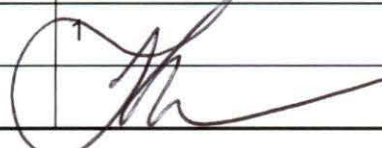




## CITY OF DELRAY BEACH

# ADMINISTRATIVE POLICIES AND PROCEDURES

<b>DEPARTMENT:</b>	Information Technology	<b>POLICY NUMBER:</b>	IT-001
<b>SUBJECT:</b>	Information Technology Policies and Procedures Manual	<b>SUPERSEDES:</b>	IT-1, IT-2, IT-3, IT-4, IT-5 Rev.2, IT-6 Rev.1
<b>REVISION:</b>	1	<b>EFFECTIVE DATE:</b>	11/4/2021
<b>APPROVED BY:</b>		Terrence R. Moore, ICMA-CM, City Manager	

### I. PURPOSE: (INCLUDE AFFECTED DEPTS)

### II. MISSION STATEMENT

The Mission of the Department of Information Technology is to consistently provide the highest quality technology-based services to support the vision for the City of Delray Beach.

### III. VISION

The Information Technology (IT) Department is the custodian of the technical infrastructure for the City of Delray Beach. As custodian, IT maintains a technical infrastructure, network, hardware, software, and human capital, which effectively supports the Departments and decision-making processes within the City while maintaining integrity and security of the City's data. IT is accountable for the strategic plan, tactical plan, and the IT project plans that support the City of Delray Beach technical infrastructure. IT's stakeholders include the City Hall, Public Works, Parks, Fire and Police Departments that utilize IBM iSeries, ERP System, 200 virtual/physical servers, 550 personal computers, and 650 laptops/tablets and peripherals. IT is also responsible for data processing, output distribution, security, data integrity, e-mail, e-government, Internet usage, business process automation, hardware and software acquisition and maintenance, LAN administration, system security, virus protection, systems analysis and design plus disaster recovery. IT continuously updates its plans to accommodate changes to the existing infrastructure based on trends and issues within the industry, business objectives, and growth. IT utilizes best practices for processes, procedures, tasks, and checklists as outlined in ITIL (Information Technology Infrastructure Library) and IT Service Management through the BOSSDesk Service Desk system.

### IV. INTRODUCTION

This policy and procedural manual (PPM) are intended to provide basic orientation information for the operational activities of the Information Technology Department of the City of Delray Beach, Florida. It is not intended to be a detailed guide describing each aspect of the IT Department's internal specific procedures.

However, this manual is intended to provide sufficient procedural detail to enable City departments, other governmental entities, and the contractor / vendor community to:

- a. be fully aware of, and comply with, City Information Technology policies, and
- b. effectively participates in the City's Information Technology program.

This document applies to all City of Delray Beach (**CDB**) users regardless of the user's location (e.g., in an office, at a customer site, on an airplane, at an Information User's residence, at a shared location, etc.); this term includes all CDB employees, and contractors / vendors that require access to CDB information resources, authorized previously by IT Chief Technical Director (**CTD**) or IT Director.

## V. POLICY INFORMATION

Continuous improvement. The content of this document is subject to regular review based on input from City of Delray Beach Information Technology staff.

## VI. DEFINITIONS

DEFINITIONS: (if applicable)

**CDB IT users:** City of Delray Beach employees, contractors, and vendors. Target audience for this policy.

**CDB IT Department:** Department in charge of enforcing, reviewing, and updating this policy.

**IT Chief Technical Director (CTD):** Resource in charge of authorizing user access to CDB IT information resources and reviewing changes to this policy.

**Information Resources:** defined as electronic and non-electronic resources owned by CDB and include, but it is not limited to documentation (designs, research material, reports, specifications, contracts); electronic media (computer software, computer tapes, computer disks, computer printouts); business operations (inventions, methods, processes, work products, customer lists); business development (municipality information, operating plans, cost and financial data); and system resources (phone systems, organization-issued cellular phones, hardware, networking resources, operating systems).

**Data:** is defined as information stored on hardware and accessed by using software.

**Software:** is defined as programs and routines written in a symbolic language that control the functioning of the hardware.

**Hardware:** is defined as the physical, touchable, and material parts of a computer.

**Third Parties:** Vendors and business partners of CDB, bound by underpinning agreements or contracts with CDB.

**Third Party Personnel:** Representatives of vendors and business partners of CDB.

**Remote Access:** Any communication to the City of Delray Beach systems and applications from an external (remote) location or facility through a data link.

**Dual Homing:** Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the corporate network via the Broadband Air card and on a local Ethernet connection on the home network.

**Split-tunneling:** Simultaneous direct access to a non-city network (such as the Internet, or a home network) from a remote device, while connected into the City of Delray Beach's corporate network via a VPN tunnel.



