# IT Policy Manual

The IT manual establishes and states the policies governing The Company's IT standards and practices. These policies define management's arrangements for managing operations and activities in accordance with computer industry practices. These top-level policies represent the plans or protocols for achieving and maintaining the confidentiality, integrity and availability of all IT Assets.

[This page intentionally left blank]

**<Company Logo>**

# <Our Company, Inc.>

# IT Policy Manual

**mm dd yyyy**

Approved By _____ Date: _____

President/CEO

This manual is intended for the sole use of Our Company, Inc., and parts may be provided to outside parties for informational purposes only.

© 20nn Our Company, Inc.

The contents of this manual may not be reproduced or reprinted, in whole or in part, without the express written permission of Our Company, Inc.

The following document contains a sample IT policy manual covering the common IT requirements and practices. This sample is intended only to provide an example of wording that might be used in an IT manual.

This sample wording can be helpful in generating ideas for developing a manual for your own company. However, IT policies should be drafted, as appropriate and necessary, in a way that accurately reflects Our Company's IT standards and requirements.

# Information Technology Policy Manual

Table of Contents

## TABLE OF FIGURES

## LIST OF REFERENCED PROCEDURES

IT Administration

1. ITAD101 Information Technology Management
2. ITAD102 IT Records Management
3. ITAD103 IT Document Management
4. ITAD104 IT Device Naming Conventions
5. ITAD105 TCP/IP Implementation Standards
6. ITAD106 Network Infrastructure Standards
7. ITAD107 Computer and Internet Usage Policy
8. ITAD108 Email Policy
9. ITAD109 IT Outsourcing
10. ITAD110 IT Department Satisfaction
11. ITAD111 BYOD Policy

IT Asset Management

1. ITAM101 IT Asset Standards
2. ITAM102 IT Asset Management
3. ITAM103 IT Vendor Selection
4. ITAM104 IT Asset Assessment
5. ITAM105 IT Asset Installation Satisfaction

IT Training and Support

1. ITTS101 IT System Administration
2. ITTS102 IT Support Center
3. ITTS103 IT Server/Network Support
4. ITTS104 IT Troubleshooting
5. ITTS105 IT User-Staff Training Plan

IT Security and Disaster Recovery

1. ITSD101 IT Threat And Risk Assessment
2. ITSD102 IT Security Plan
3. ITSD103 IT Media Storage
4. ITSD104 IT Disaster Recovery
5. ITSD105 Computer Malware
6. ITSD106 IT Access Control
7. ITSD107 IT Security Audits
8. ITSD108 IT Incident Handling

Software Development

1. ITSW101 IT Project Definition
2. ITSW102 IT Project Management
3. ITSW103 Systems Analysis
4. ITSW104 Software Design
5. ITSW105 Software Programming
6. ITSW106 Software Documentation

## 1.0 PURPOSE

The purpose of this Information Technology (IT) manual is to define, develop, and document the information policies and procedures that support organizational goals and objectives.

The policies and procedures provide:

- A foundation for a system of internal controls;
- Guidance in current Computer and Network activities;
- Criteria for decisions on appropriate IT security; and
- IT officers with direction and guidance in connection with those IT policies, procedures, and reports that should be uniform throughout the Company.

Information security policies and procedures represent the foundation for The Company's information security program. Information security policies serve as overarching guidelines for the use, management, and implementation of information security throughout the organization.

Internal controls provide a system of checks and balances intended to identify irregularities, prevent waste, fraud and abuse from occurring, and assist in resolving discrepancies that are accidentally introduced in the operations of the business.

When consistently applied throughout the Company, these policies and procedures assure that the information assets are protected from a range of threats in order to ensure business continuity and maximize the return on investments of business interests.

All additional departmental or functional policies and procedures written should conform to and parallel the policies in this manual. All changes to policies and procedures are required to be reviewed to ensure that there are no conflicts with the policies stated in this IT Policy Manual.

[This page intentionally left blank]

## 2.0 SCOPE

The IT Policy Manual is an official directive of the President. It is published and maintained by the Chief Information Officer (CIO) as part of the general responsibility for Company IT policy assigned to the IT office.

The policies stated in this manual apply to all operations and activities at Our Company. The attendant IT procedures serve to define the operational steps and practices that should be followed in order to support the organization's approach to IT management as defined by the policy statements.

## 2.1 RESPONSIBILITY

Department Managers. It is the responsibility of all department managers to help implement and maintain the procedures required by this manual and to ensure all processes conform to these requirements.

All Employees. It is the responsibility of all employees to follow procedures that implement these policies and to help strive for continuous improvement in all activities and processes of Our Company.

All Users. The goal is to make the Manual as clear and useful as possible. All users are encouraged to contact the Company CIO with any suggestions for revising or improving the Manual.

## 2.2 EXCLUSIONS

### 2.2.1 Security Planning

Some IT-related security planning functions are included with the IT manual. Additional information on *physical* security planning information is included with ABR32, ***Bizmanualz® Security Planning Policies and Procedures Manual***.

### 2.2.2 Disaster Recovery

Some IT-related disaster recovery functions are included with this IT manual. Additional information on *physical* disaster recovery is available in ABR33, ***Bizmanualz® Disaster Recovery Policies and Procedures Manual***.

### 2.2.3 Accounting

Accounting functions are not included with this manual but are available in ABR31, ***Bizmanualz® Accounting Policies and Procedures Manual***.

### 2.2.4 Human Resources

Human resources functions are not included with this manual but are available in ABR41 ***Bizmanualz® Human Resources Policies and Procedures Manual***.

[This page intentionally left blank]

## 3.0 MANAGEMENT RESPONSIBILITY

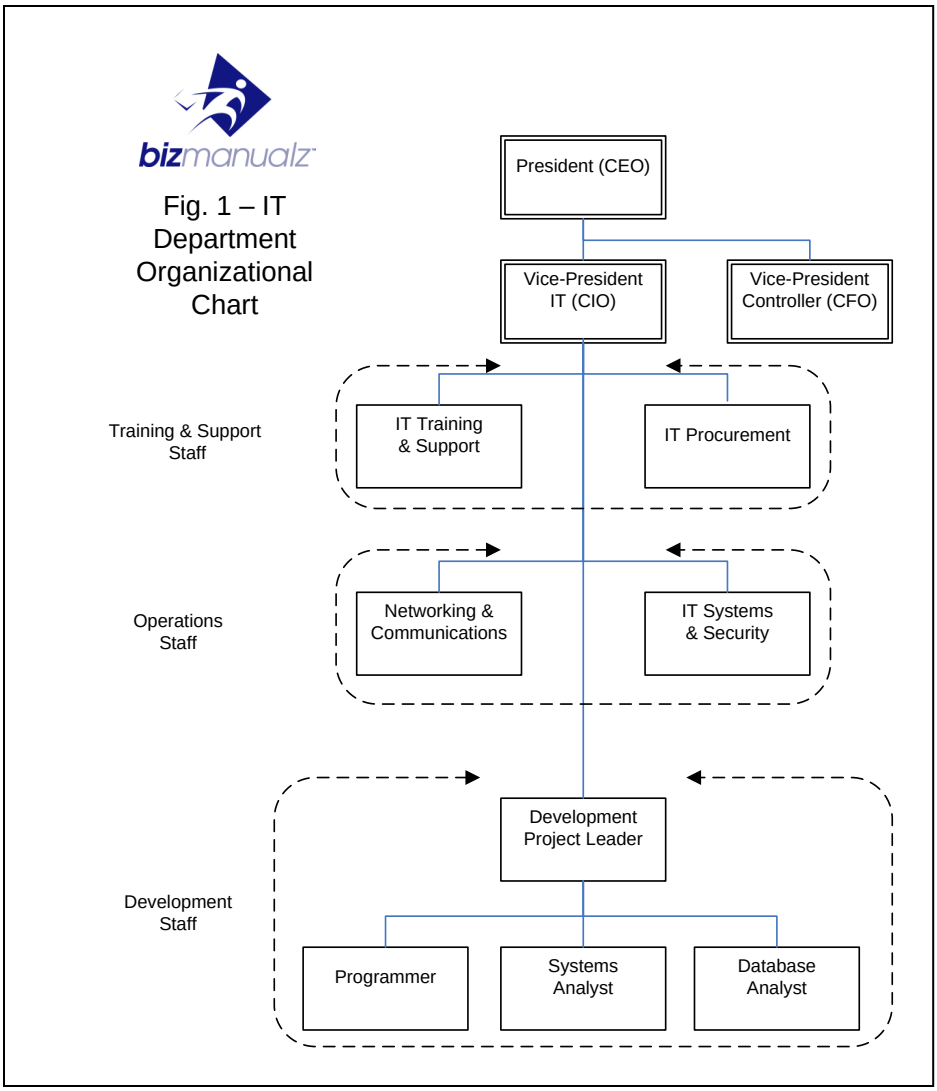
The IT department is headed by the Chief Information Officer (CIO), who is responsible for all IT functions.

