, they are immediately reviewed by the XYZ risk governance committee to determine relevance and applicability. Where necessary or appropriate, the matter may be treated as a security incident and handled via XYZ's security incident response process, as described later.

As is typical business practice by most organizations, XYZ restricts communication of matters related to the functioning of XYZ's cybersecurity program to only those stakeholders and business partners who have a need to know such information. This information may be communicated via mediums appropriate to the nature of the information and the urgency of the situation, and may include conference calls, electronic mail, memoranda, or in-person meetings. In the rare instance when public disclosure of such matters would be necessary or appropriate, XYZ's legal counsel and corporate communications representative are responsible for jointly distributing and communicating such disclosure.

Monitoring of the Cybersecurity Risk Management Program

DC15: The process for conducting ongoing and periodic evaluations of the operating effectiveness of key control activities and other components of internal control related to cybersecurity

XYZ uses several mechanisms to assess the ongoing effectiveness of internal controls designed to mitigate cybersecurity risks. Assessment and monitoring of the program are designed to meet the requirements of the NIST cybersecurity framework and ISO 27001.

Internal audit conducts periodic cybersecurity assessments and tests of internal controls that include (a) working with process owners and IT support personnel to identify specific security threats and vulnerabilities and how the associated risk is being addressed and (b) tests of the design, implementation, and operating effectiveness of internal controls that address cybersecurity risks. Members of the internal audit team have the requisite knowledge of and experience with cybersecurity risks and controls.

XYZ also uses external parties to independently evaluate the state of the cybersecurity risk management program. Quarterly vulnerability assessments and annual penetration tests are performed by an external service provider to identify specific technical threats and vulnerabilities and to benchmark the environment against leading cybersecurity practices. In addition, the entity obtains for its SaaS vendor an annual web application security assessment report. Every two years, XYZ engages a service provider to perform an independent assessment of the cybersecurity risk management program to evaluate alignment with leading industry practices and consistency with Company policies in order to identify gaps and potential opportunities for improvement.

Both internal and external evaluations are made using a risk-based approach that may vary the nature, timing, and extent of testing. The criteria for such evaluations, including the nature and frequency of such evaluations, are reviewed during the annual risk assessment and modified as needed, with consideration for changes to XYZ's operational processes, including changes to the size, scope, and operational nature of the business, recent security threats or incidents, new or emerging risks, and changes in industry standards.

DC16: The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the board of directors, as appropriate

On a quarterly basis, the information security team performs a risk assessment update that identifies changes to internal and external cyber threats and vulnerabilities to the organization. Results are

evaluated by the risk governance committee, to identify whether new protective measures or enhanced information security policies and procedures are needed. The risk governance committee is also tasked with monitoring vulnerabilities, allocating resources to address them, and reprioritizing remediation initiatives, as necessary. Key performance indicators related to average closure time have also been defined and are monitored by the committee on a monthly basis.

The results of all monitoring activities, regardless of source, are entered into a vulnerability tracking system for evaluation and identification of remediation activities that may be needed. Identified vulnerabilities are assessed with regard to the likelihood and magnitude of exploitation. All vulnerabilities evaluated are identified for remediation or additional monitoring. Responsibilities for corrective action plans are assigned and completion dates determined. The information security committee reviews the list of open vulnerabilities on a monthly basis to monitor progress toward resolution and to identify trends and responses. On a quarterly basis, the risk governance committee and executive management receive summary reports of vulnerability management activities. In addition, the CISO presents cybersecurity risk management program results, including vulnerability management activities, to the board of directors during each of its regularly scheduled meetings.

Cybersecurity Control Activities

DC17: The process for developing a response to assessed risks, including the design and implementation of control processes

A risk governance committee was established by XYZ to coordinate the risk assessment and management efforts of the entity and its units. The committee, which is chaired by the CRO and consists of the CISO, CCO, external specialists, and IT and business line personnel, ensures that risks are evaluated and that controls are designed, implemented, and operated to address all areas, as appropriate, to detect, respond to, mitigate, and recover from security events based on the assessed risks. Areas for evaluation include systems development, computer operations, program changes, and access to programs and data. Implemented controls include preventive and detective controls, such as manual, automated, or IT-dependent controls based on the environment in which the entity operates; the nature and scope of the entity's operations and its specific characteristics.

Business processes are documented in standard operating manuals; however, the risk governance committee also has business operations liaisons in each business area that are responsible for the ownership and documentation of key risk areas for the business operations. In 2014, the risk governance committee enhanced their key risk considerations for business areas to include specific consideration of cybersecurity risks.

The risk governance committee business liaisons annually revisit the risk assessments and validate the existence of controls to mitigate identified risks. The controls are captured in the Company's controls repository (CR), which is an inventory of the operations, risks, and controls associated with each business area. The CR is used to conduct quarterly self-assessments of controls and also serves as an input into the Company's annual controls maturity assessment, which is conducted by internal audit and reported to the risk governance committee.

The Company contracts for insurance coverage, including business disruptions, for risks which cannot be cost effectively mitigated through other techniques.

DC18: A summary of the entity's IT infrastructure and its network architectural characteristics

XYZ employs both internally hosted and cloud-based applications to support its manufacturing, retail, and wholesale operations. Cloud-based applications are provided through an arrangement with ABC Cloud under a service contract whereby XYZ retains the responsibility for specific server configuration and operating system change management, and ABC Cloud provides server support and maintenance. Company applications run primarily on Unix family operating systems and use industry standard database management systems. The manufacturing system uses a proprietary midrange operating system supplied

by a leading IT manufacturer. The application was developed in house using the integrated operating system database. Field sales application tablets use an industry standard operating system.

XYZ has segmented its ERP financial reporting systems from its externally facing retail, wholesale, and call center interfaces through the use of Cisco ASA firewalls, which are configured, managed, and supported by XYZ IT personnel. The firewall configurations and rules follow standards created by XYZ IT management under the direction of the CISO. All connectivity to external users occurs through defined access points protected by a redundant firewall complex. Firewalls are also used to segment the network within the Company.

Wholesale call center services are outsourced, with the call center's systems interfaced with the ERP system to facilitate ordering and problem resolution. The interface with the call center is over a virtual network connection. Custom-developed software is used to interface the call center system to the ERP interface.

The call center service provider facilities are reviewed annually by XYZ through their previously defined vendor and business partner oversight program. These vendor and business partner assessments focus on areas specific to the security configurations of the hosted applications, as well as to the network architecture related to XYZ's interfaces to the vendors.

ABC Cloud's SaaS is also reviewed annually through XYZ's vendor and business partner oversight program; however, given the nature of the responsibilities defined within the cloud agreement, XYZ configures its server settings in line with XYZ's corporate standards. XYZ has defined a standard build for cloud-based server configurations and uses that as the baseline from which servers are configured to support the SaaS environment. Also, monitoring of the configurations for adherence and compliance with defined standards is conducted by XYZ IT support personnel, as well as through the corporate internal audit and risk management teams.

Field sales automation is provided through the use of Company-owned tablet devices running third-party software customized for the Company. Tablets access the ERP system through a cellular-based VPN system that uses two-factor, token-based authentication.

DC19: The key security policies and processes implemented and operated to address the entity's cybersecurity risks, including those addressing the following:

- a. Prevention of intentional and unintentional security events**
- b. Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents**
- c. Management of processing capacity to provide for continued operations during security, operational, and environmental events**
- d. Detection, mitigation, and recovery from environmental events and the use of backup procedures to support system availability**
- e. Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the of the retention period**

XYZ has defined a set of information security standards and policies that are under the direction and ownership of the CIO and implemented through the CISO. The standards and policies address the management and implementation of security controls, ranging from the physical security of facilities and equipment to the logical security at the data element layer. The information security policies and standards are designed to provide information to employees, contractors, and vendors that is aligned to their job or functional responsibilities, while also contemplating segregation of functions that may otherwise create a segregation of duties conflict.

Security policies are published on the Company's intranet, included in onboarding packages, and reiterated through annual training that all employees are required to take and acknowledge. Security

policies related to relationships with vendors and business partners are enforced through contractual commitments and related service-level agreements (SLAs) and, where possible, are monitored for adherence through XYZ's vendor and business partner oversight program. The key components of the XYZ information security policy are discussed in the following paragraphs.

Prevention of intentional and unintentional security events. The Company has the following processes in place to prevent intentional and unintentional security events:
Physical and Logical Access Provisioning, De-provisioning, and Transfers (Including Remote Access). XYZ employees are granted network access only after completing security-awareness training. Users are granted access to XYZ systems and data based on their job role. Access requests are approved by the user's manager prior to access being granted. Upon termination, human resources sends a notification through the ticketing system, which is routed to the user administration team to remove user account access for the terminated user. Human resources provides a weekly list of terminations, which is then cross-referenced against the user account list to identify any user accounts that have not been properly terminated. User accounts that are inactive for 60 days are automatically disabled. For access modifications, the user's manager is required to submit and approve an access request ticket via the ticketing system, which is routed to the user administration team for processing.
Authentication. Users are required to authenticate using a unique user ID and password before being granted access to the network. The network domain password policy is configured to include password minimum length, expiration intervals, complexity, history, and an invalid password account-lockout threshold. A new user's account password is set to pre-expire so that the password must be reset the first time a user logs in to the network.

Credentials Management. Access is granted based on role-based security profiles that provide segregation of duties and limit transaction access. XYZ application and data owners review access rights on a semiannual basis. On an annual basis, the roles and the transactions assigned to the roles must be reviewed.

Privileged User Management. Access to privileged user or superuser accounts is authorized by management. Users with privileged user accounts are provided with a standard (nonprivileged) user account for use on a daily basis (for email and personal productivity software), and are only permitted to use their superuser accounts when performing administrative tasks. All superuser account access is logged and monitored. On a quarterly basis, the user administration team performs an access review of privileged access.

Database Security. Database administrators are the only individuals that can access XYZ databases. All database access and activity are logged. Database account access is reviewed twice a year for continued appropriateness. Direct data changes require approval, which should be documented within the Company's ticketing system and handled via the change management process.

Data Loss Prevention (DLP). The Company has a DLP solution that monitors and provides alerts about (and can take action regarding) the transmission or removal of confidential data outside of the Company or on noncompany-owned devices. The DLP solution is configured to encrypt external storage devices and prevent the saving of sensitive data to removable media. Hard drives of all servers, workstations, and laptops are encrypted. XYZ Manufacturing and its vendors utilize transport layer security for encryption of transmissions across the Internet to XYZ web servers and the email system. A VPN requiring multifactor authentication is used for all remote access to XYZ's internal network, ensuring that data is encrypted in transit when sent across the Internet from a Company computer system. Site-to-site VPNs are also utilized with certain XYZ vendors to provide encrypted channels for communication between locations.
Data Destruction. Data that exceeds its retention period is removed from systems and all backup media. Data that is labeled as confidential is erased using secure deletion techniques approved by the U.S. government (multi-pass overwrite). All computer hard drives are required to be securely deleted before disposal, and a certificate of destruction is obtained from the third-party organization that disposes of all computer equipment for XYZ.

Data Backup. Nightly incremental backups of all production servers and daily backups of production databases are conducted. Every month end, the Company is required to perform a full backup of the production servers. Backup tapes are encrypted and sent to a third-party vendor for storage. An automated backup system is implemented to monitor the completion of scheduled backups. When a backup job is not completed successfully, operations personnel create an incident ticket and assign personnel to resolve the failure.

Virus Detection and Prevention. Antivirus software is required to be installed on all XYZ servers, desktops, laptops, and email infrastructure and is centrally managed to ensure timely delivery of signature updates. The antivirus software settings are preconfigured for automatic updates and locked to prevent any user tampering or disabling. Email filtering software is in place to restrict and reject emails that contain certain malicious file types, including executable files. The Company's antivirus administrator is required to perform a quarterly inventory reconciliation against a system inventory list.

Firewalls and Perimeter Security. XYZ Manufacturing deploys enterprise firewalls at the perimeter of the network and in other strategic locations throughout the network in an active failover configuration. Only a minimal number of ports and services are allowed into the XYZ environment. All firewalls are managed using a centralized console, and XYZ installs monitoring software on the firewalls to provide alerts when changes occur at the administrative level. Firewall rulesets are reviewed twice a year to ensure that they are appropriately configured.

Secure System Configuration. Configuration specifications are installed on all systems before they are implemented into production. Monthly vulnerability and configuration scans to validate that all systems remain configured in accordance with XYZ's security hardening standards are performed. When updates to existing standards are made, the changes are implemented on production systems.

Intrusion Prevention. A threat intelligence database is regularly updated. Packets identified by the threat intelligence database that meet a certain risk threshold or exhibit certain characteristics are automatically dropped and prevented from entering the XYZ network.

Change Management. A change approval board (CAB) that consists of representation from all IT departments within XYZ is in place. On a weekly basis, the CAB meets to review upcoming system and application changes, which are requested via the Company's online ticketing software. All changes are required to have a documented back-out plan. All changes are required to have a documented test plan. All members of the CAB approve a change before it can be implemented. In the weekly CAB meeting, the previous week's changes are reviewed. A root cause analysis report is completed for any changes that did not go as planned before they can be reconsidered.