**Secure Shell** or **SSH**: is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

**TABLE of CONTENTS**

I.	PURPOSE: (include affected Depts) .....	1
II.	Mission Statement.....	1
III.	Vision.....	1
IV.	Introduction.....	1
V.	Policy Information.....	2
VI.	Definitions.....	2
VII.	IT Organization.....	11
VIII.	POLICY: .....	12
IX.	Information Security Policies .....	12
A.	Prohibited Activities .....	12
X.	Information Security .....	14
A.	Information Ownership .....	14
B.	Information Security Incident Reporting.....	14
XI.	Access Control and Authentication Mechanisms.....	15
A.	Access Philosophy .....	15
B.	Access Approval Process.....	15
C.	Default Facilities .....	15
D.	Departures from CDB .....	15
E.	Unique User IDs .....	15
F.	Segregation of Duties .....	16
G.	Password Policy .....	16
XII.	Physical Security and Remote Access.....	17
A.	Assigned Equipment.....	17
B.	Asset Inventory .....	17
C.	Computer Facilities.....	17
D.	Remote Access.....	17
XIII.	Internet Access and Email.....	18
A.	Use of Firewalls .....	18
B.	Internet Use .....	18
C.	Electronic Mail, Instant Messaging and Text Messaging Use.....	18
XIV.	Multi-Factor Authentication (MFA) Policy .....	20



A.	Introduction .....	20
B.	Purpose.....	20
C.	Definitions .....	20
D.	Policy.....	20
E.	Enforcement.....	20
XV.	Support Services.....	22
A.	Information Technology Assistance .....	22
B.	Software Development .....	22
C.	Software Product Licenses.....	22
D.	Product Registration .....	22
XVI.	Operations Management.....	23
A.	Computer Viruses .....	23
B.	Critical Data Location .....	23
C.	System Logon Banner .....	23
D.	Audit Logs.....	23
E.	Data Backups .....	23
F.	Disaster Recovery Plan .....	23
XVII.	UserID and Password.....	24
XVIII.	Electronic Systems and Communication Tools .....	26
A.	Use of Electronic Communication and Information Systems .....	26
B.	Email Specific Guidelines.....	27
XIX.	Remote Access.....	28
A.	VPN Overview .....	28
B.	VPN Standards.....	28
C.	VPN Policy.....	28
D.	VPN Procedure.....	29
E.	VPN Requirements.....	29
F.	VPN Enforcement .....	30
XX.	Security Education Training and Awareness (SETA) Policy .....	31
A.	Purpose Statement.....	31
B.	Policy Purpose.....	31
C.	Policy Scope .....	31

- D. CJIS Security Policy relationship to local Policy..... 31
- E. Definitions ..... 32
- F. Policy ..... 32
  - 1. Basic Security Requirements ..... 32
  - 2. Derived Security Requirements ..... 33
- G. Non-Compliance ..... 33
- XXI. Internet..... 34
  - A. Internet Use Guidelines ..... 34
- XXII. Hardware, Software and Data Resources ..... 35
- XXIII. Technology Replacement and Upgrade Policy ..... 36
  - A. Replacement Purpose ..... 36
  - B. Replacement Scope ..... 36
  - C. Replacement Roles and Responsibilities ..... 36
  - D. Replacement Policy Statement ..... 36
  - E. Replacement Risk Mitigation ..... 38
  - F. Replacement Software Upgrades ..... 38
  - G. Replacement Requirements ..... 38
- XXIV. Print Services Governing Principles..... 39
  - A. Utilization/Practices ..... 39
  - B. Deployment and Configuration..... 39
  - C. Security and Compliance ..... 39
  - D. Financial Management ..... 39
  - E. Connectivity and Driver Deployment..... 39
  - F. Printer / Copier Device Placement Principles ..... 39
  - Printer / Copier On-Going Management Procedures ..... 40
  - G. Strategic Department Consolidation (Department by Department) ..... 40
  - H. Tactical Device Consolidation (Device by Device) ..... 40
  - I. Planning and Acquisition ..... 41
  - J. Maintenance and Support..... 41
  - K. Retirement and Disposal ..... 42
  - L. Printer / Copier Exception Approval Process ..... 42
- XXV. Third Parties and Third-Party Personnel ..... 43