## 3.1 IT ORGANIZATION

The IT department is organized into three main responsibilities, or functions: Training and Support; Operations; and Software Development.

### 3.1.1 IT Department Organizational Chart

The company's organizational framework is the foundation for coordinating and administrating IT systems and services. A description of the roles and responsibilities applicable to the IT staff are provided. Responsibilities specific to certain procedures or tasks are presented in the related procedures.



(Note: The actual Organization Chart may vary in detail, based on the size of the department or organization involved and the type of activity performed. In a smaller company, the CIO may be an IT Manager reporting to the CFO.)

### 3.1.2 CIO Responsibilities

The Chief Information Officer (CIO) provides the vision and leadership for developing and implementing Information Technology (IT) initiatives that improve cost effectiveness and service quality. The CIO directs the IT security and control functions to ensure the integrity of all information assets.

The CIO leads the company in implementing IT systems through strategies, plans, programs and services to support both distributed and centralized business operations. The CIO ensures appropriate technology is deployed to support the organizations objectives and reports on the results of operations. The CIO is accountable to the President and supervises the IT staff.

Major Duties And Responsibilities:

- Develops and implements IT policies, coordination of processes and procedures, and the preparation of operating data and special reports as required.
- Develops and maintains IT systems architecture defining standards and protocols for data exchange, communications, software, and interconnections.
- Establishes, coordinates and administers as an integral part of management, an adequate plan for the control of operations including IT training, technical support, and software development, together with necessary controls and procedures to effectuate the plan.
- Provides advice on evaluation, selection, implementation and maintenance of information systems, ensuring appropriate investment in strategic and operational systems. Negotiates all IT acquisition contracts, soliciting involvement and participation of other management team members as appropriate.
- Ensures that enterprise information systems operate according to internal standards, external accrediting agency standards, and legal requirements.
- In conjunction with the President, coordinates IT reviews and endorses strategic IT plans, budget proposals, and proposed changes.
- Ensures appropriate training programs are in place to attract, retain and develop the key personnel required to support information services. Ensures all personnel are appropriately trained in the usage of all IT products and services in order to effectively carry out their job.
- Assures protection for the information assets of the business through internal control, internal auditing, IT security, recovery procedures and assuring proper insurance coverage.
- Develops and maintains a business IT recovery plan to ensure timely and effective restoration of IT services in the event of a disaster.
- Provides advice on all technology matters to the President.

### 3.1.3 Training and Support

Training and Support responsibilities are focused on providing assistance to personnel in the field that use all of the computer hardware, software and IT services.

The Training and Support staff consists of the following positions:

- Training and Support Manager – Directs and organizes all general IT training activities for both the IT staff and company personnel. Prepares IT assessments and satisfaction surveys and reports. Reports directly to the CIO. Coordinates activities with all departments; works closely with IT Support
- Technical Support – Installs, tests, troubleshoots, and maintains hardware and software; implements and monitors PC standards and procedures; facilitates backup and recovery; maintains service logs security incident reports; coordinates vendor updates; provides technical guidance and training to end-users; monitors problem/change activities and coordinates the involvement of staff, clients, and vendors to ensure effective resolution of user problems. Reports directly to the Training and Support Manager. Assists in supervision of support staff. Works closely with IT Training, Development, and Operations.
- IT Procurement – Responsible for purchasing all IT tools, supplies and assets for the company including negotiating price, delivery and credit terms. Evaluates vendors and determines most cost-effective supplies inventory and reorder levels. Reports to the CIO. Coordinates activities with all departments; works closely with IT Operations.

### 3.1.4 Operations Staff Responsibilities

Operations staff responsibilities are focused on diligently maintaining the computer systems, software and hardware of the company to ensure the availability of disk space, response time, and information security.

The operations staff consists of the following positions:

- Network Communications – Designs and tests data communications networks; designs, configures, and implements LAN/WAN hardware, software, and ancillary services for network operating efficiency; assists in router installation, software upgrade, and connections to Internet and telecommunications; develops methods and criteria for network data collections and analysis; ensures network operating problems are resolved; maintains network security and sets up firewalls; maintains and monitors WAN networks; Reports directly to the CIO.
- IT Systems & Security – Installs, customizes, and maintains operating systems software; evaluates operating efficiency and analyzes performance and tuning; makes modifications to tuning parameters to improve performance; Implements and monitor policies and procedures for security and disaster recovery; implements and monitors security audit

logs and access control practices to ensure adherence to policies and procedures. Reports directly to the CIO.

### 3.1.5 Development Responsibilities

The company focuses development staff responsibilities on creating, editing, and maintaining the custom software application in use.

The Development staff consists of the following positions:

- **Project Leader** – Responsible for developing project management plans and coordinating the application development with the CIO and subordinates. Reports directly to CIO. Supervises programmer, system analyst, and database analyst. Works with training, technical support and operations.
- **Programmer/Analyst** – Designs software applications writing in one or more commonly used programming languages or 4th generation languages appropriate for multi-user/multi-tasking environments; writes program documentation in accordance with published standards. Reports directly to the Project Leader.
- **Systems Analyst** – Develops system proposals and cost-benefit analyses; designs application systems ensuring design specifications and documentation meet published standards; prepares illustrative output for review and approval; approves development of logical database design; prepares system flowcharts, logic, and data management descriptions; develops program and system specifications; conducts system tests. Works with users to define IT requirements. Reports directly to the Project Leader.
- **Database Analyst** – Designs, develops, installs, and tests database systems; assures compatibility and efficiency of database applications through ongoing system monitoring and evaluation; prepares and updates data models and develops standards for updating the data dictionary; develops security requirements for all on-line applications. Reports directly to the Project Leader.

## 3.2 MANAGEMENT COMMITMENT

Top Management at Our Company shows its commitment to the IT management system through the development and implementation of this IT Policy Manual. Additionally, management commitment is demonstrated through the Company IT Policy, the specific objectives that are set and reviewed during Management Review Meetings, and by providing the resources required to meet our objectives for continually improving the effectiveness of our operations and IT system.

The management team consisting of the President and all department managers is chartered with ensuring our IT management system meets customer, as well as statutory and regulatory, requirements

## 3.3 MANAGEMENT IT POLICY

Our Company has established an IT Policy Manual that we feel is appropriate to our organization, meets the practices set forth by IEEE and ISO for information systems, and complies with all statutory and regulatory requirements. We accomplish this by adhering to our IT Management System and use operational methods as documented in our IT Policy Manual

This policy is communicated throughout the company. Department managers and supervisors are responsible for ensuring all employees understand the policy. To ensure our policy remains appropriate, it is reviewed at least annually at one of our Management Review meetings.

The Company IT Policy:

- We strive to continually improve the effectiveness of our IT Management System by monitoring our performance against our established objectives and through leadership that promotes employee involvement. This concept represents Our Company's commitment to quality IT and the increasing need to better serve our customers, shareholders, and employees.
- It is Company policy to safeguard and secure all information assets in accordance with industry-accepted standards and guidelines; for example, ISO/IEC 27002:2013, "Information Technology - Security Techniques - Code of Practice for Information Security Management", ISO/IEC 27001:2013, "Information technology - Security techniques - Information security management systems – Requirements", and ISO/IEC 27005:2011, "Information Technology Security Techniques Information Security Risk Management".
- It is Company policy to design and produce software that conforms to IEEE Standard #1058-1998, "Standards for Software Project Management Plans" and the data requirements of ISO/IEC 12207:2008, "Systems and Software Engineering - Software Life Cycle Processes".

## 3.4 PLANNING

### 3.4.1 IT Objectives

Our Company shall establish objectives on an annual basis. These objectives shall be measurable and consistent with the IT Policy, and reviewed at least annually at Management Review meetings.

### 3.4.2 IT System Planning

As part of annual strategic planning meetings, Our Company establishes strategic objectives and goals. These objectives are supported by specific measures that track performance against those objectives using the budgeting process. IT managers in turn set IT objectives with specific performance measures and targets that support the company objectives.

As situations arise that demand changes to the IT systems, either to meet objectives or because of changing business conditions, all changes will be

reviewed by the management team to ensure the integrity of the IT systems are maintained.

## 3.5 RESPONSIBILITY, AUTHORITY, AND COMMUNICATION

### 3.5.1 Responsibility and Authority

Responsibilities and authorities at Our Company are defined in each Job Description. Job Descriptions are posted on the company intranet and are also used during annual performance reviews.