Application Changes. Change requestors submit a change request within the Company's ticketing system. An application analyst reviews the change request and develop a project change budget estimate. On a monthly basis, application change requests and associated budgets are reviewed and categorized by IT and the business owners and ranked according to priority. Development occurs in a development environment that is separate from the production environment, using test data. Once development is completed, user acceptance testing takes place. Once user acceptance testing is completed, the business owner who sponsored the change and the applicable application analyst are required to approve the change within the ticket. The IT operations team migrates changes into production after they have been approved by the CAB. Emergency changes are required to be documented and logged in the ticketing system after changes are completed, and the CAB conducts an after-action review to approve the changes retroactively.

Patch Management. When new patches are released, they are reviewed by a group of IT personnel, including a representative from the information security team. The team assigns a priority level to each patch. Patches that are assigned a rating of "critical" are applied to all affected systems within 7 days. Patches that are assigned a rating of "high" are applied to all affected systems within 30 days. Patches that are assigned a rating of "medium" are applied within 60 days. All other patches are applied in regular system updates that typically occur quarterly. Once assigned a patch criticality rating, a patch is assigned to the appropriate IT system administrator for evaluation and testing in the XYZ test lab. When testing is completed, a change ticket is entered in the ticketing system, and the patch is reviewed and approved by the CAB. Monthly, the information security team is required to conduct vulnerability scanning of all

systems to ensure that patches are properly in place. Any missing patches are immediately ticketed and a resolution is required within 5 business days.

Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents. Due to the pervasive use of IT to conduct business operations and deliver products and services to customers, the ability to detect a security event in a timely manner is of significant importance. Accordingly, XYZ Manufacturing has defined formal key security policies and processes focused on identifying cybersecurity issues to detect security events. These policies and processes are focused on the following:

- Utilizing continuous security monitoring tools and programs to assist in identifying anomalies within the network and supporting infrastructure environment—inclusive of security event information relevant to third-party vendors
- Implementing security monitoring processes and procedures and other measures to identify anomalies in information flow, access, data communications, and the operation of business-critical systems
- Analyzing anomalies to identify security events and to detect abnormal events or data movement using historical baseline or behavioral analytics data to determine what is considered to be abnormal
- Escalating identified security events that occur through the course of business operations and ongoing communications, both within and outside of the organization

Detection of Security Events. A dedicated security team is available 24/7. Administrative activity and supporting infrastructure components are monitored through manual analysis and automated alerts where risk-based security monitoring, or a triage approach, is performed based on inherent risk of the anomaly or security event detected and the potential impact that said event could have on the Company's business operating environment. Security monitoring procedures are documented and consistently followed; documentation updates are made to the relevant security monitoring procedures related documentation when required or when significant procedure-related changes are made. Regular security monitoring and detection-based reporting capabilities with metrics are mapped to business drivers for security monitoring purposes. Vendor-related and custom signatures are updated regularly based on threat intelligence information gathered for security-detection purposes. Centrally stored or monitored logs are maintained, and correlation and alerting capabilities are performed on a limited basis when unusual activity is suspected based on the information gathered from the security incident and event management (SIEM) system.

Development of a Response Plan. The incident response sections of the Cybersecurity Incident Response and Recovery Plan (CIRP) includes tactical procedures to help "triage," contain, monitor, or eradicate a security incident, including procedures to do the following:

- Respond to, recover from, and restore normal business operations in a timely manner with minimal, or no, business interruption or loss of data
- Continuously improve the cybersecurity risk management program to limit the likelihood and impact of future incidents based on lessons learned from the Company's own experiences and those of others
- Communicate with employees, stakeholders, regulators, and other constituents in a structured manner about the nature of the security incident, impact to the organization and others (if applicable), and the corrective action taken to recover

The incident response sections of the CIRP have been created based on a threat scenario risk assessment performed annually as part of the review of the plan. The plan is focused on responding to those threat scenarios that have the highest impact and likelihood of occurring based on the business and markets in which the Company operates and the current technology environment. The incident response sections of the CIRP include the following key information:

- Response plan owners (those who can activate the plan), team members, and contact information for plan owners and team members
- Defined criteria required to activate the response plan
- Target business and IT performance metrics for operating in a “business as usual” environment
- Linkage to the business impact analysis and critical path recovery items within the disaster recovery (DR) and business continuity (BC) plans
- Alternate internal and external communication and operating methods to use when primary methods are unavailable
- Communication plan for notifying internal stakeholders (including legal, human resources, marketing, and investor relations), retained service providers (external counsel, forensics investigators, and the like), and external stakeholders (such as customers, vendors, regulators, and law enforcement) to manage expectations and information disclosure as part of the overall response effort. The communication plan also includes communication templates for certain formal internal and external communications, including, but not limited to, internal IT outage notifications and public press releases
- Facility recovery procedures providing linkage to the DR and BC plans regarding the hosted hot site facility located in Syracuse, NY, and the alternate call center located in Troy, MI
- Data response procedures providing linkage to the backup policies and procedures, as well as the DR plan, regarding offsite data storage and backup media
- Hardware and software access procedures enabling IT service and operations during response and recovery procedures
- Response and recovery metrics focused on the target response and recovery milestones to enable effective management, measurement, and monitoring of recovery activities
- Detailed incident response and recovery procedures to be executed based on the identification of the root cause, including operational steps to eradicate any infections, malicious code, unauthorized user accounts, and the like, and restore systems in accordance with priority and dependencies

It should also be noted that mitigating processes and controls are evaluated as part of the current CIRP-related processes and controls in place to detect and respond to security incidents and events. (These mitigation process and control factors may be directly related to the CIRP or may be part of other security monitoring related controls.)

The CIRP is reviewed annually and approved by the following members of management:

- CISO
- CIO
- CTO
- CRO
- GC
- Chief Marketing and Communications Officer
- Director, Security Operations
- Director, Crisis and Response Management

Implementation Activities to Mitigate and Recover from Identified Security Incident. The plan activation process begins when one or more of the incident response and recovery plan owners are informed of a cybersecurity event for which incident response is imminent or underway. The plan owner will ensure details about the cybersecurity event are clearly understood and documented to the extent necessary to enable future communications. This includes the identification of security monitoring or other mitigating processes and control factors which may be present and reduce the overall impact of the identified security event. Should the plan owner decide to activate the plan, he or she will convene an emergency

meeting of the CIRP leadership team (including the CIO, CISO, CRO, GC, VP of human resources, and CFO) to determine

- immediate tasks,
- departments and functions required to carry out the plan based on the cybersecurity event,
- the initial communication plan and the individual assigned to execute the plan.

Once agreement is made, the leadership team is responsible for notifying members of their teams and others, including external advisors (such as investor relations and external general counsel) about the plan activation, initial decisions made, and assigned actions.

Once activated, XYZ considers the current cybersecurity event and its effects on systems and business operations. The Company refers to the appropriate sections of the BC and DR plans, as well as the relevant and applicable data backup logs, to identify the following:

- Where the IT systems and IT infrastructure affected by the cybersecurity event reside within the asset prioritization hierarchy
- Where the business operations affected by the cybersecurity incident or event reside within the operations prioritization hierarchy
- The planned alternative IT systems (such as the failover or load-balanced servers and network devices) and business processing activities (for instance, manual sales order forms) for the effected components of the environment
- The time prior to the cybersecurity incident or event from when the Company will be able to respond to and recover from (recovery point objective [RPO]) for the affected IT systems and IT infrastructure
- The maximum length of time until IT systems, IT infrastructure, and business processes affected by the cybersecurity incident or event is returned to normal business operation, after which significant negative impact may occur (recovery time objective [RTO])

For each IT asset (hardware and software, including virtualized assets) affected by the cybersecurity event, an evaluation will be made to determine the appropriate response and recovery actions, such as the following:

- Decommission and replace
- Reconfigure with enhancements (firmware updates, vendor patches, configuration changes)
- Reconfigure with no enhancements

Recognizing that the Company may not be able to complete the chosen recovery action in a timely manner in relation to the RTO, an alternative solution will be determined to enable a return to normal processing.

Data restoration is based on the activities outlined in the backup and recovery policies and procedures. The backup procedures apply to the following:

- Network devices—such as configurations, access control lists, and firmware
- Physical and virtual servers (DNS servers, email servers, FTP servers, application servers, database servers, web servers)—operating systems, application programs, and application data
- Networked file shares
- End user computing (desktops, laptops, tablets, mobile devices) and peripherals (such as printers and copy machines)
- Telephone and voicemail systems

XYZ Manufacturing leverages a global backup management solution to manage the backup processing and monitoring of all IT assets connected to the environment. The backup solution is connected to a virtual storage area network (SAN) and supplemented by real-time disk imaging to an offsite facility for the highest-value IT assets and data. Moderate- and lower-value information and IT assets are backed up to electronic, removable media and stored at a secure offsite facility for the period of time defined by the

backup and recovery policies and procedures. Backup method and frequency is based on the volume and frequency of information processing and the importance of the data or IT asset.

Restoration of data, software, and configurations is made using the global backup management solution. Prior to restoring data, software, and configurations to the live environment, the Company will conduct tests in the security sandbox against the backup media to determine if the cybersecurity event is present. Based on results, the Company may seek to leverage an older backup or execute the eradication techniques that were successfully employed in the production environment.

Communications related to a cybersecurity event are governed by the CIRP leadership team. Throughout recovery efforts, XYZ will communicate to the extent possible, and as required, with employees, stakeholders, regulators, or law enforcement through formal written and verbal communications (email, press releases, mass voicemail) that are structured to be informative, easy to understand, and transparent and that address the following:

- Current understanding of the cybersecurity incident or event
- The known impact of the cybersecurity incident or event
- The current status of remedial action being taken in response to the cybersecurity incident or event

Communications are tailored to specific audiences (all employees, individuals of whom specific action is required, public domain), leveraging templates that have previously been created and preapproved by appropriate members of executive management and external advisors.

Within ten business days of returning to "business as usual," the CIRP requires a formal meeting of the full cybersecurity incident response and recovery team. The purpose of the meeting (which may be held via teleconference, videoconference, or in person) is to discuss lessons learned from the event and additional actions required. Defined criteria are included within the CIRP to help determine the structure of the meeting, the documentation required, and the monitoring that will be performed to ensure any new correction action agreed upon or implemented since the occurrence of the cybersecurity incident or event continues to operate over a period of time. During the meeting, at a minimum, the following are discussed:

- Identified breakdown in processes or controls, if any
- Enhancements that may need to be made to the process for identifying security monitoring or other mitigating processes and control factors which may be present in the environment and reduce the overall impact of the identified security event, prior to plan activation
- Changes required to standard configurations and the status of changes to other comparable systems that have yet to be attacked (as well as confirmation that those systems have not been compromised)
- Changes to the CIRP or the response team that would benefit incident response or recovery capabilities
- Capital investments or additional operating expenses required to more effectively prevent or detect a similar cybersecurity incident or event
- Changes to business partner relationships that may enable better response or recovery actions to be taken for future cybersecurity incidents or events
- Changes to CIRP test scenarios

The meeting minutes from the discussion are documented and appended to the CIRP.

Once per quarter, as part of the crisis management and incident response readiness activities, formal tests of response and recovery procedures are performed. Tests are based on overall-business-based scenarios that have been developed to confirm awareness of and education about the CIRP and related plans (such as the DR and BC), as well as to hone plan content in an effort to continuously improve response and recovery capabilities.

Tests performed during three of the four quarters are "tabletop" exercises in conference rooms, leveraging tele- and videoconferencing as necessary to conduct a virtual simulation with the CIRP team and other stakeholders. Tests performed during the other quarter involve a real-life simulation where a

simulated cybersecurity incident or event is triggered. Only the CIRP leadership team is initially aware of the simulation. XYZ executes the response and recovery plan in a "real life" situation until the point when communication with internal and external stakeholders would be required. The Company then completes the simulation as if it were a real event. Test results produced from this simulated event are formally discussed; ongoing updates are made to the CIRP as deemed necessary.

Management of processing capacity to provide for continued operations during security, operational, and environmental events. Policies and processes are implemented to address capacity management and include the use of the Information Technology Infrastructure Library (ITIL) IT service management framework for capacity management. Performance management and capacity monitoring tools are used to real-time information to the network operations centers. Alert levels are established based on asset priority and failover capability for the load-balanced and redundant components. Alerts may be in the form of a yellow or red color indicator on the operator console within the network operations centers. The automatic creation of a problem ticket in the service management system for investigation and resolution, or an automated text and email to the on-call IT operations lead, is acceptable.

Detection, mitigation, and recovery from environmental events and the use of backup procedures to support system availability. Policies and processes are implemented to address the detection, mitigation and recovery from environmental threats. The primary computer facility houses key IT infrastructure for the Company's integrated ERP system and midrange platforms supporting manufacturing software. The facility has been specifically designed to mitigate the risk of environmental threats to the computer hardware operations and include protection from fire and the loss or fluctuation of power, cooling, and humidity.

Fire suppression systems, in combination with smoke detection and hand-held fire extinguishers, are installed throughout the Company's facilities. Preventive maintenance is performed annually along with required inspections. An uninterruptible power supply (UPS) system provides continuous conditioned power through its strings of batteries to all infrastructure hardware to control unanticipated power interruptions. Maintenance for the UPS and batteries is performed at least quarterly. Emergency generator systems are required to be installed within the secure perimeter of the data center facilities. They are sized to provide 100 percent of the data center's electrical service in the event of a utility service failure. These generators have scheduled maintenance performed at least quarterly. The temperature and humidity inside the data center is controlled by dedicated air conditioning systems for computer hardware. These units act independently of any general building air conditioning. Maintenance is performed at least tri-annually. The data center environment, temperature, humidity, power, and fire prevention systems are required to be monitored through a building management system within the command operations center. Operations personnel man the facility 24 hours a day, 7 days a week.