A.	Third Party Personnel User IDs .....	43
B.	Third Party Personnel Remote Access .....	43
C.	Third Party Compliance and Non-Disclosure Agreements.....	43
D.	Network Connected Third Party Systems .....	43
XXVI.	BOSSDesk Service Desk .....	44
A.	Purpose.....	44
B.	Approvals .....	44
C.	Employee Related Requests.....	44
D.	IT Department use of BOSSDesk .....	44
XXVII.	BOSSDesk Incident Management.....	46
A.	Purpose.....	46
B.	Scope .....	46
C.	Roles and Responsibilities .....	46
1.	Incident Managers .....	46
2.	Service Desk Operator .....	47
3.	Second-Line Support.....	47
4.	Third-Line Support.....	47
D.	Revision Control .....	47
E.	Communication of Policies.....	48
	Incident Management .....	48
F.	Incident Management Process .....	48
G.	Service Desk.....	49
	Service Levels and Metrics .....	49
H.	Incident Prioritization .....	49
1.	Business Impact Chart .....	49
2.	Urgency Chart.....	49
3.	Impact/Urgency Chart.....	49
I.	Incident Response Times .....	50
J.	Escalation Management .....	50
XXVIII.	BOSSDesk Request Management.....	52
A.	Purpose.....	52
B.	Scope.....	52

C.	Roles and Responsibilities .....	52
1.	Request Managers .....	52
2.	Service Desk Operator (Ticket Creator) .....	52
3.	Resolver Group (s) .....	53
D.	Revision Control .....	53
E.	Communication of Policies .....	53
	Request Management .....	53
F.	Request Management Process .....	53
G.	IT Operations Service Desk .....	54
H.	Request Classification .....	54
I.	Request Service Types .....	54
J.	Escalation Management .....	54
XXIX.	BOSSDesk Problem Management .....	56
A.	Purpose .....	56
B.	Scope .....	56
C.	Roles and Responsibilities .....	56
1.	Problem Manager .....	56
2.	Problem Ticket Requester .....	57
3.	Problem Analyst .....	57
4.	Service Desk .....	57
D.	Policy .....	57
E.	Goal .....	58
F.	Problem Management Principles .....	58
XXX.	BOSSDesk Change Management .....	59
A.	Purpose .....	59
B.	Scope .....	59
C.	Roles and Responsibilities .....	59
1.	Change Requester .....	59
2.	Change Assignee .....	59
3.	Change Manager .....	59
D.	Change Advisory Board (CAB) .....	60
E.	Revision Control .....	60