### 3.5.2 Management Representative

The President has appointed the CIO as the Management Representative with the responsibility and authority to:

a) Ensure that processes needed for IT Management are established, implemented and maintained.

b) Report to top management on the performance of the IT Systems and any need for improvement.

c) Ensure the promotion of awareness of IT requirements throughout the organization.

d) Serve as the liaison with external parties on matters relating to the IT Management System.

### 3.5.3 Internal Communication

In line with Our Company's policy of leadership through employee involvement, Our Company's personnel policies have been designed to establish and promote open communication throughout the organization.

The effectiveness of our IT Management System is evident through Internal Audit results, Management Reports, department satisfaction and departmental performance measures. Other than confidential information, company and departmental performance measures are posted on bulletin boards throughout Our Company. Internal Audit results are shared at departmental meetings, as appropriate.

### 3.5.4 Referenced Procedures:

ITAD101 – Information Technology Management
ITSD107 – IT Security Audits
ITSW102 – IT Project Management
ITAD110 – IT Department Satisfaction

## 3.6 MANAGEMENT REPORTING

### 3.6.1 General

The President and management team shall review the Company's IT Management Systems, on a semi-annual basis and more frequently if needed, to ensure its continuing suitability, adequacy and effectiveness. This review shall include

assessing opportunities for improvement and the need for changes to the IT Management Systems, including the IT policy and objectives.

The CIO is responsible for maintaining records of management reviews.

3.6.2 **Review Input**

The CIO and IT managers provide the following information for Management Review meetings:

a) Results of audits
b) Department and employee feedback
c) Process performance
d) Follow-up actions from previous management reviews
e) Changes that could affect IT Management Systems
f) Recommendations for improvement

3.6.3 **Review Output**

Records shall include the output from the management review and shall include any decisions and actions related to:

a) Improvement of the effectiveness of IT Management Systems and its processes
b) Improvement of processes related to IT requirements
c) Resource needs

3.6.4 **Referenced Procedures:**

ITAD101 – Information Technology Management

## 3.7 BUSINESS CONDUCT

Unethical business conduct, actions or even the appearance of unethical behavior is unacceptable under any conditions. The reputation of the Company depends on each employee applying common sense in situations where specific rules of conduct are insufficient to provide clear direction. A strong sense of personal ethics, which should extend beyond compliance with applicable laws, is necessary to guide the behavior of all employees.

All employees should comply with the ethical standards of the Company as set forth in this manual. If a situation feels awkward or uncomfortable, employees should ask themselves:

- Is my action legal and ethical?
- Does my action comply with corporate policy?
- Is my action appropriate in the situation?
- Would my action be an embarrassment to the Company, if known?
- Does my action agree with my personal ethics or behavior?

Employees should be able to answer "yes" to all of these questions (except the fourth, of course) before taking action.

All Managers are responsible for the ethical business conduct and behavior of their employees. Managers should consider the appropriate courses of action in

terms of both ethical and economic factors. Each decision should be based on the guidelines provided in this IT Manual as well as their own personal beliefs of what's right and wrong.

All employees are responsible for awareness of - and respect for - the intellectual property rights of others, for complying with the U.S. Digital Millennium Copyright Act of 1998, and for complying with privacy, trans-border data flow, and cryptographic regulations applicable to the Company's IT practices.

# 4.0 IT MANAGEMENT SYSTEM

## 4.1 OBJECTIVES

Through this manual and associated procedures and documents, Our Company has established, documented, and implemented an IT Management System. The system is designed to result in improving the effectiveness of our IT operations and in our ability to satisfy auditor requirements.

## 4.2 REQUIREMENTS

Maintenance of the IT Management System is the responsibility of the CIO, in conjunction with the IT Department.

### 4.2.1 **Overview**

The CIO maintains all documents that identify the sequence of IT processes and, in conjunction with the appropriate department managers, defines the interactions of the processes within the procedures defining these processes.

Processes for management activities, provision of resources, and measurement reporting are included. Procedures shall include the methods needed to ensure that the accountability and control of processes are effective.

Top Management will ensure the availability of resources to support the operation and monitoring of processes through regular interaction with department managers and through review activities at Management Review meetings.

Department Managers and the CIO will monitor, measure, and analyze processes and implement any actions necessary to achieve intended results and ensure continual improvement of processes. These results will also be monitored at Management Review meetings.

Any processes that are outsourced that may affect Our Company's conformity to requirements shall be controlled. The CIO and appropriate department manager(s) are responsible for defining the methods to control outsourced processes in procedures.

### 4.2.2 **Internal Controls**

Controls should be selected based on the cost of implementation relative to the reduction of risk and potential for loss, if and when a security breach occurs. Non-monetary factors, such as loss of reputation, should also be taken into account.

Internal controls, procedures, and practices ensure that:

- Risks are reduced to an acceptable level.
- All assets are safeguarded against waste, fraud, loss, unauthorized use or disclosure, and misappropriation.
- Programs are efficiently and effectively carried out in accordance with applicable laws and management policy.

### 4.2.3 Access Controls

Access to all IT assets should be properly controlled and recorded into the IT Management System in accordance with Company IT policies defined in this manual.

All transactions should be supported by documentary evidence, which becomes part of the IT records. Error transactions should be reviewed, resolved, and cleared in a timely fashion. Manually determined control should be reconciled with recorded results.

Access control should ensure that:

- Information access is authorized for effective use of media and application security.
- Personnel information is protected including defining and assigning access levels, guidelines for hiring/transfer/separation, and security awareness training.
- Rules for managing IT security are in place for regular testing, auditing and accreditation.
- Audit trails exist for detective and reactive response to system penetration, infection of systems and data due to malicious code, catastrophic system loss or a compromise of data integrity.

### 4.2.4 Audit Findings

Managers are to promptly evaluate findings and recommendations reported by auditors and then determine proper actions in response to audit findings and recommendations (e.g., develop corrective actions). Managers should complete, within established time frames, all actions that correct or otherwise resolve the matters brought to management's attention.

The audit resolution process begins when the results of an audit are reported to management, and is completed only after actions have been taken that correct identified deficiencies, produce improvements, or demonstrate the audit findings and recommendations are either invalid or do not warrant management actions.

## 4.3 TRANSACTIONS

All transactions recorded into the IT Management System should be properly authorized and accurately represent the activity occurring. The timing of the transaction should be in accordance with Company IT policies defined in this manual.

### 4.3.1 Authorization

Access to systems, transactions and other significant events are to be authorized and executed only by persons acting within the scope of their authority. It is the principal means of assuring that only valid transactions and other events are entered into. Modification or adjustment to previously recorded transactions requires authorization.

### 4.3.2 Accuracy

Transactions should be recorded in the IT system accurately. All transaction dates recorded in the Company IT system should accurately reflect the date the transaction occurred.

All transactions should be supported by documentary evidence, which becomes part of the IT records.

### 4.3.3 Referenced Procedures:

ITAD101 Information Technology Management
ITSD101 IT Threat And Risk Assessment
ITSD106 IT Access Control
ITSD107 IT Security Audits

## 4.4 DOCUMENTATION

This IT Manual and the associated procedures are intended to satisfy the documentation requirements for an IT Management System. Department managers and supervisors are responsible for identifying any additional documents needed to ensure the effective planning, operation and control of processes.

Procedures may vary in detail based on the size of the department or organization involved and the type of activity performed. Procedure developers shall consider this as well as the complexity of the processes and interactions, and the competence of the personnel involved.

The IT Management System utilizes standard forms and provides control and accountability over these forms. Supervisors should review posted IT transactions with source documents and processing documents. Documents may be any medium including: software programs, electronic text files, or hardcopy documents for example.

### 4.4.1 IT Policy Manual

This IT Policy Manual includes the scope of Our Company's IT Management system and sets forth management policy.

### 4.4.2 Control of Documents

All Documents required by the IT Management System shall be controlled. The Document Control Procedure defines the controls needed to:

a) Approve documents for adequacy prior to issue.
b) Review and update as necessary and re-approve documents.
c) Ensure that changes and the current revision status of documents are identified.
d) Ensure that relevant versions of applicable documents are available at points of use.
e) Ensure that documents remain legible and readily identifiable.
f) Ensure that documents of external origin are identified and their distribution controlled.

g) Prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose.

### 4.4.3 Control of Records

Procedures define appropriate records to be maintained in order to provide evidence of conformity to requirements and of the effective operation of the IT Management System. Records shall remain legible, readily identifiable and retrievable. The Files and Records Management Procedure defines the controls needed for the identification, storage, protection, retrieval, retention time, and disposition of records.

### 4.4.4 IT Transactions

All transactions and other significant events should be clearly documented, properly classified and readily available for examination.