Physical Access. Access to the computer facility entrances and to the network operations centers (including the raised floor areas) is controlled by the badge access reader system. Building access points are required to be locked at all hours except for the main entrance, which can be unlocked during normal business hours and manned by a security guard. At each facility entrance, visitors are required to provide relevant identification, such as name, representing company, and employee contact. All visitors receive a visitor badge and sign in on the visitor log. All personnel are required to display their badge at all times while in the facility. Visitors are escorted while in restricted-access areas of the facility; when leaving, they are required to sign out on the visitor log. Video cameras are monitored 24/7 and provide surveillance over the interior and exterior of the building. All camera activity is recorded on digital video and retained for at least 60 days.

Backup Media. Data and programs are backed up in accordance with defined schedules. The backup schedule, rotation schedule, and retention period of tapes at the offsite storage facility are determined based on business need. The offsite tape storage is located approximately 30 miles from the computer facility. Backup job failures are monitored and tracked to resolution through the incident management process. Monitoring tools established in the job scheduling and monitoring process are utilized to monitor backup jobs. Job monitoring tools are in place to automatically generate an incident ticket in the incident management system for backup failures. Tape management systems are used to manage tape activities in the data center. Features of these systems include onsite media inventory, offsite media inventory, picking list for the vault, distribution list for the vault, and scratch lists.

The tape management systems produce reports to facilitate tape movement between the tape racks and drives in the data center as well as between the data center and the offsite facility. Tape rotation is monitored. Reports are reconciled daily and discrepancies are evaluated and resolved. Periodic inventories of tapes located both onsite and at the offsite facility are required to be conducted. Backup media is periodically tested. Periodic testing of backup media is coordinated by the business continuity team and performed by the appropriate technology groups.

Alternate Processing. BC plans are in place for all major business units and updated on an annual basis. DR plans are in place to support BC plans covering the critical IT infrastructure and networking equipment. The DR plan is updated annually. The main data center is physically separated from business operating units and dedicated solely to processing functions. The DR plans are reviewed annually and tested at least once a year. During a testing exercise, locations that are part of the testing exercise access the DR location through VPNs to segregate the network and prevent interruption to production services.

All business units with RTOs of less than 72 hours participate in a DR exercise once every three years. Business units with RTOs of 48 hours or less participate in the recovery testing exercise on an annual basis. The results of the tests are documented and assembled into a problem and resolution log.

Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the of the retention period. Policies and processes are implemented to address capacity management and include the following:

Data Classification and Retention. The data classification and retention policy and relevant security and confidentiality policies describe how information is designated as confidential and ceases to be confidential. The handling, destruction, maintenance, storage, backup, and distribution and transmission of confidential information are documented in the data classification and retention policy, XYZ's general business terms, and in some cases, in customer and business partner-specific contracts and service-level agreements.

Confidential policies and processes have been implemented to limit access to logical input routines and physical input media to authorized individuals. Each type of confidential information is classified, handled, secured, retained, and disposed of. All nonpublic customer information is confidential. Data that carries a confidential classification is subject to the Company's information security policy, which defines protection requirements, access rights, and access restrictions, as well as retention and destruction requirements. Customer, vendor, and business partner information is presumed to be confidential (as a default) unless obviously not.

As part of their standard process for establishing service levels and operational protocols with vendors or business partners such as ABC Cloud and UVW Trading, XYZ will evaluate data shared between the two organizations and agree on what is confidential. XYZ also requests that business partners disclose their security, data classification, and retention policies to ensure that XYZ's data is afforded the proper retention and information protection. The CISO, with the information security team, is responsible for maintaining and updating confidentiality, system security, and related policies.

At the time of hire or affiliation, the code of conduct and confidentiality agreements that employees are required to sign prohibit any disclosures, beyond the extent authorized, of information and other data to which the employee has been granted access. Individual manufacturing contracts also define how confidential information is authorized and rescinded. Signed nondisclosure agreements are required from third parties before information designated as confidential can be shared with them. XYZ's business partners are also subject to nondisclosure agreements or other contractual confidentiality provisions, as outlined in the Business Associate Agreement. Customer contracts, service-level agreements, and vendor contracts are negotiated before performance or receipt of service and formally signed off on by management.

Logical Access. Customers, groups of individuals, or other entities are restricted from accessing confidential information, other than their own. Users, contractors, or vendors who have the ability to access confidential information are properly authorized or supervised, in line with the Company's employees. The information supervisor for a business unit determines whether users require access to confidential information to perform their specific job functions.

Data Retention. Retention periods, and policies for ensuring retention during the specified period and proper disposal of data at the end of the retention period, are also outlined in the data classification and retention policy. The retention period assigned to data is based on the (1) classification of the data, (2) regulatory requirements and legal statutes, and (3) the general requirements of the business. During the designated retention period, XYZ ensures that backup media (whether offline or online) are stored in a protected environment for the duration of the designated document retention period. Computer backup media is included. When the retention period has ended, XYZ Manufacturing destroys the information securely. Electronic information and other information is disposed of securely by proven means.



Association
of International
Certified Professional
Accountants®

© 2017 Association of International Certified Professional Accountants. All rights reserved.

AICPA is a trademark of the American Institute of Certified Public Accountants and is registered in the United States, the European Union and other jurisdictions. The design mark is a trademark of the Association of International Certified Professional Accountants. 22125A-312

Draft Cybersecurity Framework and Risk Assessment

Identify the types of critical and sensitive data

Risk management program objectives

Availability	<i>Maintaining necessary access and control to the town's banking/accounting, utility billing, communications infrastructure as well as critical data.</i>
Confidentiality	<i>Availability of all information should be generally uninterrupted and able to be recovered within 72 hours in the case of server failure.</i>
Integrity of data	<i>Ensuring that data of a sensitive nature is protected from unauthorized access at all times.</i>
Integrity of Processing	<i>Verifying that the data is correct and can be recovered if in doubt or corrupted</i>
	<i>Protecting systems and controls from improper alteration to ensure correct processing and functionality</i>

How are objectives established, maintained, and approved?

What factors have a significant effect on the entity's inherent cybersecurity risks?

Characteristics of technologies

- A. Connection types*
- B. Frequency of backups*
- C. On-site and off-site backup storage*
- D. Firewall protections?*

Organizational and user characteristics

- A. User practices?*
- B. Password practices?*

Environmental, technological, organizational and other changes during the period

- A. Personnel changes?*
- B. Departmental changes?*
- C. Vendor changes?*
- D. New threats identified?*
- E. Changes in any of the technological characteristics or organizational/user characteristics listed above?*

Security incidents and response?

What security incidents were identified during the 12-month period immediately prior to the begin date of the period reviewed?

Who, what, when, where, why, how?

What steps were taken to mitigate the threat of their reoccurrence?

Cybersecurity Risk Governance Structure

What is the process for establishing, maintaining and communicating the principles of ethics and integrity as they relate to cybersecurity?

How does the town maintain internal and external oversight of the risk management program?

Cybersecurity Risk Assessment Process

How are current and potential cybersecurity risks identified?

How does the town assess the related risks and mitigate appropriately?

Cybersecurity Communications and Quality of Cybersecurity Information

What is the process for internally communicating relevant cybersecurity information, such as objectives/responsibilities, how to identify something unusual and of potential concern (and related consequences)?

What is the process for externally communicating relevant cybersecurity information, such as objectives/responsibilities, how to identify something unusual and of potential concern (and related consequences)?

Monitoring of the Cybersecurity Risk Management Program

What is the process for conducting ongoing and periodic evaluations of internal controls related to cybersecurity?

What is the process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities and control deficiencies to parties responsible for taking corrective actions?

Cybersecurity Control Activities

How are responses to assessed risks developed, including design and implementation of control processes?
Provide a summary of the entity's IT infrastructure and its network architectural characteristics.

What are the key security policies and processes implemented and operated to address the entity's cybersecurity risks, including:

- a. Prevention of intentional and unintentional security events
- b. Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents
- c. Management of processing capacity to provide for continued operations during security, operational and
- d. Detection, mitigation and recovery from environmental events and use of backup procedures to support system
- e. Identification of confidential information when received or created, determination of retention period for that information, retention and then destruction after period expires

Prevention of intentional and unintentional security events

How are credentials levels determined and how often are they reviewed?

How is data loss prevented?

What intrusion prevention tools are in place (generally)?

How are security events detected, identified, responded to and mitigated against?

How is processing capacity managed to provide continued operations during security, operational and environmental events?

How are environmental events detected, mitigated against, and recovered from, and how are backup procedures used to support system availability?



Legislation Details (With Text)

File #: 17-0181 **Version:** 1 **Name:**
Type: Discussion Items **Status:** Agenda Ready
File created: 8/15/2017 **In control:** Finance Board
On agenda: 8/17/2017 **Final action:**
Title: Discussion of 2017-2018 Annual Budget
Sponsors: JP Murphy
Indexes:
Code sections:
Attachments: [FB0817Budget.pdf](#)

Date	Ver.	Action By	Action	Result
------	------	-----------	--------	--------

Summary

To: Finance Board
From: Ashley Bernal, Management Analyst
Date: 8/15/2017

Subject:

Discussion of 2017-2018 Fiscal Year Budget

Summary:

All major funds are presented as balanced at this time. The General Fund is balanced with a proposed 3% salary enhancement and no change to the millage calculation. In addition, the Water and Solid Waste funds are balanced with no proposed utility rate increase. The Commission will conduct a Budget Workshop on 8/24 to examine in detail the proposed budget. Staff provide a detailed discussion and analysis at the meeting regarding the changes, and assumptions.

Previous Commission Action: Commission approved the Tentative Millage Rate of 5.9257.

Background/Problem Discussion: The final millage rate shall not exceed the previously set maximum millage preliminary (MMP) rate of 5.9257. The Commission may set a final rate equal to, or less than the MMP. The proposed fiscal year 2017-18 millage is 5.9257: 4.9427 to the General Fund, and 0.9830 to the Infrastructure Fund, which is the same distribution as the prior year. All millage calculations are based upon the certified total taxable value of \$713,138,935. This is an increase of 6.355% from the prior year's total taxable value

GENERAL FUND

Revenues

Ad Valorem revenues have increased 8.125% for the upcoming year, which equates to an increase of \$256,250. Communication services tax has increased this year by \$11,850, totaling \$178,000. State Revenue Sharing saw a small increase of \$1,950, while State Sales Tax has a larger increase of \$3,250.

As part of the new construction associated with the Golf Course, building permit revenue has increased \$75,000, bringing this year's total to \$375,000. Staff expects this revenue to continue to grow with construction, which will be replaced with an increase of Ad Valorem once construction finishes.

Miscellaneous revenue increased by \$14,700.

Staff has made an effort to rectify any sort of structural imbalances within the revenue of this budget by halting transfers from reserves. This prevents the Town's reserves from depleting entirely, but also creates a large hole in the general revenue.

Expenditures

Overall, Staff is still working to find extra funds for salary enhancements. A large majority of increases in expenditures this year are related to personnel costs.

Administration - The overall budget for this department has increased by \$50,000. This is largely due to an increase to the part-time salary line.

Building - Increased costs are related to contracted inspection costs. There is an increase in construction inspections due to the construction of the Pelican Course and Belleview Place.

Support Services - There is an increase of \$173,550 this year mainly due to personnel expenses. A large majority of this is from the department absorbing building maintenance from Public Works.

Police - The largest increase for expenditures in this department is also related to personnel costs. Salaries increased dramatically due to the mandatory 3% enhancement, causing other personnel lines to increase as well.

Public Works - Though Public Works lost building maintenance, the department expanded by including Parks and Streets from the Recreation department. The rationale is to have the expense for parks and streets be combined for reporting and management reasons.

Recreation - This department is seeing a decrease in expenditure this fiscal year associated with the release of Parks and Streets.

ENTERPRISE FUNDS

WATER

Revenues

Water Utility Revenue is expected to increase by \$51,200 this year. Staff analyzed water usage data from the Fiscal Year 2014-2015, 2015-2016, and a portion of 2016-2017.

Expenditures

Minor increases were made to operating expenditures. The largest change in expenditure comes from Capital Purchase. This year the department needs to replace sand filters (\$62,000) and rehabilitate wells (\$55,000).

SOLID WASTE

Revenues

The Sanitation line item, which is the collection for sanitation fees, will see a decrease of about \$20,000. This decrease is based on a reconciliation of customers' accounts and prior revenue assumptions.

Expenditures

With Belleair's pilot recycling program continuing, costs connected with the recycling line item have decreased by about \$19,750. Staff will provide additional information as to the collection options at the meeting. Mr. Massol will provide detail to the changes in depreciation at the meeting.

Expenditure Challenges N/A

Financial Implications: N/A

Recommendation: Staff recommends the budget as proposed

Proposed Motion I move that the Finance Board recommend the budget as proposed to the Town Commission.