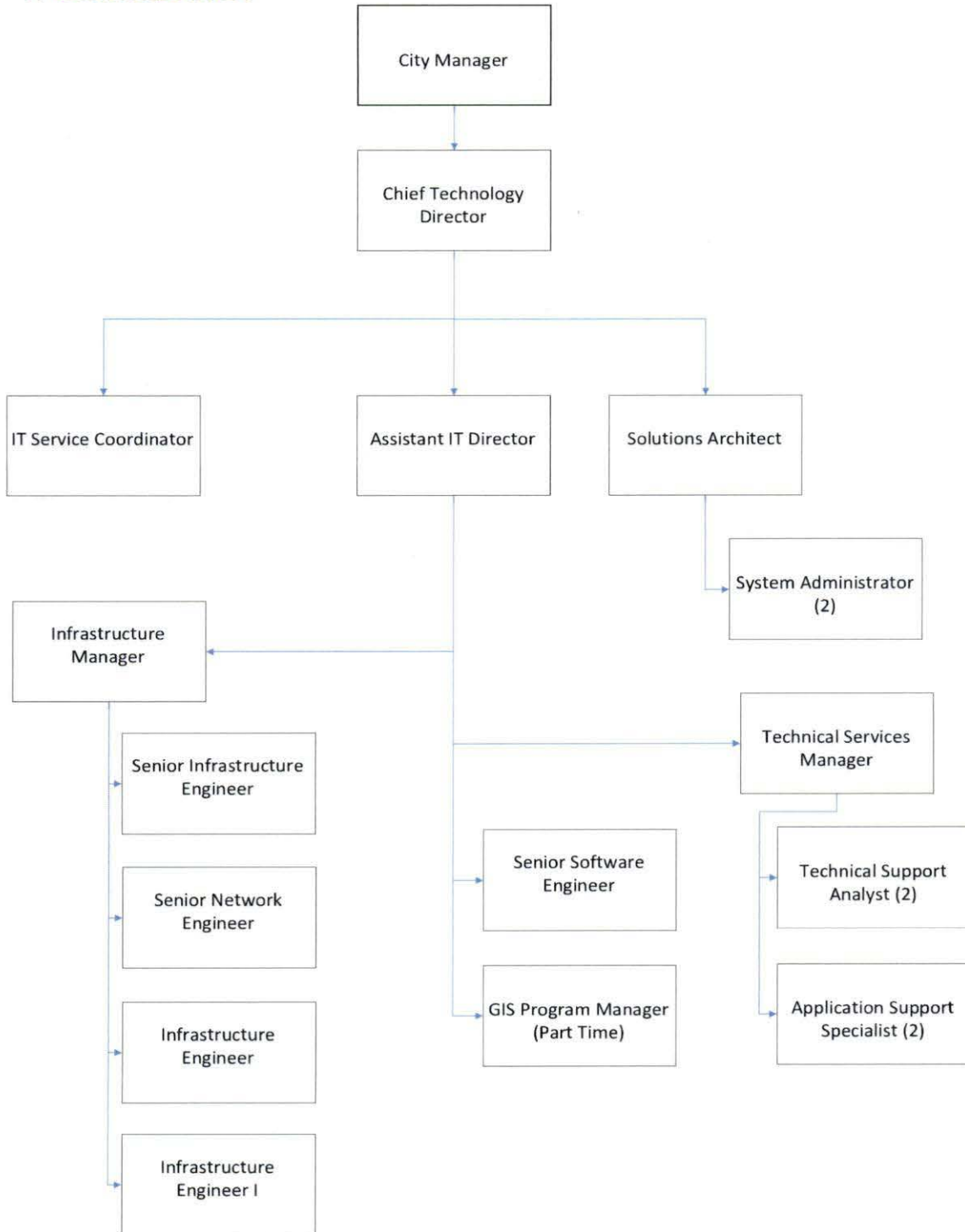


Change Management .....	61
F. Change Management Process Activities .....	61
G. Advisory Board Meetings .....	61
H. Forward Schedule of Changes .....	62
I. Change Reviews .....	62
J. Relationship to Other Service Management Functions Processes .....	62
K. Change Categories.....	63
L. Change Testing and Back out .....	63
XXXI. Public Wi-Fi.....	65
A. Disclaimer .....	65
B. Prohibited.....	65
C. Conditions.....	65
XXXII. Security Incident Response Policy .....	67
A. Purpose.....	67
B. Scope.....	67
C. Maintaining Currency.....	67
D. Definitions .....	67
E. Evidence Preservation.....	68
F. Incident Response .....	68
1. Preparation .....	69
2. Staffing.....	70
3. Training.....	70
G. Detection and Analysis .....	70
1. Detection.....	70
2. Analysis.....	70
3. Incident Categories.....	71
4. Incident Reporting .....	72
H. Containment, Eradication, and Recovery .....	72
1. Containment.....	72
2. Eradication.....	72
3. Recovery.....	72
I. Post-Incident Activity.....	73

J. Escalation.....	73
K. Appendix A: Incident Response Team .....	75
L. Appendix B: Incident Response Process Tree .....	75
XXXIII. Policy Violations .....	79



## VII. IT ORGANIZATION



## VIII. POLICY:

## IX. INFORMATION SECURITY POLICIES

### A. PROHIBITED ACTIVITIES

CDB information must be used only for the business purposes expressly authorized by management. The following list of activities are a minimum subset of prohibited activities.

CDB expressly prohibits CDB workers from:

Uploading, downloading, printing, transmitting, and viewing any information (image, sound, program, or document) that could be deemed offensive, derogatory, harassing, on the basis of:

- Race,
- Gender,
- National origin,
- Sexual Orientation,
- Religion,
- Political Belief,
- Disability,
- Age.

Uploading, downloading, printing, transmitting, and viewing any information (document, image, sound, or program) containing the following without CDB and/or the author's authorization:

- Trade Secrets,
- Copyrighted Materials,
- Trademark Materials,
- Patented Materials,
- Other Confidential, Private or Proprietary Information or Materials, including all non-public Client material.

Using CDB computers to:

- Forge (or attempt to forge) electronic mail messages,
- Obtain unauthorized access or conduct tampering of the electronic mail of others,
- Send harassing, obscene and/or other threatening e-mail to others,
- Send unsolicited junk mail, "for-profit" messages, or chain letter messages,
- Gain unauthorized access to any computer system, including remote computers or other systems in any way,
- Damage, alter, or disrupt any computer system, including remote computers or other systems in any way,
- Participate in illegal activities,
- Decrypt system or user Passwords from any computer system, including remote computers or other systems in any way,
- Copy system files from any computer system, including remote computers or other systems in any way,

- Copy copyrighted materials, such as third-party software, without the expressed written permission of the owner or the proper license,
- Intentionally attempt to "crash" Network systems or programs,
- Attempt to secure a higher level of privilege on the Network,
- Willfully introduce computer programs into the organization Network or into external Networks,
- Willfully introduce computer viruses into the organization Network or into external Networks.
- Solicit business, sell products, or otherwise engage in commercial activities other than those required by their job responsibilities.
- Using anyone's code or Password without authorization,
- Allowing system access to non-CDB personnel without supervisor's and Information Technology's permission,
- Jeopardizing or breaching the security of CDB computer systems in any way,
- Excessive internet usage for non-CDB related matters,
- Tampering with any of CDB computer systems in any way.



## **X. INFORMATION SECURITY**

### **A. INFORMATION OWNERSHIP**

All information, data and documentation gathered by, generated by, or provided by CDB workers, in the course of their employment and/or utilizing organization owned assets for the CDB's business purposes are the property of CDB.