This standard applies to:

- The entire process or life cycle of a transaction or event and includes the initiation and authorization
- All aspects of the transaction while in process
- Its final classification in summary records.

### 4.4.5 Software Coding

Formal change control is required for all production systems. All software libraries and other significant code should be clearly documented, properly classified and readily available for examination using a Source Code Control System (SCCS). The SCCS should be used to control all source code and software revisions.

Developers should document all code changes within the software. An appropriate comment should be made within the SCCS reflecting the changes made when code is checked-in and checked-out.

### 4.4.6 Referenced Procedures:

ITAD102 IT Records Management
ITAD103 IT Document Management
ITSW106 Software Documentation
ITSD107 IT Security Audits

## 4.5 SECURITY

Access to resources and records should be limited to authorized personnel only. Accountability for the custody and use of resources should be assigned and maintained as well.

Periodic comparisons should be made of the resources with the recorded accountability to determine whether the two agree. The frequency of the comparison shall be a function of the vulnerability of the asset.

Restrictions of access to resources shall also depend upon the vulnerability of the resource as well as the perceived risk of loss, both of which shall be periodically assessed.

### 4.5.1 Physical Security

Physical security measures should be adopted to protect the assets and employees of the Company from abuse, fraud, theft, or damage. Security procedures for the protection of assets and employees are addressed within the Company's Security Manual. See ABR32, ***Bizmanualz® Security Planning Policies and Procedures Manual***.

### 4.5.2 Disaster Security

Disaster security measures should be adopted to enable the Company to continue the operations of the IT Management System with limited interruption. Disaster procedures for operations recovery are addressed within the Company's Disaster Manual. See ABR33, ***Bizmanualz® Disaster Recovery Policies and Procedures Manual***.

### 4.5.3 Information Security

Information security policies and procedures represent the foundation upon which companies construct their information security program. Information security policies serve as overarching guidelines for the use, management, and implementation of information security throughout the organization.

### 4.5.4 Referenced Procedures:

ITSD101 IT Threat / Risk Assessment
ITSD102 IT Security Plan
ITSD104 IT Disaster Recovery
ITSD105 Computer Malware
ITSD106 IT Access Control
ITSD107 IT Security Audits
ITSD108 IT Incident Handling

[This page intentionally left blank]

## 5.0 PROCESSES AND CONTROLS

The following processes, controls, and procedures serve to define specific operational steps and practices to support the organization's approach to information security, operations, development, and support, as defined by the policy statements.

These processes and procedures include the IT objectives and requirements for our Company, the required verification, validation, and inspection activities specific to our Company and the criteria for software and hardware acceptance. The records needed to provide evidence that these processes meet all compliance requirements are defined in the procedures.

Consideration is given for the need to establish processes, documents, and obtain resources specific to information security to ensure the safety of all information assets.

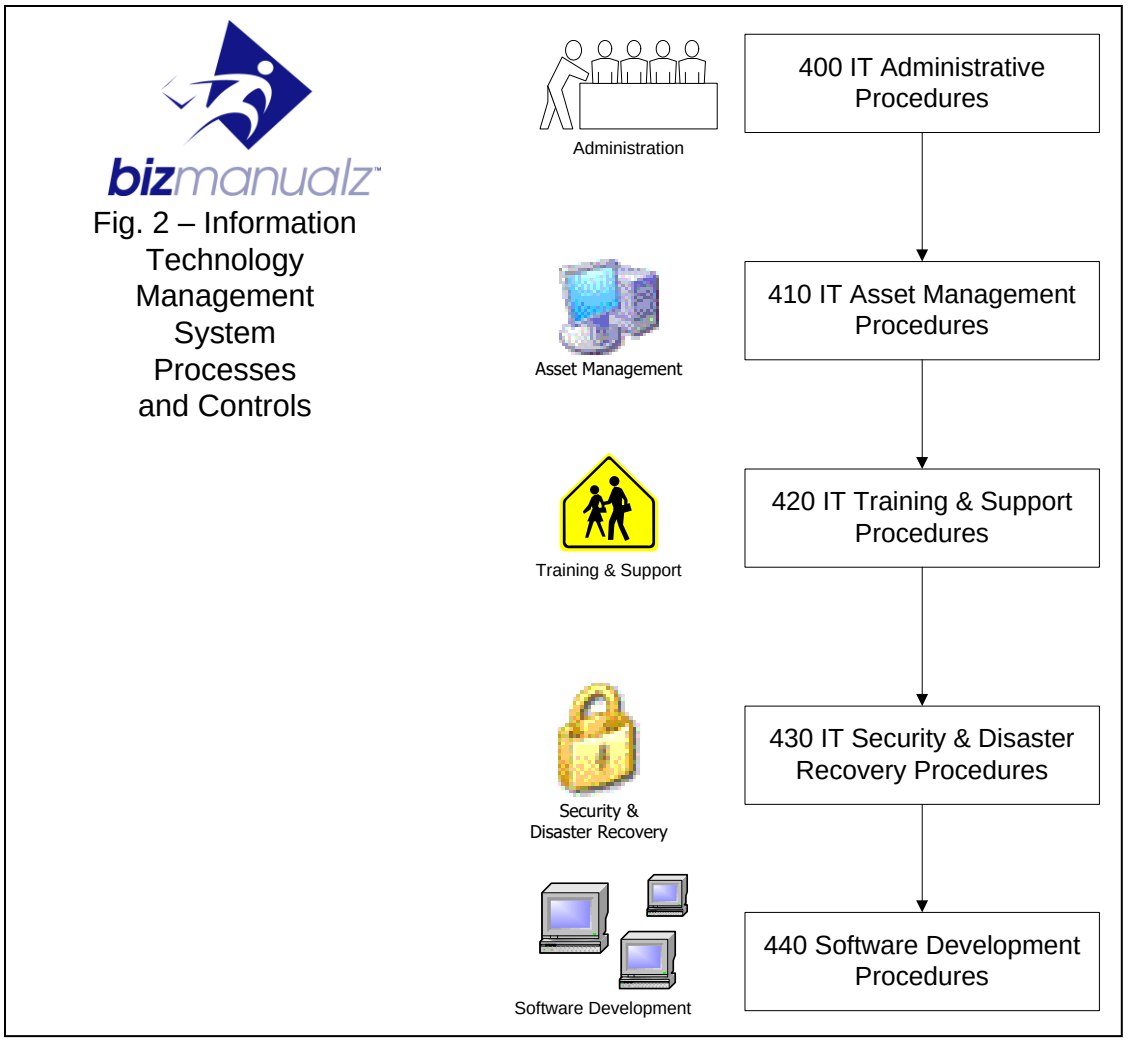


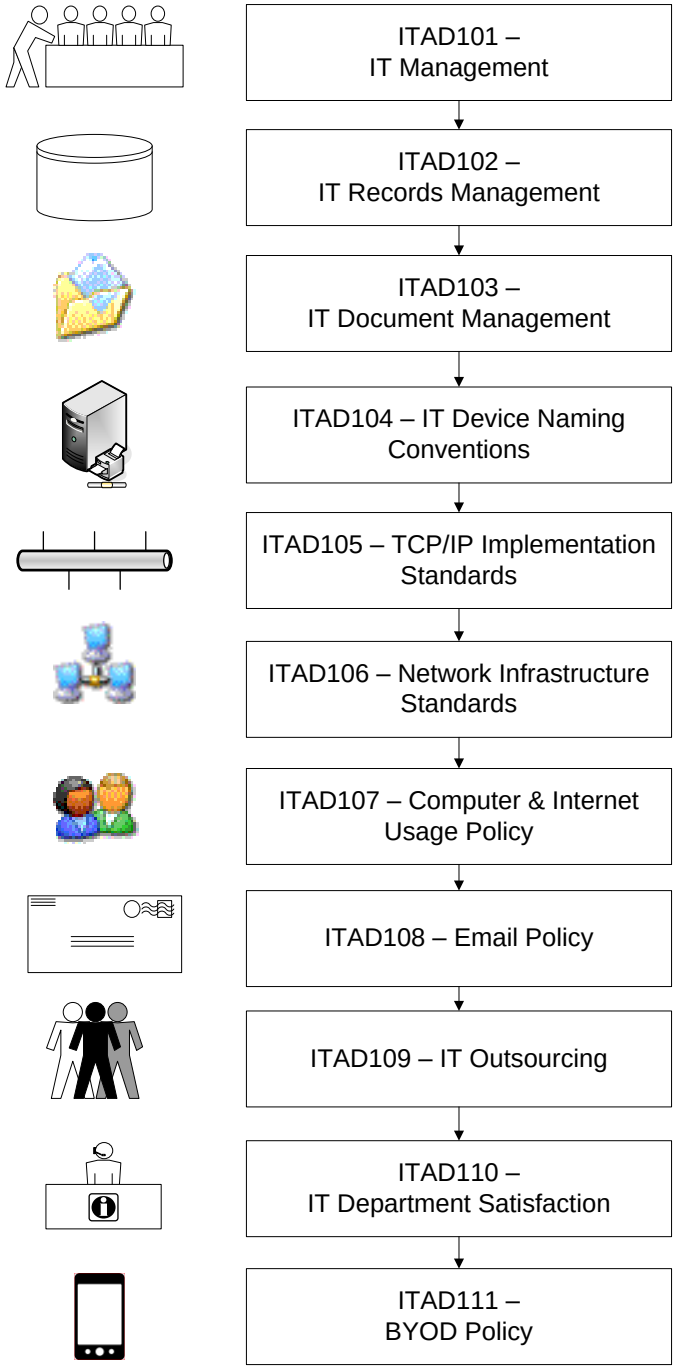

Fig. 2 – Information Technology Management System Processes and Controls

[This page intentionally left blank]