Summary Page

	FY 2016-17 Budget	FY 2017-18 Budget	
Revenues	\$5,776,350	\$5,980,750	\$204,400
Expenditures	FY 2016-17	FY 2017-18	Change Between FY
Administration	\$562,150	\$612,190	\$50,040
Building	\$142,250	\$150,260	\$8,010
Support Services	\$1,860,350	\$2,033,900	\$173,550
Police	\$1,383,000	\$1,520,800	\$137,800
Public Works	\$680,402	\$865,000	\$184,598
Parks & Rec	\$1,197,450	\$798,600	-\$398,850
Total	\$5,825,602	\$5,980,750	\$155,148
	Net	\$0	

08/15/17
16:33:16

TOWN OF BELLEAIR
Revenue Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 1 of 8
Report ID: B250

1 GENERAL FUND

Account	13-14	14-15	15-16	16-17	Current Budget 16-17	% Rec. 16-17	Prelim. Budget 17-18	Budget Change 17-18	Final Budget 17-18	% Old Budget 17-18
300300										
300320 TENNIS ANNUAL PERMITS	2,460	2,199	2,369	530	2,500	21%	2,500		2,500	100%
Group:	2,460	2,199	2,369	530	2,500	21%	2,500	0	2,500	100%
311100 AD VALOREM										
311100 AD VALOREM	2,839,083	2,898,636	3,025,852	3,210,217	3,154,000	102%	3,410,250		3,410,250	108%
Group:	2,839,083	2,898,636	3,025,852	3,210,217	3,154,000	102%	3,410,250	0	3,410,250	108%
313100 ELECTRIC FRANCHISE										
313100 ELECTRIC FRANCHISE	368,811	367,005	348,537	232,897	367,000	63%	367,000		367,000	100%
Group:	368,811	367,005	348,537	232,897	367,000	63%	367,000	0	367,000	100%
313400 GAS FRANCHISE										
313400 GAS FRANCHISE	26,394	21,058	21,174	16,282	22,000	74%	22,000		22,000	100%
Group:	26,394	21,058	21,174	16,282	22,000	74%	22,000	0	22,000	100%
315000 COMMUNICATION SERVICES TAX										
315000 COMMUNICATION SERVICES	172,283	182,915	173,413	115,417	166,450	69%	178,300		178,300	107%
Group:	172,283	182,915	173,413	115,417	166,450	69%	178,300	0	178,300	107%
321100 OCCUPATIONAL LICENSE (TOWN LICENSE)										
321100 OCCUPATIONAL LICENSE	25,643	23,815	24,364	11,602	25,000	46%	25,000		25,000	100%
Group:	25,643	23,815	24,364	11,602	25,000	46%	25,000	0	25,000	100%
331200 FEDERAL GRANT-PUBLIC SAFETY										
331201 JAG GRANT	1,000				0	0%			0	0%
Group:	1,000				0	0%	0	0	0	0%
335100 ALCOHOL BEVERAGE LICENSE										
335100 ALCOHOL BEVERAGE LICENSE	916	916	916		400	0%	150		150	37%
335120 STATE REVENUE SHARING	91,596	96,097	97,630	79,242	100,950	78%	102,900		102,900	101%
335180 SALES TAX	207,846	237,384	244,096	145,645	251,450	58%	254,700		254,700	101%
Group:	300,358	334,397	342,642	224,887	352,800	64%	357,750	0	357,750	101%
335400 TRANSPORTATION STATE REVENUE SHARING										
335410 GASOLINE REBATE	3,917	3,947	2,051	1,873	3,000	62%	3,000		3,000	100%
Group:	3,917	3,947	2,051	1,873	3,000	62%	3,000	0	3,000	100%

08/15/17
16:33:16

TOWN OF BELLEAIR
Revenue Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 2 of 8
Report ID: B250

1 GENERAL FUND

Account	13-14	14-15	Actuals 15-16	16-17	Current Budget 16-17	% Rec. 16-17	Prelim. Budget 17-18	Budget Change 17-18	Final Budget 17-18	% Old Budget 17-18
337200 GRANTS										
337200 GRANTS		765	480	61,765	34,600	179%	50,000		50,000	144%
Group:		765	480	61,765	34,600	179%	50,000	0	50,000	144%
341200 ZONING & VARIANCE FEES										
341200 ZONING & VARIANCE FEES	20,513	600	3,100	1,200	800	150%	800		800	100%
Group:	20,513	600	3,100	1,200	800	150%	800	0	800	100%
341800 COUNTY OFFICER COMMISSION AND FEES										
341802 BUILDING PERMITS	344,824	325,425	382,371	449,992	305,000	148%	375,000		375,000	122%
Group:	344,824	325,425	382,371	449,992	305,000	148%	375,000	0	375,000	122%
342100 SERVICE CHARGE-LAW ENFORCEMENT SERVICES										
342103 SPECIAL DUTY POLICE	2,713	4,611	4,685	1,103	2,000	55%	2,000		2,000	100%
Group:	2,713	4,611	4,685	1,103	2,000	55%	2,000	0	2,000	100%
343900 LOT MOWING										
343900 LOT MOWING	10,095	5,017		3,176	2,700	118%	3,000		3,000	111%
Group:	10,095	5,017		3,176	2,700	118%	3,000	0	3,000	111%
347200 SERVICE CHARGE-PARKS AND RECREATION										
347210 RECREATION (PROG.	272,875	268,709	242,621	236,690	282,750	84%	282,750		282,750	100%
347211 RECREATION PERMITS	26,975	24,844	21,370	22,100	24,000	92%	24,000		24,000	100%
347213 REC-VENDING MACHINE SALES	3,632	3,976	3,553	2,404	10,000	24%	10,000		10,000	100%
347214 Concession Stand Sales	7,755	11,056	8,182	9,648	3,500	276%	3,500		3,500	100%
347217 MERCHANDISE		125	25	28	0	***			0	0%
Group:	311,237	308,710	275,751	270,870	320,250	85%	320,250	0	320,250	100%
347500 SERVICE CHARGE-SPECIAL RECREATION FACILITIES										
347530 SPECIAL EVENTS-Private	6,540	6,069	5,654	4,843	6,000	81%	6,000		6,000	100%
347540 SPECIAL EVENTS-ATHLETIC	23,787	23,562	19,705	15,685	25,000	63%	23,000		23,000	92%
Group:	30,327	29,631	25,359	20,528	31,000	66%	29,000	0	29,000	93%
351100 COURT FINES (POLICE FINES)										
351100 COURT FINES (POLICE	2,272	3,006	2,027	1,782	6,000	30%	4,000		4,000	66%
Group:	2,272	3,006	2,027	1,782	6,000	30%	4,000	0	4,000	66%
351300 POLICE ACADEMY										
351300 POLICE ACADEMY	170	223	174	136	300	45%	300		300	100%
Group:	170	223	174	136	300	45%	300	0	300	100%

08/15/17
16:33:16

TOWN OF BELLEAIR
Revenue Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 3 of 8
Report ID: B250

1 GENERAL FUND

Account	13-14	14-15	15-16	16-17	Current Budget 16-17	% Rec. 16-17	Prelim. Budget 17-18	Budget Change 17-18	Final Budget 17-18	% Old Budget 17-18
351400 RESTITUTION										
351400 RESTITUTION	1,094	2,042	535	883	1,500	59%	1,500		1,500	100%
351402 OTC FINES AND TICKETS	180	270	920	630	250	252%	250		250	100%
Group:	1,274	2,312	1,455	1,513	1,750	86%	1,750	0	1,750	100%
354000 ORDINANCE VIOLATION										
354000 ORDINANCE VIOLATION	72,618	151,418	4,972		2,000	0%	2,000		2,000	100%
Group:	72,618	151,418	4,972		2,000	0%	2,000	0	2,000	100%
361000 INTEREST										
361000 INTEREST	6,856	17,971	747	684	9,000	8%	25,000		25,000	277%
Group:	6,856	17,971	747	684	9,000	8%	25,000	0	25,000	277%
362000 RENTAL INCOME										
362000 RENTAL INCOME	4,800	4,800	4,600	4,000	4,800	83%	4,800		4,800	100%
Group:	4,800	4,800	4,600	4,000	4,800	83%	4,800	0	4,800	100%
364000 GAIN ON SALE OF FIXED ASSETS										
364001 SALE OF FIXED ASSETS		239,585			0	0%	6,000		6,000	*****
Group:		239,585			0	0%	6,000	0	6,000	*****
364100 INSURANCE PROCEEDS										
364100 INSURANCE PROCEEDS	1,264	1,000		2,076	0	***			0	0%
Group:	1,264	1,000		2,076	0	***	0	0	0	0%
365900 SALE OF SURPLUS METAL										
365900 SALE OF SURPLUS METAL	830	168			0	0%			0	0%
365901 SALE OF AUCTIONED ASSETS	28,469	1,353	3,961	2,034	0	***	2,000		2,000	*****
Group:	29,299	1,521	3,961	2,034	0	***	2,000	0	2,000	*****
366900 DONATIONS-PARK IMPROVE. FD.										
366903 DONATION-RECREATION	22,060	15,060	26,549	21,958	10,000	220%			0	0%
366904 BCF CONTRIBUTION HUNTER		2,000	1,700	1,700	1,700	100%	1,700		1,700	100%
366905 CONTRIBUTION - POL.	250	200	5,412	11,220	0	***			0	0%
366909 DONATION - VANITY PLATE	100	25	15	15	0	***			0	0%
366911 SPECIAL EVENTS	174,377	160,555	140,029	146,288	155,775	94%	143,000		143,000	91%
366913 DONATIONS		1,700			0	0%			0	0%
Group:	196,787	179,540	173,705	181,181	167,475	108%	144,700	0	144,700	86%

08/15/17
16:33:16

TOWN OF BELLEAIR
Revenue Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 4 of 8
Report ID: B250

1 GENERAL FUND

Account	13-14	14-15	Actuals 15-16	16-17	Current Budget 16-17	% Rec. 16-17	Prelim. Budget 17-18	Budget Change 17-18	Final Budget 17-18	% Old Budget 17-18
369000 MISCELLANEOUS										
369000 MISCELLANEOUS	35,548	21,358	16,478	26,702	27,500	97%	34,700		34,700	126%
Group:	35,548	21,358	16,478	26,702	27,500	97%	34,700	0	34,700	126%
369900 OTHER MISCELLANEOUS REVENUES										
369901 VENDING MACHINE PROCEEDS		67	212		0	0%			0	0%
Group:		67	212		0	0%	0	0	0	0%
370200 PARKER PROPERTY RESERVES										
370201 RESERVES					40,000	0%	40,000		40,000	100%
Group:					40,000	0%	40,000	0	40,000	100%
381000 RESERVES (PRIOR YEARS)										
381000 RESERVES (PRIOR YEARS)					189,250	0%			0	0%
Group:					189,250	0%	0	0	0	0%
381200 TRANSFER FROM 301										
381200 TRANSFER FROM 301	32,200		65,050		25,400	0%			0	0%
381210 TRANSFER FROM 110	4,500				34,300	0%	63,850		63,850	186%
Group:	36,700		65,050		59,700	0%	63,850	0	63,850	106%
381300 TRANSFER FROM LAND DEVELOPMENT										
381302 TRANSFER FROM 305	200,000	175,000	150,000		135,000	0%			0	0%
Group:	200,000	175,000	150,000		135,000	0%	0	0	0	0%
381400 TRANSFER FROM 001										
381401 TRANSFER FROM 401			14,700		0	0%			0	0%
381406 TRANSFER FROM 113 (TREE		4,500			0	0%			0	0%
381407 TRANSFER FROM 115 (GOLF		111,000	43,000	43,000	887,750	5%			0	0%
Group:		115,500	57,700	43,000	887,750	5%	0	0	0	0%
383000 ADMINISTRATIVE FEES										
383000 ADMINISTRATIVE FEES	476,800	469,750	485,750		505,800	0%	505,800		505,800	100%
Group:	476,800	469,750	485,750		505,800	0%	505,800	0	505,800	100%
384000 LOAN FROM OPERATING										
384010 DEBT PROCEEDS			259,091		28,600	0%			0	0%
Group:			259,091		28,600	0%	0	0	0	0%

08/15/17
16:33:16

TOWN OF BELLEAIR
Revenue Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 5 of 8
Report ID: B250

1 GENERAL FUND

Account	13-14	14-15	15-16	16-17	Current Budget 16-17	% Rec. 16-17	Prelim. Budget 17-18	Budget Change 17-18	Final Budget 17-18	% Old Budget 17-18
385000										
385005 FORFEITURE ACCOUNT (ICMA)					14,000	0%				0 0%
Group:					14,000	0%	0	0	0	0%
Fund:	5,524,046	5,891,782	5,858,070	4,885,447	6,868,025	71%	5,980,750	0	5,980,750	87%

08/15/17
16:35:57

TOWN OF BELLEAIR
Expenditure Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 1 of 13
Report ID: B240