CDB has legal ownership of, or rights to, the contents of all files, information and messages stored or transmitted on its computer and network systems and reserves the right to examine all data stored in or transmitted by its computer and communications systems, without prior notice, whenever there is a business need which includes, but is not limited to, any investigation of unauthorized or inappropriate use of the systems or other investigation conducted with a business purpose. There should be no expectation of privacy associated with the information stored in or sent through CDB systems.

The use of encryption, the labeling of an email or document as private, the deletion of an email or document, or any other such process or action, shall not diminish the organization's rights to examine and review such information in any manner, as stated above. Unauthorized use of passwords/encryption to prevent CDB management from gaining access to a computer related resource is prohibited.

### **B. INFORMATION SECURITY INCIDENT REPORTING**

CDB workers must immediately report all suspected information security problems, vulnerabilities, unauthorized activity, and incidents to either their immediate manager or to IT. All suspected information security incidents must be reported as quickly as possible to CDB IT management.

## **XI. ACCESS CONTROL AND AUTHENTICATION MECHANISMS**

### **A. ACCESS PHILOSOPHY**

Access to CDB information must be granted only when a legitimate business need has been demonstrated and access has been approved in advance by the CDB worker's authorized supervisor. Network and/or system privileges of all users must be restricted based on the need for access.

### **B. ACCESS APPROVAL PROCESS**

All requests for new or changes to access privileges on CDB systems or networks must be submitted through BOSSDesk on a complete system access request form that is authorized by the CDB worker's immediate manager. The CDB worker's manager must initiate the access control approval process. The privileges granted will remain in effect until the user's job changes or he/she leaves CDB. If either of these two events occurs, the manager must notify IT immediately.

In accordance with the above, changes to access to Purchasing and Payment systems requiring defined authority levels of approvals per administrative, financial, purchasing, or other CDB policies, must be approved at one level above authority level being granted through BOSSDesk approvals. CDB IT will record all such changes and approvals for audit.

### **C. DEFAULT FACILITIES**

CDB workers that require access to network services will be granted basic information systems services such as electronic mail and word processing facilities. All other system capabilities and access to specific applications must be specifically requested and approved by the supervising manager. The existence of certain access privileges does not, in and of itself, mean that an individual is authorized to use these privileges. If CDB workers have any questions about access control privileges, they must direct these questions to IT.

### **D. DEPARTURES FROM CDB**

Any change in the employment status of CDB Workers must be immediately reported by management to IT. When a CDB Worker leaves the organization, all system privileges and access to CDB information must cease immediately. Departed CDB workers must not be permitted to continue to maintain an electronic mail account with CDB, unless specifically authorized by the City Manager. All CDB information disclosed to CDB workers must be returned or destroyed. All work done by CDB workers for CDB is CDB property and will remain with CDB when CDB workers depart.

### **E. UNIQUE USER IDs**

Each CDB worker will be assigned a unique user ID. All user IDs on CDB networks/applications must be constructed according to the CDB user ID construction standard and must clearly indicate the responsible individual's name. This user ID follows an individual as they move through the organization. It must be permanently decommissioned when a user leaves CDB. Re-use of user IDs is not permitted with the exception of re-hiring.



Users are responsible for all activity that takes place with their user ID and password or other authentication mechanism. User IDs are linked to specific people, and are not associated with computer terminals, departments, or job titles. With the exception of Internet pages, intranet pages, and other places where anonymous interaction is both generally understood and expected, anonymous and guest user IDs are not permitted unless approved in advance by IT.

The system privileges granted to every employee must be reevaluated by the user's manager every 12 months to determine whether currently enabled system privileges are needed to perform the user's current job duties.

The access for contractors and temporary workers will be set to expire after three months by default. The privileges of these CDB workers must be immediately revoked by IT when the project is complete, or when the contractor or temporary worker stops working with CDB. The relevant project manager must review the need for the continuing privileges of contractors and temporary workers every three months.

#### **F. SEGREGATION OF DUTIES**

Whenever a CDB computer-based process involves sensitive, valuable, or critical information, the system must include controls involving a separation of duties or other compensating control measures that ensure that no individual has exclusive control over these types of information assets.

System administrators managing computer systems with administrative privileges must have at least two user IDs, one that provides privileged access and the other that provides the privileges of a normal user for day-to-day work. All privilege access activity will be logged.

#### **G. PASSWORD POLICY**

All production information system user IDs must have a password to ensure that only the authorized user is able to utilize the user ID.

Every CDB user ID and related password is intended for the exclusive use of a specific individual; passwords are confidential and must not be shared. Users will be required to change passwords on a periodic basis and will not be able to use recent previously used passwords.

Passwords must be complex in nature, and use, when possible, a combination of at least 8 case-sensitive letters, numbers and special characters. Passwords must not employ any password structure or characteristic that results in a password that is predictable or easily guessed including, but not limited to, words in a dictionary, derivatives of user IDs, common character sequences or personal details.