## 5.1 IT ADMINISTRATION

The IT Administrative procedures encompass a wide range of miscellaneous activities from the overall direction of IT Management, maintaining IT records and documentation, to network management standards and department satisfaction. The following IT Administrative procedures should be utilized to control the Company's miscellaneous IT activities.

Fig. 3 – IT Administrative Procedures



### 5.1.1 Information Technology Management

IT Management supports the Company's Strategic Plan through strategic planning and effective use of information technologies. Its goals include deployment of information technologies that increase overall Company productivity and performance, achieve greater efficiencies, and achieve positive returns on the investment in technology.

The Company should link Information Technology department goals and objectives to the Company's strategic vision, ultimately assuring that the Company meets customer requirements while undergoing continual improvement.

### 5.1.2 IT Records Management

The IT department organizes and manages Company records in a controlled, consistent, and effective manner while conforming to specified requirements and ensuring the safety, availability, confidentiality, and integrity of all electronic records.

### 5.1.3 IT Document Management

The IT department manages all electronic documents connected with official Company functions, storing them securely, ensuring their integrity, and allowing appropriate parties access to them. It is intended to provide methods and set forth responsibilities with regard to the control, storage, revision, retrieval, and disposal of documents.

### 5.1.4 IT Device Naming Conventions

All devices joined to the Company network are to be named in a way that facilitates management of network resources and delineates conventions for the assignment of host or device names for any equipment included with the Company IT infrastructure.

### 5.1.5 TCP/IP Implementation Standards

TCP/IP addresses are to be assigned in a way that facilitates management of the network and provide conventions for assigning TCP/IP addresses to equipment that is part of the Company IT infrastructure.

### 5.1.6 Network Management Standards

The Company network infrastructure shall be engineered and installed in accordance with appropriate industry standards and state and local building and electrical codes, to ensure safety, security, adequate capacity, and maximum efficiency.

Specific standards regarding the installation of the IT network infrastructure, such as cabling, routers, gateways, and other equipment, are spelled out.

### 5.1.7 Computer and Internet Usage Policy

Any employee using the Company IT network for any reason must adhere to strict guidelines regarding its use. Employees are being entrusted with the safety and security of Company information assets, not the least of which is Company

information. A sound security policy for information and other IT assets will include the participation of every employee, at all times. Sound policy promotes information security.

### 5.1.8 Email Policy

Company email and the hardware and software that support it belong to the Company. Email can be a tool for promoting cooperation and collaboration between and among employees, clients, and suppliers. Any use of email on Company time while using Company assets should promote the Company's interests, as well as those of its customers and vendors.

### 5.1.9 IT Outsourcing

The Company must provide guidance to IT Management with regard to outsourcing IT functions or capabilities. This ensures that the customer's needs continue to be met while allowing the company to control costs, maintain its flexibility, and take advantage of specialized knowledge and expertise on an as-needed basis.

### 5.1.10 IT Department Satisfaction

The customers of the Company's IT department will most often be its internal user base. In order to enable greater productivity on the part of the user community and ensure the satisfaction of the Company's ultimate customers, the IT department must strive to improve service, enhance the users' satisfaction with IT products and services in general, and increase the user community's performance and productivity, supplying products and services that add value.

### 5.1.11 BYOD Policy

Company employees and contractors may use their personal electronic devices (e.g., smartphones, tablets) to conduct company business, provided they understand and agree with the policy, have been granted express permission to use their devices, and act in accordance with the policy.

### 5.1.12 Referenced Procedures:

ITAD101 Information Technology Management
ITAD102 IT Records Management
ITAD103 IT Document Management
ITAD104 IT Device Naming Conventions
ITAD105 TCP/IP Implementation Standards
ITAD106 Network Infrastructure Standards
ITAD107 Computer and Internet Usage Policy
ITAD108 Email Policy
ITAD109 IT Outsourcing
ITAD110 IT Department Satisfaction
ITAD111 BYOD Policy

[This page intentionally left blank]

## 5.2 ASSET MANAGEMENT

Adequate control over all IT assets – in this case, meaning the computer hardware and software the Company relies on, not only for conducting its day-to-day business, but for positioning itself for growth, which it achieves through increased customer satisfaction. The following procedures help the Company maintain control over its IT assets.

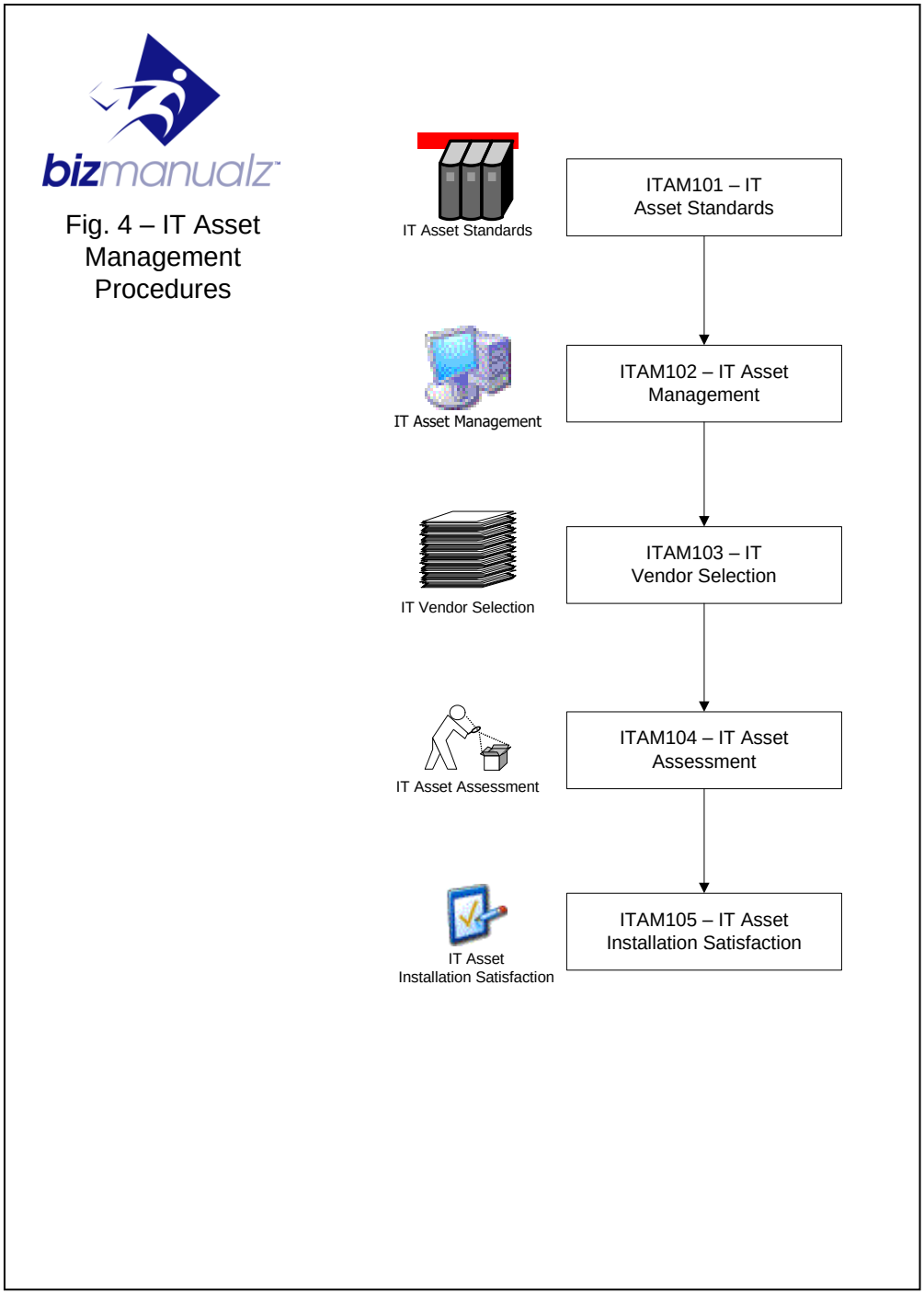



Fig. 4 – IT Asset Management Procedures

### 5.2.1 IT Asset Standards

Proper internal control should be maintained over all IT assets, at all times. The Company should identify and develop a set of IT asset standards that will allow it to minimize the complexity and cost of building and managing IT systems.