1 GENERAL FUND

Account	Object	----- 13-14	----- 14-15	----- 15-16	----- 16-17	Current Budget 16-17	% Exp. 16-17	Prelim. Budget 17-18	Budget Changes 17-18	Final Budget 17-18	% Old Budget 17-18
513100	ADMINISTRATION										
51100	SALARIES:EXEC.		1,086	9,314	7,600	9,600	79%	9,600		9,600	100%
51200	SALARIES	124,836	148,532	273,410	294,518	364,200	81%	323,250		323,250	89%
51201	PT SALARIES	121			7,097	7,100	100%	60,000		60,000	845%
51210	Unused Medical			807	1,432	2,204	65%			0	0%
51500	SICK LEAVE	6,003	3,375	10,688		10,235	0%	10,250		10,250	100%
52100	FICA	9,827	10,905	21,876	22,545	27,750	81%	25,500		25,500	92%
52200	RETIREMENT-401K GENERAL P	11,699	13,672	21,522	23,692	30,550	78%	29,100		29,100	95%
52300	LIFE/HOSP. INS.	15,731	21,910	43,386	39,963	47,100	85%	55,600		55,600	118%
52301	MEDICAL BENEFIT	1,530	2,066	4,178	2,424	3,797	64%	6,000		6,000	158%
54000	TRAV & PER DIEM	7,202	22,415	18,659	24,291	25,800	94%	20,000		20,000	78%
54100	TELEPHONE	2,511	2,809	3,564	2,285	4,400	52%	4,400		4,400	100%
54200	POSTAGE			1,828	666	1,600	42%	1,600		1,600	100%
54620	MAIN. - VEHICLE	129	794		1,705	1,750	97%	1,000		1,000	57%
54700	ORDINANCE CODES		2,775	1,184	3,296	3,300	100%	3,000		3,000	91%
54930	ADVERTISING		500	3,188	4,830	5,500	88%	3,500		3,500	64%
54940	FILING FEES		318	489	272	1,500	18%	1,250		1,250	83%
55100	OFFICE SUPPLIES		199	2,281	1,214	2,250	54%	3,100		3,100	138%
55101	BOARDS EXPENSES		812	3,892	1,295	3,000	43%	5,000		5,000	167%
55210	OPERATING SUPPL	1,112	1,980	3,720	2,284	2,300	99%	4,540		4,540	197%
55222	RECORDS MGMT.-FEES		787	2,498	10,922	12,350	88%	3,000		3,000	24%
55240	UNIFORMS	60	89	139	308	650	47%	650		650	100%
55260	PROTECT. CLOTH.				140	250	56%	250		250	100%
55290	ELECTIONS			1,996		0	0%	5,000		5,000	*****
55410	MEMBERSHIPS	5,067	7,584	10,995	7,360	7,800	94%	10,800		10,800	138%
55420	TRAINING, AIDS	3,823	21,707	25,091	12,447	14,500	86%	19,500		19,500	134%
56402	CARS			27,614		0	0%			0	0%
56405	COMPUTER SYSTEM		4,325		4,084	4,265	96%			0	0%
57001	VEHICLE DEBT SERVICE			2,938	5,900	5,900	100%	5,900		5,900	100%
57900	ARCHIVES		38	137	283	400	71%	400		400	100%
58101	CAPITAL PURCH.	9,917				0	0%			0	0%
58102	TRANSFER TO 301	6,000	6,000			0	0%			0	0%
Account:		205,568	274,678	495,394	482,853	600,051	80%	612,190	0	612,190	102%

08/15/17
16:35:57

TOWN OF BELLEAIR
Expenditure Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 2 of 13
Report ID: B240

1 GENERAL FUND

Account	Object	----- 13-14	Actuals 14-15	----- 15-16	----- 16-17	Current Budget 16-17	% Exp. 16-17	Prelim. Budget 17-18	Budget Changes 17-18	Final Budget 17-18	% Old Budget 17-18
513300	TOWN CLERK'S DEPT.										
51100	SALARIES:EXEC.		4,800			0	0%			0	0%
51200	SALARIES	128,129	91,720			0	0%			0	0%
51500	SICK LEAVE	5,019				0	0%			0	0%
52100	FICA	10,122	7,349			0	0%			0	0%
52200	RETIREMENT-401K GENERAL P	11,983	8,255			0	0%			0	0%
52300	LIFE/HOSP. INS.	24,409	13,657			0	0%			0	0%
52301	MEDICAL BENEFIT	1,425	788			0	0%			0	0%
53151	PROF. SERVICES		2,263			0	0%			0	0%
54000	TRAV & PER DIEM	735	144			0	0%			0	0%
54100	TELEPHONE	212	766			0	0%			0	0%
54200	POSTAGE	925	777			0	0%			0	0%
54670	MAINT. - EQUIP	138				0	0%			0	0%
54700	ORDINANCE CODES	4,488	9,211			0	0%			0	0%
54930	ADVERTISING	6,363	11,461			0	0%			0	0%
54940	FILING FEES	1,265	1,227			0	0%			0	0%
55100	OFFICE SUPPLIES	1,399	399			0	0%			0	0%
55101	BOARDS EXPENSES	12,629	6,129			0	0%			0	0%
55210	OPERATING SUPPL	2,337	1,705			0	0%			0	0%
55222	RECORDS MGMT.-FEES	2,358	1,231			0	0%			0	0%
55290	ELECTIONS		4,707			0	0%			0	0%
55410	MEMBERSHIPS	230	155			0	0%			0	0%
55420	TRAINING, AIDS	945	85			0	0%			0	0%
56405	COMPUTER SYSTEM		28,134			0	0%			0	0%
57900	ARCHIVES	114				0	0%			0	0%
	Account:	215,225	194,963			0	***%	0	0	0	0%

08/15/17
16:35:57

TOWN OF BELLEAIR
Expenditure Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 3 of 13
Report ID: B240

1 GENERAL FUND

Account	Object	----- 13-14	----- 14-15	----- 15-16	----- 16-17	Current Budget 16-17	% Exp. 16-17	Prelim. Budget 17-18	Budget Changes 17-18	Final Budget 17-18	% Old Budget 17-18
515000	BUILDING DEPT.										
51200	SALARIES	40,544	41,145	40,469	33,601	42,150	80%	42,200		42,200	100%
51400	OVERTIME	262		59	357	0	***%			0	0%
51500	SICK LEAVE	1,478	1,735	1,281		1,750	0%	1,750		1,750	100%
52100	FICA	3,177	3,187	3,109	2,541	3,250	78%	3,250		3,250	100%
52200	RETIREMENT-401K GENERAL P	3,806	3,859	3,763	3,056	3,800	80%	3,800		3,800	100%
52300	LIFE/HOSP. INS.	6,741	7,476	8,023	6,859	8,350	82%	8,750		8,750	105%
52301	MEDICAL BENEFIT	1,154	1,204	1,182	975	1,200	81%	1,200		1,200	100%
53160	CONTRAC. LABOR	105,649	80,824	70,700	74,295	80,000	93%	87,360		87,360	109%
54100	TELEPHONE	306	10	9	4	250	2%	250		250	100%
54670	MAINT. - EQUIP	2,306	208	200	424	500	85%	500		500	100%
55100	OFFICE SUPPLIES	399	360	276	246	300	82%	500		500	167%
55210	OPERATING SUPPL	352	4,886	196	228	500	46%	500		500	100%
55240	UNIFORMS	154	265		127	200	64%	200		200	100%
55420	TRAINING, AIDS	289				0	0%			0	0%
56405	COMPUTER SYSTEM		1,103	298		0	0%			0	0%
58102	TRANSFER TO 301			4,706		0	0%			0	0%
	Account:	166,617	146,262	134,271	122,713	142,250	86%	150,260	0	150,260	106%

08/15/17
16:35:57

TOWN OF BELLEAIR
Expenditure Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 4 of 13
Report ID: B240

1 GENERAL FUND

Account	Object	Actuals				Current	%	Prelim.	Budget	Final	% Old
		13-14	14-15	15-16	16-17	Budget 16-17	Exp. 16-17	Budget 17-18	Changes 17-18	Budget 17-18	Budget 17-18
519000	SUPPORT SERVICES										
51200	SALARIES	353,296	355,190	306,410	254,762	342,800	74%	419,000		419,000	122%
51210	Unused Medical	691	486	875	1,645	1,795	92%			0	0%
51400	OVERTIME	1,567	270	111	328	1,000	33%	1,500		1,500	150%
51500	SICK LEAVE	15,240	11,279	9,895		7,350	0%	8,350		8,350	114%
52100	FICA	28,179	28,041	24,139	19,540	26,250	74%	32,050		32,050	122%
52200	RETIREMENT-401K GENERAL P	33,247	33,175	28,556	21,303	30,850	69%	37,700		37,700	122%
52300	LIFE/HOSP. INS.	56,329	63,554	58,105	50,781	62,950	81%	76,650		76,650	122%
52301	MEDICAL BENEFIT	6,958	6,748	5,662	4,684	4,805	97%	10,200		10,200	212%
53100	PHYSICAL EXAMS	38		5,063	455	500	91%	500		500	100%
53110	TOWN ATTORNEY	128,268	191,595	73,623	111,013	124,250	89%	75,750		75,750	61%
53151	PROF. SERVICES	81,213	16,390	771		0	0%	50,000		50,000	*****
53152	FIRE SERVICES	480,155	490,286	487,540	559,000	559,000	100%	575,600		575,600	103%
53153	COPIES	16,289	458	38	110	500	22%			0	0%
53155	COMMUNITY DEVELOPMENT SER	35,813			1,000	1,000	100%	40,000		40,000	4000%
53200	ACCTG. & AUDIT.	32,189	41,488	38,828	14,998	36,750	41%	35,000		35,000	95%
54000	TRAV & PER DIEM	5,911	218			0	0%			0	0%
54100	TELEPHONE	9,095	12,966	12,737	8,842	12,100	73%	13,500		13,500	112%
54200	POSTAGE	6,299	3,714	6,885	2,211	3,500	63%	3,500		3,500	100%
54212	INSURANCE-OPEB		2,958	20,475		20,500	0%			0	0%
54300	ELECTRICITY	24,413	22,175	19,425	16,735	21,250	79%	20,500		20,500	96%
54301	WATER					6,400	0%	6,400		6,400	100%
54302	SANITATION					6,900	0%	6,900		6,900	100%
54303	SEWER					1,000	0%	1,000		1,000	100%
54401	EQUIP LEASING	2,229	914	3,295	13,381	18,100	74%	18,100		18,100	100%
54510	INS. GEN. LIAB.	183,543	215,758	218,215	234,810	235,650	100%	237,000		237,000	101%
54620	MAIN. - VEHICLE	3,189	920	2,541	1,902	2,000	95%	2,000		2,000	100%
54630	MAINT.-BLDG.	53	271			0	0%	41,000		41,000	*****
54670	MAINT. - EQUIP	10,103	11,271	11,127		0	0%			0	0%
54901	CLAIMS/SETTLEMENTS		721			0	0%			0	0%
54905	AHLF PROPERTY	19,253	22,668	24,612	26,272	26,700	98%	26,200		26,200	98%
54930	ADVERTISING	3,538	1,836	1,577		500	0%	2,000		2,000	400%
54950	EMPLOY.RELATION	6,946	10,746	8,487	8,151	8,500	96%	8,500		8,500	100%
55100	OFFICE SUPPLIES	3,441	3,402	3,070	3,276	4,500	73%	4,500		4,500	100%
55210	OPERATING SUPPL	23,282	25,796	9,084	10,877	12,100	90%	16,100		16,100	133%
55215	PLANNING & ZON.	41,585	31,366	54,068	25,428	30,100	84%	10,000		10,000	33%
55220	GASOLINE & OIL	101,907	48,756	33,579	36,506	46,500	79%	43,200		43,200	93%
55221	TOOLS		38	648	246	250	98%	650		650	260%
55235	REFUND EXP		9,475			0	0%			0	0%
55240	UNIFORMS	489	522		65	700	9%	1,200		1,200	171%
55250	CLEANING SPLIES			12		0	0%	4,500		4,500	*****
55260	PROTECT. CLOTH.					0	0%	450		450	*****
55410	MEMBERSHIPS	3,020	263			0	0%			0	0%
55420	TRAINING, AIDS	5,189	45			0	0%			0	0%
56402	CARS			500		0	0%			0	0%
56405	COMPUTER SYSTEM	43,940	132,716	154,334	166,108	166,500	100%	169,000		169,000	102%
57001	VEHICLE DEBT SERVICE			4,177	7,993	8,000	100%	8,000		8,000	100%
57100	LIBRARY	15,540	14,300	14,340	11,040	12,000	92%	15,000		15,000	125%

08/15/17
16:35:57

TOWN OF BELLEAIR
Expenditure Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 5 of 13
Report ID: B240

1 GENERAL FUND

Account	Object	----- 13-14	Actuals 14-15	----- 15-16	----- 16-17	Current Budget 16-17	% Exp. 16-17	Prelim. Budget 17-18	Budget Changes 17-18	Final Budget 17-18	% Old Budget 17-18
58001	TRANSFER OF RESERVES		7,285			800,000	0%			0	0%
58101	CAPITAL PURCH.			64,804	500	18,900	3%			0	0%
58102	TRANSFER TO 301	19,900	17,500	11,900		12,400	0%	12,400		12,400	100%
58113	TRANSFER TO 113 (TREE FUN			4,000		0	0%			0	0%
58114	TRANSFER TO 305					60,000	0%	60,000	-60,000	0	0%
58116	TRANSFER TO 402	10,684				0	0%			0	0%
	Account:	1,813,021	1,837,560	1,723,508	1,613,962	2,734,850	59%	2,093,900	-60,000	2,033,900	74%

08/15/17
16:35:57

TOWN OF BELLEAIR
Expenditure Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 6 of 13
Report ID: B240