All CDB applications that employ fixed passwords at logon must be configured to permit a maximum of three attempts to enter a correct password, after which the user ID is deactivated.

All vendor-supplied default passwords must be changed before any computer or communications system is used for CDB business.

A CDB worker must change their password immediately if they suspect that it has been discovered or used by another person. Users must notify the Information Technology Department the access control mechanisms are broken or if they suspect that these mechanisms have been compromised.



## **XII. PHYSICAL SECURITY AND REMOTE ACCESS**

### **A. ASSIGNED EQUIPMENT**

All hardware and software required by a user to perform their function must be procured through a BOSSDesk request to IT approved by the user's manager and according to CDB IT standards. CDB workers will ensure that all computer and communication assets that are assigned to or regularly used by them are maintained and used in a manner consistent with their function and such that the possibility of damage and/or loss is minimized. Damage to or loss of organization equipment caused by negligence and/or violation of this policy may result in the responsible party being charged for the repair or replacement costs. CDB workers must promptly report to their manager any damage to or loss of CDB equipment, software, or information that has been entrusted to their care.

Computer equipment and software provided by CDB must not be altered or added to in any way without Information Technology knowledge and authorization. Requests for changes to equipment or software must be submitted to IT.

### **B. ASSET INVENTORY**

All CDB servers, and communications equipment, personal computers, and peripherals must have a unique identifier attached, so that physical inventories can be efficiently conducted. IT will keep and maintain an inventory of production information systems detailing all existing production hardware, software, and communications links.

### **C. COMPUTER FACILITIES**

All production computer systems including, but not limited to, servers, firewalls, switches, routers, and voice mail systems must be physically located within a secure area. These computer facility rooms must be equipped with security mechanisms that protect against unauthorized access. Telephone closets, network router and hub rooms, voice mail system rooms, and similar areas containing communications equipment must be kept locked at all times and not accessed by visitors or non-technical personnel unless authorized by the CTD or Assistant IT Director and accompanied by an CDB IT resource.

### **D. REMOTE ACCESS**

Remote access to CDB internal LAN will not be granted to any CDB worker by default. Remote users must be authorized through the appropriate change procedures and subject to a controlled environment. CDB workers with remote access VPN capability (whether internal or external) are required to use their unique ID's and adhere to security policies and procedures governing the environment.

Employees working on CDB business at alternative work sites not within the LAN/WAN environment must use CDB -provided computer and network equipment, unless other equipment has been approved by IT as compatible with CDB information systems and controls.

### **XIII. INTERNET ACCESS AND EMAIL**

#### **A. USE OF FIREWALLS**

All connections between CDB internal networks and the Internet or any other publicly accessible computer network must include an approved firewall and related access controls. The internal system addresses, configurations, and related system design information for CDB networked computer systems must be restricted such that both systems and users outside the CDB internal network cannot access this information.

All CDB firewalls connecting to the Internet must be configured so that every Internet service is disabled by default, unless specifically allowed.

#### **B. INTERNET USE**

CDB may monitor and log Internet traffic of web sites visited by users and/or transmissions sent or received through corporate infrastructure. CDB Internet access is intended to further the business purposes of the corporation; incidental personal use of the Internet access is permissible, however, Internet sites containing pornography, sexist material, racist material, defamatory material, obscene material, pirated software, or any other inappropriate material shall not be accessed and is strictly forbidden.

#### **C. ELECTRONIC MAIL, INSTANT MESSAGING AND TEXT MESSAGING USE**

CDB Workers must not employ any electronic mail addresses other than official CDB assigned email addresses for all CDB business matters.

CDB workers must not create and send, or forward externally provided electronic mail, instant messages ("IM") or text messages ("TM") that use profanity, obscenities, or derogatory remarks, that may be considered defamatory, harassing, or explicitly sexual, or would likely offend someone based on race, gender, national origin, sexual orientation, religion, political beliefs, or disability, or that may contribute to a hostile work environment. Workers must not use CDB computer systems for the transmission of any type of unsolicited bulk electronic mail advertisements or commercial messages.

CDB workers should restrict their communications to business matters in recognition that CDB may employ automatic electronic mail content scanning tools to identify selected keywords, file types, and other information. All messages sent by electronic mail are CDB records; CDB reserves the right to access and disclose all messages for any business purpose without prior notice to anyone and supervisors may review the electronic mail communications of workers they supervise to determine whether they have breached security, violated organization policies, or taken other unauthorized actions.

CDB workers will not subscribe with their CDB assigned email addresses to any email lists that are not directly relevant to their assigned duties.

CDB workers have no reasonable expectation of privacy when using instant messaging. CDB reserves the right to monitor access and disclose all CDB worker IM messages. IM messages will be treated as business records that may be retained and used as evidence in litigation, audits, and investigations.