The Company should also be looking to the future at all times, knowing that whatever assets serve it (and its customers) well at this moment cannot continue to serve it indefinitely. The Company should expect its standards to change with business demands and should anticipate – even promote – change.

### 5.2.2 IT Asset Management

Proper IT asset management – from requisition to disposal – ensures a much greater likelihood that the Company will continue to meet customer requirements into the indefinite future by planning in an orderly fashion and mandating consistency throughout the enterprise.

### 5.2.3 IT Vendor Selection

The Company should establish and follow a set of guidelines for selecting IT vendors and maintaining vendor relationships.

### 5.2.4 IT Asset Assessment

The Company should review its IT assets on a regular basis to ensure their continuing ability to meet Company (and the customers') requirements, as well as to anticipate changing business conditions and assess the Company's ability to adapt by properly managing its IT assets.

The Company should ensure that only approved hardware and software (see IT Asset Standards) are used and that those are properly versioned, licensed, and adequately meet the users' (and Company) requirements.

The Company should also have a mechanism for adapting to changing business conditions, to ensure its hardware and software are not inadequate or obsolete.

### 5.2.5 IT Asset Installation Satisfaction

The Company should ensure that its internal users' requirements are being met, by measuring their level of satisfaction with the way the IT department conducts its business; in this case, not only whether an installation was performed, but whether the user's ***perceived*** (as well as actual) needs were satisfied.

### 5.2.6 Referenced Procedures:

ITAM101 IT Asset Standards
ITAM102 IT Asset Management
ITAM103 IT Vendor Selection
ITAM104 IT Asset Assessment
ITAM105 IT Asset Installation Satisfaction

## 5.3 IT TRAINING AND SUPPORT

Training and support are critical elements of information technology. In order to maintain the rapid pace of technological change the company shall plan for change and provide a framework for its employees' personal and professional growth.

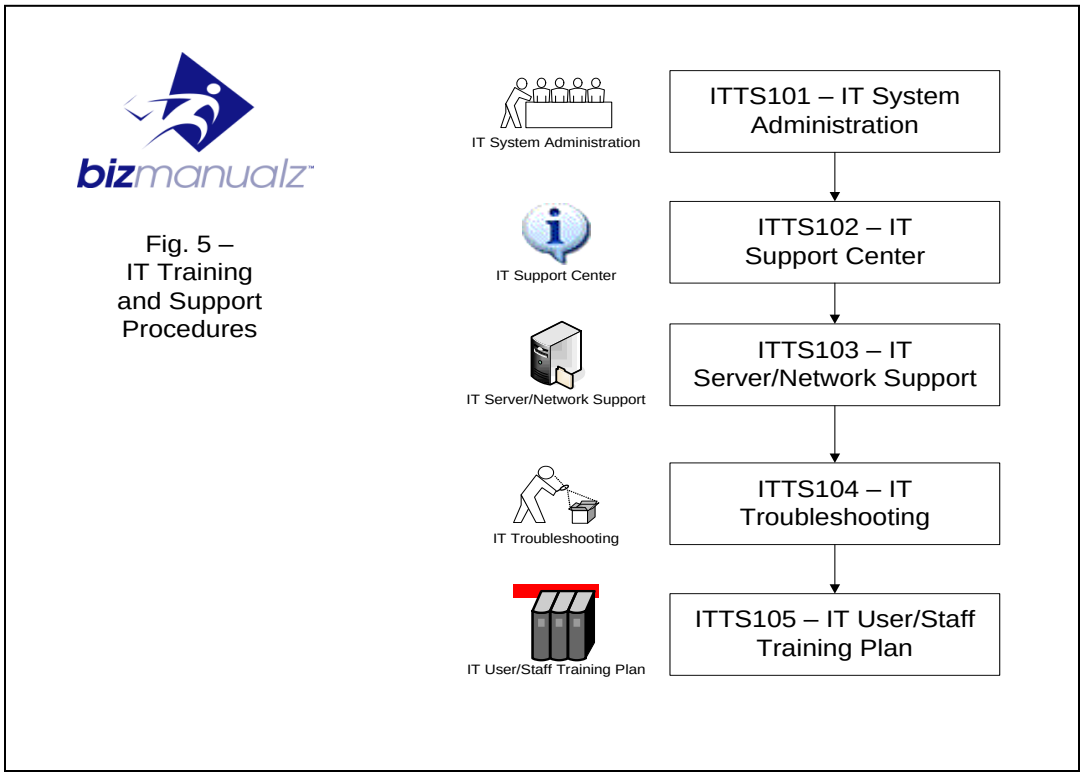



Fig. 5 – IT Training and Support Procedures

### 5.3.1 Systems Administration

The Company should have a central authority – a System Administrator (or "Sys Admin") – whose responsibility it is to oversee the day-to-day operation of all IT-based systems. The Sys Admin should be charged with administering the Company's IT systems in a manner that promotes the achievement of Company goals and objectives and provides for Company growth.

### 5.3.2 IT Support Center

The Company should operate an IT Support Center for the purpose of providing ongoing technology support (emergency and non-emergency) to all departments and IT users. Staffing, training, and logistic requirements for this support center should be identified and training provided in order that the support center satisfies user needs and maintains its effectiveness.

### 5.3.3 Server and Network Support

The Company should provide support for its servers and the network that enables sharing of data, ensuring a secure and effective environment.

### 5.3.4 Troubleshooting

The Company should develop and maintain guidelines for troubleshooting IT-related problems in order to ensure effectiveness, consistency, and continual improvement of the troubleshooting process.

The Company should seek to minimize disruptions, enhance employee productivity, and promote user satisfaction with the process and the people performing the service.

### 5.3.5 User-Staff Training Plan

The Company should determine adequate levels of competence for technical and non-technical personnel who use the Company's IT systems to perform work, then provide training or take other actions to satisfy training requirements.

The Company should provide personnel (IT personnel, in particular) with a learning path or guide, so that the employees in question build a skill set that benefits the Company and rewards the individual. An adequate training plan should aim to improve the Company's performance by reducing training/skill gaps, anticipating the Company's needs, and continually improving training availability and methods.

### 5.3.6 Referenced Procedures:

ITTS101 IT Systems Administration
ITTS102 IT Support Center
ITTS103 IT Server/Network Support
ITTS104 IT Troubleshooting
ITTS105 IT User-Staff Training Plan

## 5.4 IT SECURITY AND DISASTER RECOVERY

The Company should provide a safe, secure IT environment to serve its customers' requirements, ensure stability and continuity of the business, and promote confidence in its ability to not only continuously provide goods and/or services, but also to recover quickly from disaster and minimize disruption.