1 GENERAL FUND

Account	Object	13-14	14-15	15-16	16-17	Current Budget 16-17	% Exp. 16-17	Prelim. Budget 17-18	Budget Changes 17-18	Final Budget 17-18	% Old Budget 17-18
521000	POLICE										
51000	INCENTIVE PAY	13,565	11,729	12,446	9,915	15,000	66%	13,000		13,000	87%
51200	SALARIES	806,878	776,768	762,777	659,506	842,500	78%	938,250		938,250	111%
51201	PT SALARIES	107,830	134,711	152,341	68,478	75,200	91%	55,200		55,200	73%
51210	Unused Medical	1,702	1,309	1,304	4,562	5,621	81%			0	0%
51400	OVERTIME	11,677	11,960	8,735	13,775	13,000	106%	13,000		13,000	100%
51500	SICK LEAVE	15,020	10,825	10,897		14,300	0%	14,300		14,300	100%
52100	FICA	73,068	72,241	72,409	57,681	73,200	79%	77,000		77,000	105%
52200	RETIREMENT-401K GENERAL P	13,280	4,816	5,916	4,919	5,850	84%	6,150		6,150	105%
52220	RETIREMENT-POLICE OFFICER	286,041	213,361	147,375		176,150	0%	181,750		181,750	103%
52300	LIFE/HOSP. INS.	82,311	77,410	74,118	59,710	91,450	65%	90,900		90,900	99%
52301	MEDICAL BENEFIT	11,619	13,656	14,103	9,616	9,479	101%	18,000		18,000	190%
52900	CODE ENFORCE.	2,789	2,598	3,553	1,798	4,000	45%	4,000		4,000	100%
53100	PHYSICAL EXAMS	1,038	1,546	559	660	1,000	66%	1,000		1,000	100%
53151	PROF. SERVICES	31,869	25,609	22,296	27,076	27,100	100%	26,100		26,100	96%
54100	TELEPHONE	8,584	5,966	6,859	5,824	7,000	83%	7,000		7,000	100%
54200	POSTAGE	853	292	704	380	800	48%	800		800	100%
54401	EQUIP LEASING	5,300	5,087	5,176	5,159	6,250	83%	6,250		6,250	100%
54510	INS. GEN. LIAB.			-44		0	0%			0	0%
54604	LOT MOWING			150	100	0	***%			0	0%
54620	MAIN. - VEHICLE	20,403	15,391	16,578	4,960	5,000	99%	5,000		5,000	100%
54650	MAINT. - RADIOS	159	4,247	11,144	4,574	4,600	99%	5,000		5,000	109%
54670	MAINT. - EQUIP	8,973	6,145	2,497	2,397	5,000	48%	5,000		5,000	100%
55100	OFFICE SUPPLIES	938	597	1,174	708	2,000	35%	2,000		2,000	100%
55209	CRIME PREVENTIO	753	239	1,392	922	1,000	92%	2,000		2,000	200%
55210	OPERATING SUPPL	5,857	10,908	18,240	17,829	19,000	94%	11,000		11,000	58%
55221	TOOLS	51		11	124	400	31%	400		400	100%
55223	TRAF CONT EQUIP			5,760		0	0%			0	0%
55240	UNIFORMS	5,399	7,614	5,313	7,275	7,800	93%	6,000		6,000	77%
55260	PROTECT. CLOTH.	7,116	2,891	100	2,067	3,200	65%	3,000		3,000	94%
55410	MEMBERSHIPS	50		15		0	0%			0	0%
55420	TRAINING, AIDS	4,878				0	0%			0	0%
56402	CARS	30,067	34,230	133,353		0	0%			0	0%
57001	VEHICLE DEBT SERVICE			11,471	23,800	23,800	100%	23,800		23,800	100%
58101	CAPITAL PURCH.		23,500	9,092		0	0%			0	0%
58102	TRANSFER TO 301	5,000		22,000		4,900	0%	4,900		4,900	100%
Account:		1,563,068	1,475,646	1,539,814	993,815	1,444,600	69%	1,520,800	0	1,520,800	105%

08/15/17
16:35:57

TOWN OF BELLEAIR
Expenditure Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 7 of 13
Report ID: B240

1 GENERAL FUND

Account	Object	13-14	14-15	15-16	16-17	Current Budget 16-17	% Exp. 16-17	Prelim. Budget 17-18	Budget Changes 17-18	Final Budget 17-18	% Old Budget 17-18
572100	PUBLIC WORKS										
51200	SALARIES	321,889	228,585	222,124	142,317	186,150	76%	352,200		352,200	189%
51210	Unused Medical	1,542	969	893	515	1,775	29%			0	0%
51400	OVERTIME		15	210		1,000	0%	850		850	85%
51500	SICK LEAVE	1,214	3,596	3,552		1,850	0%			0	0%
52100	FICA	24,192	16,650	16,124	10,000	14,550	69%	26,950		26,950	185%
52200	RETIREMENT-401K GENERAL P	27,820	20,985	20,400	10,427	14,000	74%	31,700		31,700	226%
52300	LIFE/HOSP. INS.	50,535	46,854	49,244	33,014	42,650	77%	83,800		83,800	196%
52301	MEDICAL BENEFIT	6,575	4,838	3,842	2,168	5,425	40%	10,200		10,200	188%
52500	UNEMPLOY. COMP.				3,300	7,150	46%			0	0%
53100	PHYSICAL EXAMS	639	230	100	150	400	38%	500		500	125%
53151	PROF. SERVICES		12,537	14,515	18,528	20,500	90%	16,500		16,500	80%
53153	COPIES			137		0	0%			0	0%
53160	CONTRAC. LABOR					0	0%	61,800		61,800	*****
53410	STREET SWEEPING	6,819	17,273	14,805	15,000	19,500	77%	19,500		19,500	100%
54000	TRAV & PER DIEM	924				0	0%			0	0%
54100	TELEPHONE	2,835	2,774	2,928	2,139	3,150	68%	2,050		2,050	65%
54310	ENERGY	12,830	8,768	9,479	30,322	39,250	77%	40,250		40,250	103%
54312	ENERGY-STREET LIGHT	24,548	32,046	27,555		0	0%			0	0%
54321	PATCHING MTLs.	30,379				0	0%			0	0%
54601	MAINT.-HUNTER PARK					0	0%	5,600		5,600	*****
54618	TENNIS COURTS-MAINT					0	0%	2,000		2,000	*****
54619	FIELDS/COURTS					0	0%	15,000		15,000	*****
54620	MAIN. - VEHICLE	2,798	10,334	1,991	1,270	2,000	64%	2,000		2,000	100%
54630	MAINT.-BLDG.	38,733	49,738	56,845	39,495	40,000	99%			0	0%
54640	MAINT.-AIR COND	27,769	17,555	23,969	7,871	6,000	131%			0	0%
54670	MAINT. - EQUIP	3,678	939	1,861	1,087	2,000	54%	5,000		5,000	250%
54680	MAINT.-GROUNDS					0	0%	20,000		20,000	*****
54682	TREE TRIMMING					0	0%	35,000		35,000	*****
54686	HOLIDAY LIGHTIN					0	0%	8,000		8,000	*****
54910	PLANTINGS					0	0%	4,700		4,700	*****
55100	OFFICE SUPPLIES	940	707	253	277	300	92%	800		800	267%
55210	OPERATING SUPPL	813	2,114	1,942	1,990	2,000	100%	5,500		5,500	275%
55221	TOOLS	1,653	836	469	667	800	83%	700		700	88%
55223	TRAF CONT EQUIP		1,933	3,687		0	0%			0	0%
55230	CHEMICALS					0	0%	9,500		9,500	*****
55240	UNIFORMS	2,612	1,161	1,182	1,345	1,600	84%	1,900		1,900	119%
55250	CLEANING SPLIES			4,714	4,544	5,500	83%			0	0%
55260	PROTECT. CLOTH.	1,467	903	1,496	786	900	87%	1,700		1,700	189%
55300	ROAD MATERIALS & SUPPLIES		29,722	26,809	79,711	84,200	95%	30,000		30,000	36%
55410	MEMBERSHIPS	490				0	0%			0	0%
55420	TRAINING, AIDS	2,184				0	0%			0	0%
56402	CARS	41,428		87,728		0	0%			0	0%
56405	COMPUTER SYSTEM					0	0%	500		500	*****
56568	RENOVATIONS		40,733	283,264		0	0%			0	0%
57001	VEHICLE DEBT SERVICE			9,335	18,500	18,500	100%	26,150		26,150	141%
58101	CAPITAL PURCH.	25,000		24,239		0	0%	8,100		8,100	*****
58102	TRANSFER TO 301	31,000	97,100	50,144		47,900	0%	36,550		36,550	76%
Account:		693,306	649,895	965,836	425,423	569,050	75%	865,000	0	865,000	152%

08/15/17
16:35:57

TOWN OF BELLEAIR
Expenditure Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 8 of 13
Report ID: B240

1 GENERAL FUND

Account	Object	Actuals				Current	%	Prelim.	Budget	Final	% Old
		13-14	14-15	15-16	16-17	Budget 16-17	Exp. 16-17	Budget 17-18	Changes 17-18	Budget 17-18	Budget 17-18
572200	RECREATION										
51200	SALARIES	379,265	351,059	378,819	339,038	429,800	79%	229,150		229,150	53%
51201	PT SALARIES	121,546	126,092	116,786	80,319	96,750	83%	96,750		96,750	100%
51210	Unused Medical	1,941	1,415	1,158	2,785	4,745	59%			0	0%
51400	OVERTIME	46	28	526		1,200	0%	850		850	71%
51500	SICK LEAVE	9,519	12,474	13,570		15,050	0%	12,050		12,050	80%
52100	FICA	38,863	36,885	38,617	36,684	40,400	91%	24,950		24,950	62%
52200	RETIREMENT-401K GENERAL P	33,985	32,848	35,455	29,059	38,400	76%	20,600		20,600	54%
52300	LIFE/HOSP. INS.	94,746	97,729	86,566	87,947	94,600	93%	72,800		72,800	77%
52301	MEDICAL BENEFIT	7,039	6,372	7,188	4,596	6,055	76%	6,600		6,600	109%
52400	WORKMEN'S COMP.		250	-250		0	0%			0	0%
53100	PHYSICAL EXAMS	946	1,282	873	724	750	97%	650		650	87%
53151	PROF. SERVICES	77,085	62,883	60,557	46,231	67,000	69%	60,000		60,000	90%
53153	COPIES	3,791	4,788	2,989	2,966	5,000	59%	5,000		5,000	100%
53154	FOOD SERVICE	2,116	3,368	2,742	2,994	3,000	100%	3,000		3,000	100%
53160	CONTRAC. LABOR	65,782	61,787	58,088	54,754	54,800	100%			0	0%
54000	TRAV & PER DIEM	2,748	179			0	0%			0	0%
54100	TELEPHONE	5,657	5,085	4,981	4,266	5,600	76%	4,600		4,600	82%
54300	ELECTRICITY	38,953	37,706	34,134	19,505	37,000	53%	37,000		37,000	100%
54601	MAINT.-HUNTER PARK		2,192	7,944	5,326	5,600	95%			0	0%
54618	TENNIS COURTS-MAINT	382	1,243	12,467	67	2,000	3%			0	0%
54619	FIELDS/COURTS	17,539	17,501	16,770	14,294	15,000	95%			0	0%
54670	MAINT. - EQUIP	4,716	5,484	11,571	4,563	7,000	65%	2,000		2,000	29%
54680	MAINT.-GROUNDS	17,592	16,815	15,666	19,071	20,000	95%			0	0%
54682	TREE TRIMMING	20,584	20,023	38,007	38,847	41,500	94%			0	0%
54684	PARK (HUNTER)		1,268			0	0%			0	0%
54685	TREE REPLACE.	4,583	5,978	2,231		0	0%			0	0%
54686	HOLIDAY LIGHTIN	6,767	7,768	8,822	9,494	9,500	100%			0	0%
54910	PLANTINGS	3,175	5,691	4,371	1,621	4,700	34%			0	0%
55100	OFFICE SUPPLIES	1,943	1,798	1,612	1,056	1,800	59%	1,300		1,300	72%
55210	OPERATING SUPPL	9,810	13,699	14,359	9,746	10,000	97%	6,500		6,500	65%
55218	BEAUTIFICATION	13,823	8,717			0	0%			0	0%
55221	TOOLS	447	279	529	265	500	53%	200		200	40%
55230	CHEMICALS	9,071	8,806	7,404	9,395	9,500	99%			0	0%
55231	SUMMER CAMP	18,454	17,405	16,032	17,690	19,000	93%	19,000		19,000	100%
55232	TEEN CAMP	3,415	4,264	5,207	1,686	3,650	46%	6,650		6,650	182%
55233	SPORTS LEAGUES	25,679	23,421	22,951	21,496	27,000	80%	27,000		27,000	100%
55234	SPECIAL EVENTS	139,871	127,760	136,545	125,390	123,775	101%	127,000		127,000	103%
55235	REFUND EXP	4,870	6,013	4,659	285	0	***			0	0%
55237	DAY CAMPS	1,924	2,300	2,808	2,684	3,200	84%	3,200		3,200	100%
55238	FUNKY FRIDAY	3,504	5,297	4,682	3,064	5,000	61%	5,000		5,000	100%
55239	SPECIALTY CAMPS	2,354	3,183	2,463	3,948	5,200	76%	5,200		5,200	100%
55240	UNIFORMS	1,479	1,951	1,995	962	2,500	38%	1,700		1,700	68%
55260	PROTECT. CLOTH.	1,117	892	503	664	1,250	53%	250		250	20%
55410	MEMBERSHIPS	1,821	20			0	0%			0	0%
55420	TRAINING, AIDS	10,045	16			0	0%			0	0%
56402	CARS			35,948		28,600	0%			0	0%
56405	COMPUTER SYSTEM	7,321	5,957	5,142	5,500	5,500	100%	5,000		5,000	91%