CDB workers must not use IM to transmit confidential, proprietary, or non-public information about



the organization, employees, citizens, business associates or third parties. Instant Messaging within CDB is intended for business use only. CDB workers are discouraged from wasting computer resources, work time sending personal IMs not related to business. CDB workers are to share their external IM user IDs with business colleagues strictly on a need-to-know basis.



## **XIV. MULTI-FACTOR AUTHENTICATION (MFA) POLICY**

### **A. INTRODUCTION**

This policy is to give the City of Delray Beach guidance to Multi-Factor Authentication (MFA) service, which helps deter the use of compromised credentials. The standards set forth in this policy are intended to minimize potential security risks which may result from unauthorized use of City computing resources. Cyber criminals and hackers are becoming cleverer in their efforts to not only steal information, but also modify data, remove data entirely, or spread malicious code, propaganda and spam. No organization is too big or small for such an attack. Password theft has also been on the rise with the use of methods such as key logging, phishing, and pharming. Requiring an additional layer of authentication will help alleviate the risk of a breach.

### **B. PURPOSE**

The purpose of this policy is to provide guidelines for Multi-Factor Authentication connections to the City network. This policy applies to any system that requires an additional layer of protection as determined by the City of Delray Beach Information Technology Department. Systems requiring multi-factor authentication include those supported by Information Technology as well as systems administered by non-centralized departmental IT staff. Systems requiring the use of multi-factor authentication include, but are not limited, to virtual private network (VPN), systems utilizing Single Sign-On (SSO), system administration tools, and privileged accounts.

### **C. DEFINITIONS**

MFA is a method of authentication that requires more than one verification method. This adds a critical second layer of security when users sign-in to their City Network and Office 365 account. It does this by requiring more than one method of verifying that it is really you logging into the account.

### **D. POLICY**

With new technological advances it is easy for individuals to inadvertently fall victim to highly sophisticated phishing attacks. This could give a hacker unauthorized access to our network and information system (Network). The Information Technology Department has taken several steps to protect and monitor our Network. As part of its efforts, the IT Department has established a Multi-Factor Authentication Policy (MFA Policy), which provides a common method of protection for organizations like ours, that utilize and store sensitive personal, and financial information. In order to access City resources, Office365 and the Network, all individuals will be required to engage in one additional step beyond the normal logon process. Individuals will be required to register a second approved device. The MFA system will send a message to the device which the individual must use to authenticate. Upon successful completion of this 2-step authentication process, the individual will be able to access the system.

### **E. ENFORCEMENT**

This policy regulates the use of all MFA access to the City network and users must comply with the IT Policies and Procedures Manual. Services will be terminated immediately if any suspicious

activity is observed. Service will remain disabled until the issue has been identified and resolved. Any CDB employee found to have intentionally violated the Acceptable Use Policy will be subject to loss of privileges. By choosing to use the City Network and Office365 service, you hereby agree to all terms and conditions listed above.



## **XV. SUPPORT SERVICES**

### **A. INFORMATION TECHNOLOGY ASSISTANCE**

All requests for IT assistance must be initiated through the CDB BOSSDesk Service Desk, in accordance with CDB's Incident Management Policy. This includes hardware and software problems and information requests.

A Service Desk request can be initiated by making a call to the local helpdesk extension 7191 or e-mailing a detailed description of the request to [ITSupport@mydelraybeach.com](mailto:ITSupport@mydelraybeach.com)

All IT change requests must be initiated through IT, in accordance with the CDB's Change Management Policy. This includes hardware and software configuration changes to CDB configuration items.

### **B. SOFTWARE DEVELOPMENT**

All CDB business applications that handle critical information and that have been developed by end users (including spreadsheets, databases, scripts or macros within office productivity software), must have appropriate controls approved by IT. All CDB production data and computer applications will only be modified by authorized personnel according to the appropriate Change Management procedures.

### **C. SOFTWARE PRODUCT LICENSES**

All software purchased by, licensed by, or created by CDB is the exclusive property of CDB and may not be transferred to, given to, or loaned to any other organization or outside individual without express written authorization.

CDB licenses the use of computer software from a variety of outside companies. CDB does not own this software or its related documentation and, unless authorized by the software manufacturer, does not have the right to reproduce it. Regarding use on local area networks or on multiple machines, CDB employees shall use the software only in accordance with the license agreement.

According to the US Copyright Law, illegal reproduction of software can be subject to civil damages and criminal penalties, including fines and imprisonment. CDB employees who make, acquire, or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances

### **D. PRODUCT REGISTRATION**

All 3<sup>rd</sup> party acquired products must be registered with the appropriate vendors immediately after CDB technical staff takes delivery of new or upgraded information systems products, or soon after it has been determined that such products are not yet registered.