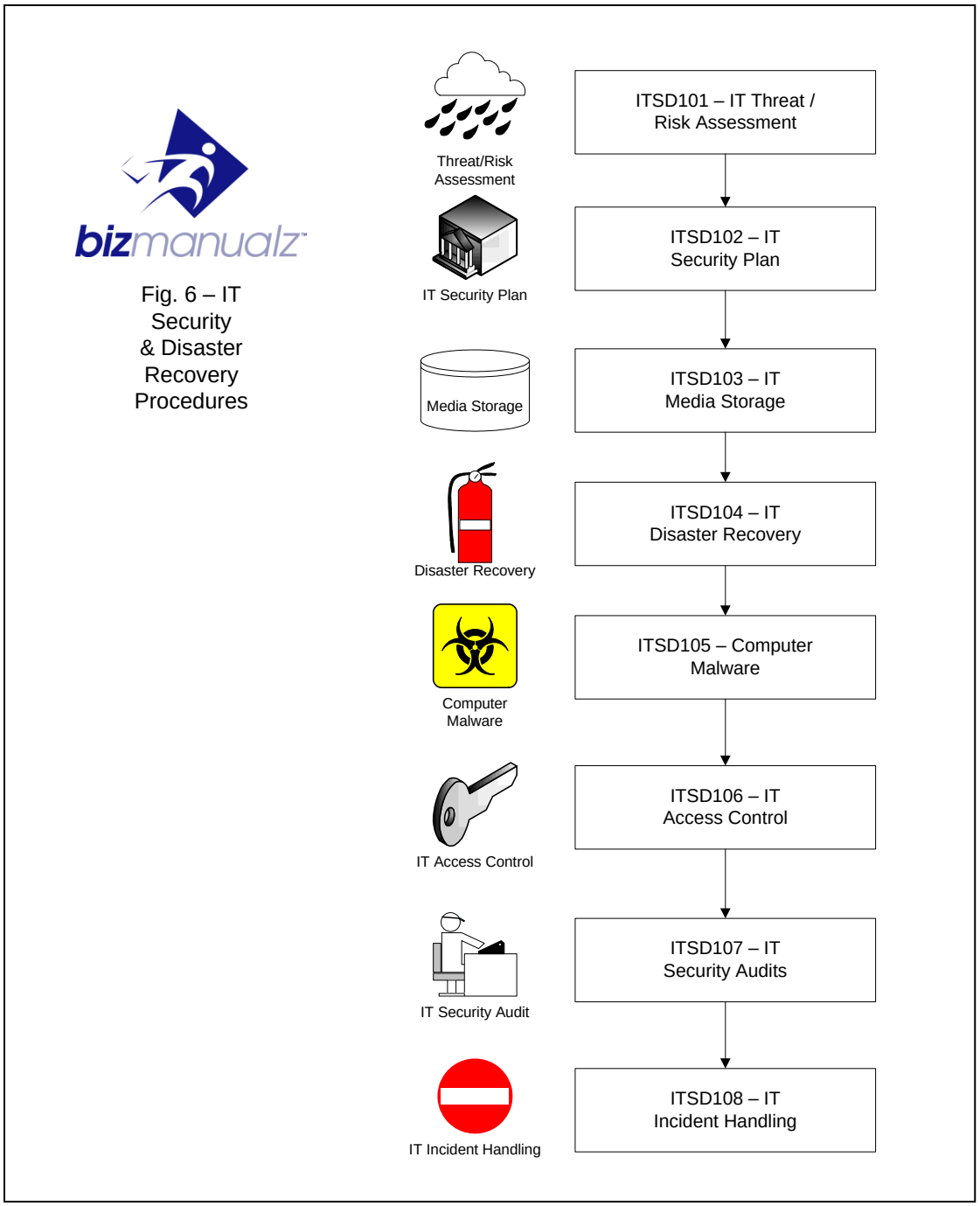



Fig. 6 – IT Security & Disaster Recovery Procedures

### 5.4.1 IT Threat/Risk Assessment

The Company should periodically evaluate its IT systems and network for threats and vulnerabilities, to protect its IT assets and reduce the Company's risk.

The Company should develop and follow a set of procedures for identifying threats to the Company's IT assets, assess those threats for probability and risk, and minimize the chances of loss or disruption.

### 5.4.2 IT Security Plan

The Company should develop and implement a plan to ensure the confidentiality and integrity of Company information while maintaining appropriate levels of accessibility.

The Company should set forth its own security requirements, which should be equal to or greater than security requirements prescribed by law and/or standards bodies (ISO, IEEE, etc.). The Company should also strive to keep its IT security plan current and active – continual improvement of the process is crucial to its success.

The Company should put in place all reasonable technological means (i.e., security software/hardware) to keep information and facilities secure.

Regardless of whatever technological means are available to the Company, it must ensure that its employees accept and understand the security plan and put it into practice on the jobs. Employees are a key part – if not the most important part – of the IT security plan.

### 5.4.3 IT Media Storage

The Company should establish controls and procedures for storage, protection, access, procurement, and destruction of Company data.

The Company should plan for cost-effective storage technologies that offer long asset life and scalability and ensure data integrity and availability.

### 5.4.4 IT Disaster Recovery

The Company should develop and implement a straightforward, workable plan to not only cope with the initial effects of a disaster, but to return the Company's IT operations to normal as quickly as possible.

The company should regularly test the IT disaster recovery plans. Every employee, regardless of his/her relation to the IT department, should be educated with regard to the IT disaster recovery plan and be prepared to play a part.

### 5.4.5 Computer Malware

To prevent data loss, corruption, or misuse of Company computing resources or information, the Company should develop and implement a plan for mitigating the risk posed by malware (*mal*icious soft*ware* – i.e., viruses, worms, spyware).

### 5.4.6 IT Access Control

The Company's requirements for controlling access should meet or exceed those set forth by standards bodies and by applicable laws.

The Company should control access to its information, to help ensure confidentiality and integrity of its data while making the data available to authorized parties.

### 5.4.7 IT Security Audits

The Company should, once it has implemented a security plan for IT, ensure that the plan is being effectively carried out in accordance with regulatory and Company requirements and meets or exceeds industry standards for information security.

The Company should have a qualified third party auditor conduct an audit of its IT security system on a regular basis, to ensure the plan's conformance to applicable standards and requirements and to promote continual improvement of the plan.

### 5.4.8 IT Incident Handling

An "IT incident" is an actual or suspected compromise of the Company's IT assets and/or operations. If an employee suspects Company assets are being misused or are under attack, that employee has an obligation to report that incident to IT Security.

When such an incident occurs, the Company should have a plan for dealing with (i.e., reporting, investigating, and resolving) the incident. This plan should help ensure the safety, confidentiality, availability, and integrity of Company information.

### 5.4.9 Referenced Procedures:

ITSD101 IT Threat / Risk Assessment
ITSD102 IT Security Plan
ITSD103 IT Media Storage
ITSD104 IT Disaster Recovery
ITSD105 Computer Malware
ITSD106 IT Access Control
ITSD107 IT Security Audits
ITSD108 IT Incident Handling

[This page intentionally left blank]

## 5.5 SOFTWARE DEVELOPMENT

Successful software products begin with careful planning and attention to detail. Documenting the organization's software policies and procedures provide a structure that streamlines development efforts and empowers employees. Documented policies and procedures eliminate guesswork, promote good working relationships, build quality standards into products/services, and simplify training for new employees.

The following sample policies and procedures document the functions performed by the software development organization.