TOWN OF BELLEAIR
Expenditure Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

1 GENERAL FUND

					Current	%	Prelim.	Budget	Final	% Old	
		Actuals				Budget	Exp.	Budget	Changes	Budget	Budget
Account	Object	13-14	14-15	15-16	16-17	16-17	16-17	17-18	17-18	17-18	17-18
57001	VEHICLE DEBT SERVICE			4,001	7,650	7,650	100%			0	0%
57201	REC-VENDING	2,471	3,371	993	2,918	3,000	97%	3,000		3,000	100%
58101	CAPITAL PURCH.	26,338	12,968	29,435	43,452	73,500	59%			0	0%
58102	TRANSFER TO 301	32,500	38,050	28,650		22,150	0%	11,600		11,600	52%
	Account:	1,277,623	1,212,360	1,286,566	1,063,002	1,358,225	78%	798,600	0	798,600	59%
	Fund:	5,934,428	5,791,364	6,145,389	4,701,768	6,849,026	69%	6,040,750	-60,000	5,980,750	87%
											%

Water

08/15/17
16:33:16

TOWN OF BELLEAIR
Revenue Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 6 of 8
Report ID: B250

401 ENTERPRISE - WATER FUND

Account	13-14	14-15	15-16	16-17	Current Budget 16-17	% Rec. 16-17	Prelim. Budget 17-18	Budget Change 17-18	Final Budget 17-18	% Old Budget 17-18
337900 LOCAL GOV UNIT GRANT										
337901 WATER SUPPLY/DIST GRANT	45,713	10,575	7,713		0	0%			0	0%
Group:	45,713	10,575	7,713		0	0%	0	0	0	0%
343300 WATER UTILITY REVENUE										
343300 WATER UTILITY REVENUE	1,417,237	1,421,489	1,035,776	1,568,394	1,457,000	108%	1,480,000		1,480,000	101%
343310 WATER TAP FEES	3,800	5,370	7,908	3,175	600	529%	600		600	100%
Group:	1,421,037	1,426,859	1,043,684	1,571,569	1,457,600	108%	1,480,600	0	1,480,600	101%
361000 INTEREST										
361000 INTEREST	34	1,831			1,000	0%	1,000		1,000	100%
Group:	34	1,831			1,000	0%	1,000	0	1,000	100%
361100 INTEREST - METER DEPOSITS										
361100 INTEREST - METER DEPOSITS	22	15	8	6	0	***%			0	0%
Group:	22	15	8	6	0	***%	0	0	0	0%
365900 SALE OF SURPLUS METAL										
365900 SALE OF SURPLUS METAL		2,376	815	619	0	***%			0	0%
365901 SALE OF AUCTIONED ASSETS			29,277	-4,278	0	***%			0	0%
Group:		2,376	30,092	-3,659	0	***%	0	0	0	0%
369000 MISCELLANEOUS										
369000 MISCELLANEOUS	2,755	16,024	70	1,800	0	***%			0	0%
Group:	2,755	16,024	70	1,800	0	***%	0	0	0	0%
381000 RESERVES (PRIOR YEARS)										
381000 RESERVES (PRIOR YEARS)					39,800	0%			0	0%
Group:					39,800	0%	0	0	0	0%
381200 TRANSFER FROM 301										
381200 TRANSFER FROM 301	9,000	14,500	26,700		26,800	0%			0	0%
Group:	9,000	14,500	26,700		26,800	0%	0	0	0	0%
381400 TRANSFER FROM 001										
381402 TRANSFER FROM 403					0	0%	55,000		55,000	*****%
Group:					0	0%	55,000	0	55,000	*****%
Fund:	1,478,561	1,472,180	1,108,267	1,569,716	1,525,200	103%	1,536,600	0	1,536,600	100%

08/15/17
16:35:57

TOWN OF BELLEAIR
Expenditure Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 10 of 13
Report ID: B240

401 ENTERPRISE - WATER FUND

Account	Object	Actuals				Current	%	Prelim.	Budget	Final	% Old
		13-14	14-15	15-16	16-17	Budget 16-17	Exp. 16-17	Budget 17-18	Changes 17-18	Budget 17-18	Budget 17-18
533000	WATER										
51200	SALARIES	438,558	397,935	372,830	300,220	384,250	78%	350,350		350,350	91%
51201	PT SALARIES		160			0	0%	16,100		16,100	*****
51210	Unused Medical	1,200	1,363	429	2,059	2,854	72%			0	0%
51400	OVERTIME	1,872	2,108	1,170	1,532	8,000	19%	8,000		8,000	100%
51500	SICK LEAVE	2,986	6,339	3,715		4,750	0%	4,750		4,750	100%
52100	FICA	33,898	31,742	28,781	23,209	29,400	79%	28,650		28,650	97%
52200	RETIREMENT-401K GENERAL P	36,778	35,128	34,033	25,490	34,600	74%	31,550		31,550	91%
52300	LIFE/HOSP. INS.	76,361	76,381	76,219	63,866	81,500	78%	87,400		87,400	107%
52301	MEDICAL BENEFIT	11,789	10,908	10,803	6,998	7,646	92%	13,300		13,300	174%
53100	PHYSICAL EXAMS	230	75	70	270	300	90%	300		300	100%
53151	PROF. SERVICES	113,468	47,075	19,900	18,105	20,500	88%	11,500		11,500	56%
54000	TRAV & PER DIEM	720	2,358	1,876	727	2,500	29%	2,500		2,500	100%
54100	TELEPHONE	3,172	2,450	2,304	3,101	3,200	97%	3,200		3,200	100%
54200	POSTAGE	5,111	6,206	5,768	3,685	4,700	78%	6,000		6,000	128%
54300	ELECTRICITY	59,139	62,528	58,068	53,407	58,000	92%	60,000		60,000	103%
54301	WATER					300	0%	300		300	100%
54302	SANITATION					2,300	0%	2,300		2,300	100%
54303	SEWER					200	0%	200		200	100%
54315	PIN. CTY. WATER	8,394	13,496	14,274	18,113	20,700	88%	15,000		15,000	72%
54400	EQUIP. RENTAL	112			2,203	2,750	80%	2,750		2,750	100%
54614	MAINT. - METERS	31,095	103,299	52,387	28,245	31,600	89%	31,600		31,600	100%
54620	MAIN. - VEHICLE	8,363	2,325	4,271	5,004	6,000	83%	4,000		4,000	67%
54630	MAINT.-BLDG.	11,822	10,471	5,340	4,097	6,000	68%	8,000		8,000	133%
54670	MAINT. - EQUIP	23,131	19,053	11,177	9,326	15,000	62%	5,000		5,000	33%
54900	BAD DEBT					400	0%	400		400	100%
55100	OFFICE SUPPLIES	2,832	1,419	2,126	2,330	2,500	93%	2,500		2,500	100%
55210	OPERATING SUPPL	5,213	4,738	5,834	6,422	7,800	82%	7,800		7,800	100%
55213	LABORATORY TEST	16,295	14,415	14,089	17,821	18,200	98%	18,200		18,200	100%
55214	LAB SUPPLIES	7,545	6,040	2,597	7,424	8,100	92%	8,100		8,100	100%
55220	GASOLINE & OIL		7,647	7,080	5,985	7,000	86%	7,500		7,500	107%
55221	TOOLS	2,006	1,339	2,148	1,476	2,000	74%	2,000		2,000	100%
55230	CHEMICALS	13,647	18,493	19,759	22,444	22,450	100%	22,450		22,450	100%
55235	REFUND EXP		219			0	0%			0	0%
55240	UNIFORMS	1,668	1,499	1,576	1,407	1,500	94%	1,500		1,500	100%
55260	PROTECT. CLOTH.	1,437	1,688	1,923	2,275	2,500	91%	2,500		2,500	100%
55410	MEMBERSHIPS	1,377	1,394	2,043	1,507	2,000	75%	2,000		2,000	100%
55420	TRAINING, AIDS	3,835	1,788	4,129	3,813	4,000	95%	4,000		4,000	100%
56402	CARS	32,883	32,200		61,756	61,800	100%			0	0%
56405	COMPUTER SYSTEM	2,507	500	13,221	13,043	13,250	98%	13,250		13,250	100%
56491	EQUIP. REPLACE.	4,893				0	0%			0	0%
57301	MISCELLANEOUS	6,912	7,425	4,456	7,017	7,200	97%	7,200		7,200	100%
58001	TRANSFER OF RESERVES					120,350	0%	74,900		74,900	62%
58101	CAPITAL PURCH.			3,702	26,841	32,500	83%	138,000		138,000	425%
58102	TRANSFER TO 301	38,000	36,700	24,600		33,400	0%			0	0%
58115	TRANSFER TO 001			14,700		0	0%			0	0%
59200	REPAY-LOAN-GF					0	0%	40,000		40,000	*****
59900	DEPRECIATION					127,500	0%	127,500		127,500	100%

08/15/17
16:35:57

TOWN OF BELLEAIR
Expenditure Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 11 of 13
Report ID: B240

401 ENTERPRISE - WATER FUND

Account	Object	----- 13-14	----- 14-15	----- 15-16	----- 16-17	Current Budget 16-17	% Exp. 16-17	Prelim. Budget 17-18	Budget Changes 17-18	Final Budget 17-18	% Old Budget 17-18
59904	FEES-SPT SERVIC	243,500	264,600	274,300		242,100	0%	275,300		275,300	114%
59906	FEES-PUB. WORKS	30,300	38,450	39,100		81,600	0%	88,750		88,750	109%
59907	FEES-MECHANICAL	32,500				0	0%			0	0%
	Account:	1,315,549	1,271,954	1,140,798	751,218	1,525,200	49%	1,536,600	0	1,536,600	101%
	Fund:	1,315,549	1,271,954	1,140,798	751,218	1,525,200	49%	1,536,600	0	1,536,600	101%

Solid Waste

08/15/17
16:33:16

TOWN OF BELLEAIR
Revenue Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 7 of 8
Report ID: B250

402 ENTERPRISE - SOLID WASTE/RECYCLING											
Account	Actuals				Current	%	Prelim.	Budget	Final	% Old	
	13-14	14-15	15-16	16-17	Budget 16-17	Rec. 16-17	Budget 17-18	Change 17-18	Budget 17-18	Budget 17-18	

337300 RECYC GRANT (STATE OF FLORIDA)											
337300 RECYC GRANT (STATE OF	3,004	2,978	2,941	2,900	3,000	97%	3,000	_____	3,000	100%	
Group:	3,004	2,978	2,941	2,900	3,000	97%	3,000	0	3,000	100%	
343400 SANITATION											
343400 SANITATION	801,112	788,562	551,332	694,321	825,900	84%	805,000	_____	805,000	97%	
343401 PERMIT-ROLL OFF CONTAINER	1,150	950	1,000	950	500	190%	500	_____	500	100%	
Group:	802,262	789,512	552,332	695,271	826,400	84%	805,500	0	805,500	97%	
361000 INTEREST											
361000 INTEREST	31	1,831			500	0%	500	_____	500	100%	
Group:	31	1,831			500	0%	500	0	500	100%	
364000 GAIN ON SALE OF FIXED ASSETS											
364000 GAIN ON SALE OF FIXED					10,000	0%	60,000	_____	60,000	600%	
Group:					10,000	0%	60,000	0	60,000	600%	
365900 SALE OF SURPLUS METAL											
365900 SALE OF SURPLUS METAL			134		0	0%	_____	_____	0	0%	
Group:			134		0	0%	0	0	0	0%	
369000 MISCELLANEOUS											
369000 MISCELLANEOUS	626	2,414	1,240	899	0	***%	_____	_____	0	0%	
Group:	626	2,414	1,240	899	0	***%	0	0	0	0%	
381000 RESERVES (PRIOR YEARS)											
381000 RESERVES (PRIOR YEARS)					98,900	0%	150,000	_____	150,000	151%	
Group:					98,900	0%	150,000	0	150,000	151%	
381200 TRANSFER FROM 301											
381200 TRANSFER FROM 301		12,000	125,700		100,500	0%	_____	_____	0	0%	
Group:		12,000	125,700		100,500	0%	0	0	0	0%	
381400 TRANSFER FROM 001											
381400 TRANSFER FROM 001	10,684				0	0%	_____	_____	0	0%	
Group:	10,684				0	0%	0	0	0	0%	
Fund:	816,607	808,735	682,347	699,070	1,039,300	67%	1,019,000	0	1,019,000	98%	

08/15/17
16:35:57

TOWN OF BELLEAIR
Expenditure Budget Report -- MultiYear Actuals
For the Year: 2017 - 2018

Page: 12 of 13
Report ID: B240

402 ENTERPRISE - SOLID WASTE/RECYCLING

Account	Object	----- 13-14	14-15	Actuals 15-16	16-17	Current Budget 16-17	% Exp. 16-17	Prelim. Budget 17-18	Budget Changes 17-18	Final Budget 17-18	% Old Budget 17-18
534000	SOLID WASTE MANAGEMENT/RECYCLING										
51200	SALARIES	195,195	189,337	191,742	165,032	207,000	80%	225,600		225,600	109%
51201	PT SALARIES	3,354		1,052		0	0%			0	0%
51210	Unused Medical	210	93	396	2,579	2,623	98%			0	0%
51400	OVERTIME	3,040	1,857	2,501	2,144	2,500	86%	2,500		2,500	100%
51500	SICK LEAVE	2,315	2,200	775		950	0%			0	0%
52100	FICA	15,499	14,274	14,696	12,905	15,800	82%	17,250		17,250	109%
52200	RETIREMENT-401K GENERAL P	18,028	16,279	16,619	12,849	18,650	69%	20,300		20,300	109%
52300	LIFE/HOSP. INS.	34,807	41,529	41,352	40,477	48,050	84%	58,600		58,600	122%
52301	MEDICAL BENEFIT	5,801	5,170	5,174	3,306	4,277	77%	7,800		7,800	182%
53100	PHYSICAL EXAMS	1,930	263	813	373	500	75%	500		500	100%
53151	PROF. SERVICES	2,110		600		0	0%			0	0%
53160	CONTRAC. LABOR	7,626	2,705	8,990	4,962	5,000	99%	5,050		5,050	101%
54000	TRAV & PER DIEM		74			100	0%			0	0%
54100	TELEPHONE	1,264	744	706	456	1,450	31%	1,450		1,450	100%
54200	POSTAGE	5,375	5,585	5,651	3,807	5,000	76%	5,000		5,000	100%
54340	GAR. & TRA DIS.	106,938	103,404	113,838	104,291	122,400	85%	125,400		125,400	102%
54342	RECYCLING	75,471	83,000	84,578	73,098	80,000	91%	60,250		60,250	75%
54620	MAIN. - VEHICLE	31,925	20,683	20,347	19,201	25,000	77%	20,000		20,000	80%
54630	MAINT.-BLDG.	121	142	1,714		0	0%			0	0%
54670	MAINT. - EQUIP	10,369	171	104	317	1,200	26%	2,500		2,500	208%
54900	BAD DEBT					500	0%	500		500	100%
55100	OFFICE SUPPLIES	484	153	142	26	500	5%	500		500	100%
55210	OPERATING SUPPL	17,386	7,410	5,275	5,960	6,500	92%	6,500		6,500	100%
55220	GASOLINE & OIL		14,399	11,723	11,969	16,000	75%	16,000		16,000	100%
55221	TOOLS	303	173			300	0%	300		300	100%
55240	UNIFORMS	1,408	1,575	2,091	586	2,350	25%	2,350		2,350	100%
55260	PROTECT. CLOTH.	1,667	1,682	975	916	2,350	39%	2,350		2,350	100%
55410	MEMBERSHIPS		200	302		0	0%			0	0%
55420	TRAINING, AIDS	356	665	694	693	1,000	69%			0	0%
56402	CARS		110,200	146,868		150,000	0%	150,000		150,000	100%
56405	COMPUTER SYSTEM		9		1,200	1,200	100%	1,200		1,200	100%
58101	CAPITAL PURCH.	92,591				0	0%			0	0%
58102	TRANSFER TO 301	88,500	67,000	86,500		85,000	0%			0	0%
59900	DEPRECIATION					51,000	0%	77,500		77,500	152%
59904	FEES-SPT SERVIC	117,900	145,550	150,850		136,200	0%	158,500		158,500	116%
59906	FEES-PUB. WORKS	20,100	21,150	21,500		45,900	0%	51,100		51,100	111%
59907	FEES-MECHANICAL	32,500				0	0%			0	0%
Account:		894,573	857,676	938,568	467,147	1,039,300	45%	1,019,000	0	1,019,000	98%
Fund:		894,573	857,676	938,568	467,147	1,039,300	45%	1,019,000	0	1,019,000	98%

Capital Projects

Project #	Column2	Revenues	ACTUAL 15/16	Assumed 16/17	17/18	18/19	19/20	20/21	21/22	22/23	23/24	24/25	25/26	26/27	27/28	28/29	29/30	30/31
311100		Infrastructure Mill	\$ 603,308	\$ 627,300	\$ 678,200	\$ 691,750	\$ 705,600	\$ 719,700	\$ 734,100	\$ 748,800	\$ 763,800	\$ 779,100	\$ 794,700	\$ 810,600	\$ 826,800	\$ 843,350	\$ 860,200	\$ 877,400
312600		Penny	\$ 398,838	\$ 455,000	\$ 485,100	\$ 494,800	\$ 504,700	\$ 514,800	\$ 525,100	\$ 535,600	\$ 546,300	\$ 557,250	\$ 568,400	\$ 579,750	\$ 591,350	\$ 603,200	\$ 615,250	\$ 627,550
314100		Electric Utility Tax	\$ 437,310	\$ 400,000	\$ 430,000	\$ 430,000	\$ 430,000	\$ 430,000	\$ 430,000	\$ 430,000	\$ 430,000	\$ 430,000	\$ 430,000	\$ 430,000	\$ 430,000	\$ 430,000	\$ 430,000	\$ 430,000
334102		Grant SWFWMD	\$ 708,141	\$ 599,859	\$ 1,375,000	\$ 580,000	\$ 580,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
337902		Stormwater Management Grant																
341903		Intergov.Services Rendered		\$ 60,000														
343600		Stormwater Fee	\$ 337,364	\$ 337,400	\$ 337,400	\$ 337,400	\$ 337,400	\$ 337,400	\$ 337,400	\$ 337,400	\$ 337,400	\$ 337,400	\$ 337,400	\$ 337,400	\$ 337,400	\$ 337,400	\$ 337,400	\$ 337,400
361000		Interest	\$ 127															
366913		Donations	\$ 3,811															
369000		Miscellaneous	\$ 72															
381000		Reserves Prior Years	\$ -		\$ 2,058,925			\$ 23,100	\$ 684,025									
381210		Transfer From 01	\$ 60,300	\$ 140,000														
381400		Transfer From 001																
381402		Transfer From 403																
381406		Transfer From 113																
381407		Transfer From 115 (GOLF)	\$ 97,000	\$ 3,960,614		\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
384010		Loan Proceeds	\$ -		\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
			\$ 2															
		Totals	\$ 2,646,272	\$ 6,580,173	\$ 5,364,625	\$ 2,533,950	\$ 2,557,700	\$ 2,025,000	\$ 2,710,625	\$ 2,051,800	\$ 2,077,500	\$ 2,103,750	\$ 2,130,500	\$ 2,157,750	\$ 2,185,550	\$ 2,213,950	\$ 2,242,850	\$ 2,272,350
				\$ (2,406,173)														
		Expenditures			17/18	18/19	19/20	20/21	21/22	22/23	23/24	24/25	25/26	26/27	27/28	28/29	29/30	30/31
53140		Engineering			\$ -													
53151		Professional Services																
		Capital Programs																
54683		Park Improvements	\$ 24,968	\$ 16,858	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000
54684		Hunter Park	\$ 4,750															
54920		Master Landscape Plan																
54921		Pavement Management	\$ 7,700															
55201		Beautification & Entrances																
55223		Street Signs	\$ 4,085	\$ 3,742														
55235		Refund Exp																
56719		Small Roadway Projects	\$ 120,214	\$ 108,430	\$ 180,000	\$ 205,500	\$ 216,500	\$ 242,500	\$ 247,500	\$ 247,500	\$ 268,100	\$ 273,600	\$ 283,600	\$ 286,436	\$ 100,000	\$ 100,000	\$ 100,000	\$ 100,000
56304		Street Light Replacement	\$ 142,062	\$ 48,945	\$ 250,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000	\$ 25,000
56305		Indian Rocks Road	\$ 13,098	\$ 4,363														
56306		Orlando																
		Capital Parks			\$ 50,000	\$ 100,000	\$ -	\$ -	\$ -	\$ -	\$ 25,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
	Priority	Projects Years 1-5																
56302	X	Pinellas/Ponce	\$ 5,025	\$ 18,475	\$ 2,731,525	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
56517	X	Rosery Rd	\$ 1,074,542	\$ 2,627,258	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
56524		Belleair Creek																
56731	X	Harold's Lake Cleanout		\$ 18,799	\$ 155,000	\$ -	\$ -	\$ -	\$ -	\$ 175,000	\$ -	\$ -	\$ -	\$ -	\$ 175,000	\$ -	\$ -	\$ -
54603	14	Palmetto		\$ 50,292	\$ 609,700	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
	14	Carl			\$ 600,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
56502	11	Belforest			\$ 50,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
56301	14	Bayview Bridge to IRR	\$ 1,727,354	\$ 381,493	\$ -	\$ 1,161,000	\$ 1,161,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
	16/13/8	Shirley/Varona/Sunny			\$ -	\$ 31,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
	12	IRR Poinsettia to Melenbacher			\$ -	\$ 200,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 767,000	\$ 767,000
	14/13	Ponce from Roundabout to Trail			\$ -	\$ -	\$ -	\$ 1,017,500	\$ 1,017,500	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
56554		Projects Years 6-10		\$ 4,875														
	17/15	The Mall/Gardenia			\$ -	\$ -	\$ -	\$ -	\$ 680,625	\$ 680,625	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
56709	14*	Osceola East of IRR			\$ -	\$ -	\$ -	\$ -	\$ -	\$ 525,000	\$ 525,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
	12	IRR Bayview to Belleview			\$ -	\$ -	\$ -	\$ -	\$ -	\$ 179,160	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 676,000	\$ 676,000
	12	Ponce from Manatee to Oleander			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 1,007,050	\$ 1,007,050	\$ -	\$ -	\$ -	\$ -	\$ -
	11/12	Wildwood/Woodlawn			\$ -	\$ -	\$ -	\$ -	\$ -	\$ 182,488	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
56701	12	IRR Hunter Bayview to Poinsettia			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 650,925	\$ 650,925	\$ -	\$ -	\$ -
56303	12	Poinsettia			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 47,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
	12	Osecola from Oleander to Manatee	\$ 393,275		\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 372,075	\$ 372,075	\$ -
56569		Streets-Intersection Improvement			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -				
56581		Curbs/Sidewalks	\$ 78,976	\$ 50,650	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -				
56600		Drainage			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -				
56606		Manatee			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -				
56708		Oleander			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -				
56730		Belleview			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -				
56732		Druid			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -				
56734		Orange Ave/Fairview			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -				
56736		PW Building			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -				
56737		Golf Course Purchase			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -				
	11	Ponce from Manatee to Rosery			\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 797,500	\$ 797,500	\$ -	\$ -
		Other Expenses																
58001		Transfer to Reserves			\$ -	\$ 71,450	\$ 415,200											
58110		Transfer to 401																
58119		BB&T Debt Service	\$ 697,012	\$ 715,000	\$ 713,400	\$ 715,000	\$ 715,000	\$ 715,000	\$ 715,000	\$ 715,000	\$ 715,000	\$ 715,000	\$ 715,000	\$ 715,000	\$ 715,000	\$ 715,000	\$ 715,000	\$ 715,000
58115		GF Debt Service	\$ 150,000	\$ 135,000						\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
		Totals	\$ 4,443,061	\$ 4,184,179	\$ 5,364,625	\$ 2,533,950	\$ 2,557,700	\$ 2,025,000	\$ 2,710,625	\$ 2,047,285	\$ 1,765,588	\$ 2,617,650	\$ 2,055,650	\$ 1,702,361	\$ 2,488,425	\$ 2,034,575	\$ 2,680,075	\$ 2,308,000
			\$ (1,796,788)	\$ 2,395,994	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 4,515	\$ 311,912	\$ (513,900)	\$ 74,850					
		Fund Balance			17/18	18/19	19/20	20/21	21/22	22/23	23/24	24/25	25/26	26/27	27/28	28/29	29/30	30/31
		Exp	\$ 4,443,061	\$ 4,184,179	\$ 5,364,625	\$ 2,462,500	\$ 2,142,500	\$ 2,025,000	\$ 2,710,625	\$ 2,047,285	\$ 1,765,588	\$ 2,617,650	\$ 2,055,650	\$ 1,702,361	\$ 2,488,425	\$ 2,034,575	\$ 2,680,075	\$ 2,308,000
		Rev	\$ 2,646,272	\$ 6,580,173	\$ 3,305,700	\$ 2,533,950	\$ 2,557,700	\$ 2,001,900	\$ 2,026,600	\$ 2,051,800	\$ 2,077,500	\$ 2,103,750	\$ 2,130,500	\$ 2,157,750	\$ 2,185,550	\$ 2,213,950	\$ 2,242,850	\$ 2,272,350
		Change in FB	\$ (1,796,788)	\$ 2,395,994	\$ (2,058,925)	\$ 71,450	\$ 415,200	\$ (23,100)	\$ (684,025)	\$ 4,515	\$ 311,912	\$ (513,900)	\$ 74,850	\$ 455,389	\$ (302,875)	\$ 179,375	\$ (437,225)	\$ (35,650)
		Fund Balance	\$ 2,254,603	\$ 4,650,597	\$ 2,591,672	\$ 2,663,122	\$ 3,078,322	\$ 3,055,222	\$ 2,371,197	\$ 2,375,712	\$ 2,687,624	\$ 2,173,724	\$ 2,248,574	\$ 2,703,963	\$ 2,401,088	\$ 2,580,463	\$ 2,143,238	\$ 2,107,588