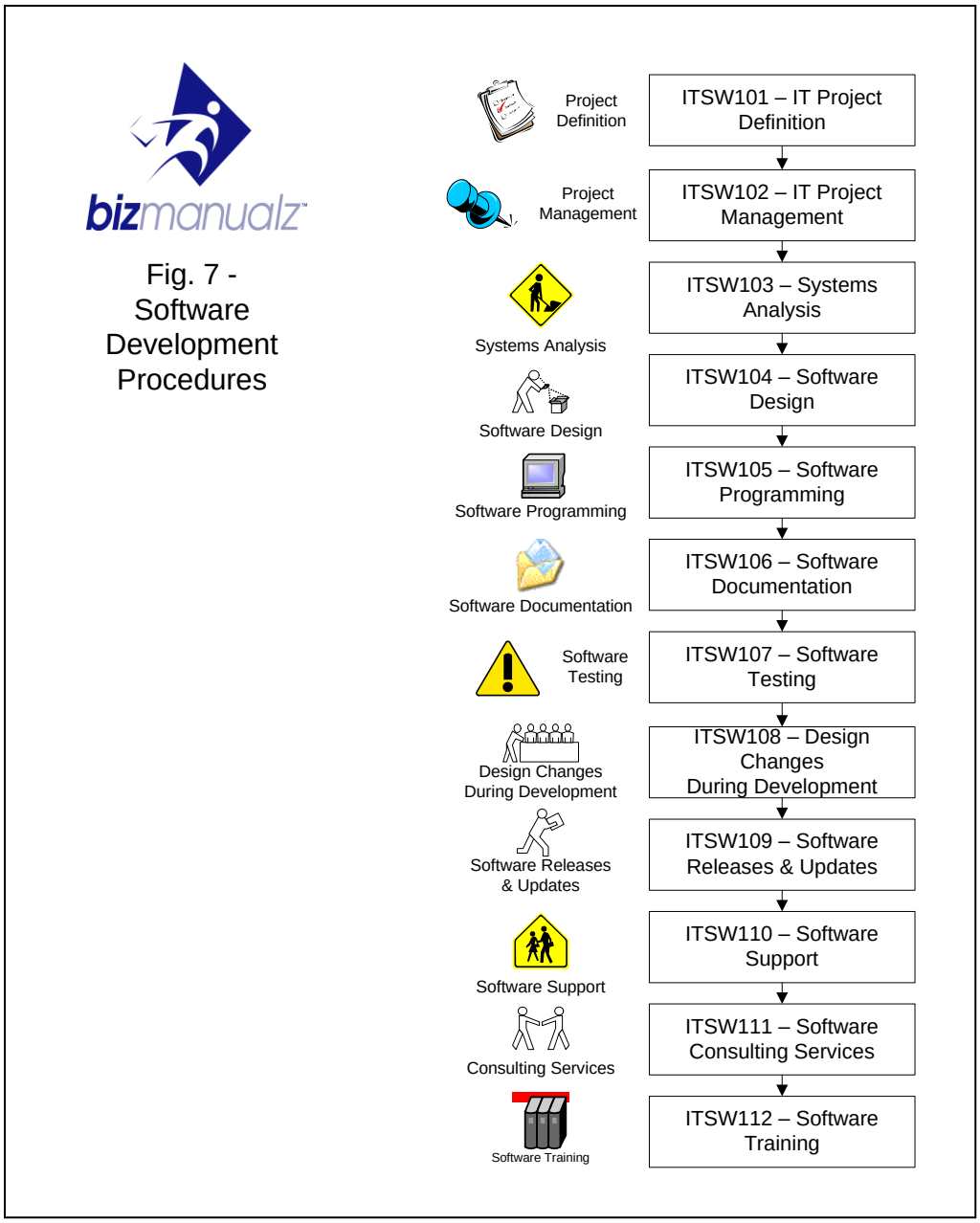



Fig. 7 - Software Development Procedures

### 5.5.1 IT Project Definition

A software development project begins with the project definition – explaining the purpose and scope of the project. The software developer must identify the goals and objectives of the project and determine the potential impact of the project on other projects, on the Company, and on the Company's customer base.

An IT Project Plan should be used as a framework for developing future IT projects. It should be reviewed prior to undertaking any project plan and should be continually reevaluated, in light of the Company's changing circumstances.

### 5.5.2 IT Project Management

All in-house software development projects should follow a defined project management procedure. This is to ensure that IT projects are clearly defined, well structured, efficiently and effectively managed, and are capable of producing the desired results, on time and within budget.

### 5.5.3 Systems Analysis

All software products developed by the organization must meet the needs of potential users. These users may be in-house or they may have contracted with the organization for software applications; in this case, the users' needs may be known and specific. In the case of software developed for an indeterminate number of users (i.e., an accounting or HR package), those needs are generalized.

The software developer must define the functions the system will perform, tell how those functions are interrelated, and describe how to test those functions.

### 5.5.4 Software Design

Software should be designed in a technically sound and efficient manner and fulfill requirements identified by the systems analyst. The software designer transforms the set of system requirements developed by the analyst into programming instructions for the software product.

### 5.5.5 Software Programming

Software products developed by the Company should, at a minimum, meet Company standards for user interface, program structure, system interface, toolset, and configuration. The job of the software programmer is to effectively and efficiently carry out the plans of the software designer, per Company standards.

### 5.5.6 Software Documentation

The Company's software products should be documented as thoroughly as practicable, with online help, user guides, and technical documentation, at a minimum. To this end, the Company should develop and implement standards for design, style, and content.

The Company should define the methods and responsibilities for controlling the revision, approval, and distribution of software reference and training materials.

### 5.5.7 Software Testing

All software products developed by the Company should undergo a series of tests – including acceptance tests, beta tests, and software release tests – before they are released to the customer or user community. Company-developed software must be tested free of errors in order to improve the likelihood of customer/user satisfaction.

### 5.5.8 Design Changes During Development

The Company should plan on design changes such that they are managed, controlled, and communicated effectively and efficiently.

The Company should expect that the user/customer will request product changes at some point in the software development process. The customer/client may come upon information only after such a project has begun – information that could have a significant impact on the project.

### 5.5.9 Software Releases and Updates

All of the Company's software releases and updates should be issued in a controlled manner to reduce difficulty and maintain consistency, quality, and versioning of its software products throughout the release and update sequence.

### 5.5.10 Software Support

The Company should ensure that their customers/users are able to install and operate software with as little effort and wasted time as possible.

The Company should provide a number of avenues for customers to ask questions, alert the Company to problems with its software, or request additional services.

The Company should continually solicit – and act on – feedback from customers/users in an effort to improve customer support.

### 5.5.11 Software Consulting Services

The Company should strive to engage its users proactively in a number of ways. Especially where the software product is complex, customers may need assistance through the life of the software, starting with installation. Users may require customization of the software.

### 5.5.12 Software Training

The Company should provide a sufficient level of training on the product, to ensure the users are actively learning to use the product by offering a range of training options. Ensuring that customers/users are able to effectively operate the Company's software helps to promote greater customer satisfaction.

The Company should actively seek feedback from the user on the training process.

### 5.5.13 **Referenced Procedures:**

ITSW101 IT Project Definition
ITSW102 IT Project Management
ITSW103 Systems Analysis
ITSW104 Software Design
ITSW105 Software Programming
ITSW106 Software Documentation
ITSW107 Software Testing
ITSW108 Design Changes During Development
ITSW109 Software Releases and Updates
ITSW110 Software Support
ITSW111 Software Consulting Services
ITSW112 Software Training

# 6.0 RESOURCE MANAGEMENT

## 6.1 PROVISION OF RESOURCES

During planning and budgeting processes and as needed throughout the year, the President, CIO and management team determine and ensure that the appropriate resources are available to implement and maintain the IT Management System and continually improve its effectiveness.

## 6.2 HUMAN RESOURCES

### 6.2.1 IT Staff

Managers and employees are to have personal and professional integrity and are to maintain a level of competence that allows them to accomplish their assigned duties, as well as understand the importance of developing and implementing good internal controls.

This requires managers and their staff to maintain and demonstrate at all times:

- Personal and professional integrity
- A level of skill necessary to help ensure effective performance
- An understanding of information security and internal controls sufficient to effectively discharge their responsibilities

IT staff shall be subject to a security clearance check before they are hired, transferred, or promoted. The level of checking shall depend on the relative sensitivity of the position. Any employee who was not subjected to such a clearance check when first hired should not be placed in a sensitive position until security clearance has been obtained.

### 6.2.2 Competence, Awareness, and Training

IT personnel shall be competent based on appropriate education, training, skills and experience. The minimum competencies required for each position at Our Company are defined in each position's Job Description. Human Resources, department managers and supervisors are responsible for ensuring job descriptions are current and adequate.

Where otherwise qualified personnel require additional training or other action to meet the minimum competency requirements, these needs are identified. The department provides task-specific training. General training or education is provided or coordinated by Human Resources. The department or Human Resources evaluate the effectiveness of training or other actions taken as appropriate.

The department generates records of task-specific training. Human Resources maintain records of all training and education, skills and experience in accordance with Human Resources Policies and Procedures and Computer and Network Policies and Procedures.

Department managers are responsible for ensuring their employees are aware of the relevance and importance of their activities and how they contribute to the achievement of the IT objectives.

### 6.2.3 Separation and Supervision of Duties

Key duties and responsibilities should be separated among individuals. Duties and responsibilities shall be assigned systematically to a number of individuals to ensure that effective checks and balances exist. Key duties include authorizing, approving, and recording transactions; issuing and receiving assets; and reviewing or auditing transactions.

A separation of duties should be maintained between the following functions:

- Data entry;
- Computer operation;
- Network management;
- System administration;
- Systems development and maintenance;
- Change management;
- Security administration; and
- Security audit.

Qualified and continuous supervision is to be provided to ensure that internal control objectives are achieved. This standard requires supervisors to continuously review and approve the assigned work of their staffs as well as provide the necessary guidance and training to ensure that errors, waste, and wrongful acts are minimized and that specific management directives are followed.

### 6.2.4 Cross-Training and Succession Planning

Cross-training and succession planning guidelines should be created to ensure backup for key personnel. Persons holding sensitive or key positions should take vacations (holidays) of at least a week in length, so that the Company can verify the effectiveness of its cross-training and prevent and detect fraudulent activity.

### 6.2.5 Referenced Procedures:

See ABR41 ***Bizmanualz® Human Resources Policies and Procedures Manual***.

## 6.3 INFRASTRUCTURE

Our Company provides the infrastructure necessary to achieve conformity to IT standards and requirements. During the annual budgeting and strategic planning processes, buildings, workspace, hardware, software and associated utilities are evaluated and provided.

When new personnel are added, Human Resources coordinates activities to ensure appropriate process equipment including hardware and software, if required, and supporting services such as telephones etc., are available based on information provided on the Personnel Requisition.

## 6.4 WORK ENVIRONMENT

The management team, CIO and Office Manager determines and manages the work environment to ensure Our Company provides a safe and desirable place to work. They ensure the environment is appropriate for achieving conformity to product requirements.

## IT MANUAL - REVISION HISTORY

| Revision | Date | Description of Changes | Requested By |
|---|---|---|---|
| 0 | mm/dd/yyyy | Initial Release | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

[This page intentionally left blank]