## **XVI. OPERATIONS MANAGEMENT**

### **A. COMPUTER VIRUSES**

All computers, servers, or network devices susceptible to computer virus infestation will be protected by corporate anti-virus programs. Virus screening software will be installed and enabled with real-time functionality on all CDB local area network servers, and networked personal computers and will be configured to be automatically update virus definitions.

Any user who suspects infection by a virus must immediately shut-down the involved computer, disconnect from all networks, contact the IT Service Desk, and make no attempt to eradicate the virus.

Workers must not download software on any computer system property of CDB. Users must not install software on their workstation computers, network servers, or other machines without receiving advance authorization to do so from IT. Users will exercise extreme caution in downloading and executing any files attached to email.

### **B. CRITICAL DATA LOCATION**

CDB users must not store confidential or critical business information on workstation hard disk drives. This type of information must reside on security protected server shares.

### **C. SYSTEM LOGON BANNER**

Logon screens for computers and/or network devices must include a special notice that must state that the system may only be accessed by authorized users, users who logon represent that they are authorized to do so, unauthorized system usage or abuse is subject to criminal prosecution, and system usage will be monitored and logged. By logging into this Computer and the City of Delray Beach network, I have read, understand, and will comply with the City of Delray Beach Information Technology Policies and Procedure Manual.

### **D. AUDIT LOGS**

All production application systems that handle critical CDB information must generate logs that capture user-initiated logon attempts (successful or failed), addition, modification, and deletion transactions, user session activity including user IDs, logon date and time, logoff date and time, changes to the privileges of users, and system start-ups and shut-downs if the subject application system is able to produce such audit logs.

### **E. DATA BACKUPS**

All critical business information and critical software resident on CDB server systems must be periodically backed-up for recovery purposes. The rotation, recycling of the media used for backups and the storage location used will be defined by IT, as per the business requirements.

### **F. DISASTER RECOVERY PLAN**

IT will assist in the preparation, periodical update, and testing of a disaster recovery plan that will permit all critical computer and communication systems to be available in the event of a major loss such as may be caused by the event of nature or a catastrophe.

## XVII. USERID AND PASSWORD

- All users of the CDB internal network, or the Enterprise Resource Planning (**ERP**) servers are required to have a user profile, with secure passwords to access the resources.
- Every workstation must have a password-protected screen saver.
- Every user is held accountable of his / her activity when using a CDB workstation, ERP server, or when connected to the CDB network.
- Every user must keep his / her password confidential; it is forbidden to share user credentials to other users. All IT activity is traced by the IT Department.
- If a user detects his / her credentials have been compromised, the user must immediately change his / her password, and proceed to notify IT of this event.
- User passwords must comply to the requirements below:
  - a. Password minimum length: eight (8) characters.
  - b. Password usage: must not be identical to the previous ten (10) passwords.
  - c. Password validity: Ninety (90) days
  - d. Password components restrictions: Password must contain at a minimum three of the following four items: alphanumeric characters (A-Z) upper case and/or lowercase, numeric characters (0-9), non-alphanumeric characters (symbols) ~!@#\$%^&\*()\_-=`[]\{}|:;'"<>.,?/
- Department Heads will notify IT department (through the BOSSDesk IT Service Desk) and HR Department of the termination or suspension of an employee, for IT to deactivate and / or delete that employee's user profile(s) from all CDB IT systems. In case there is a possible risk for the confidentiality and integrity of the CDB information, the respective Department Head must contact the IT CTD or Assistant Director immediately by phone.
- To request access for a CDB employee to an IT system (hardware / software), the corresponding Department head or Designee will submit an Employee – New Hire request in the BOSSDesk Service Catalog Service Desk System, containing the following information:
  - a. Department / Division
  - b. Full name of user
  - c. Hardware / software access required.
  - d. Application information (needed for CDB network and ERP setup)

Human Resources will approve the BOSSDesk request, and IT will process the request and return the credentials information to the requesting Department Head.



When a CDB worker is hired or otherwise engaged, it is the responsibility of the Human Resources Department to verify that the new Information User has been provided with the IT Policies documentation, collect the signed **Agreement to Comply** and request the appropriate access to the IT environment.

When a CDB worker leaves the organization, it is the responsibility of the worker's immediate Manager and the Human Resources Department to promptly inform IT that the privileges associated with the CDB worker's user ID must be revoked. User IDs are specific to individuals, and must not be reassigned to, or used by, others. Shortly after separation from CDB, a CDB worker's manager is additionally responsible for reassigning the involved duties and files to other workers.



## **XVIII. ELECTRONIC SYSTEMS AND COMMUNICATION TOOLS**

All electronic systems, hardware, software, temporary or permanent files and any related systems or devices are the property of the City of Delray Beach. These include, but are not limited to computers, terminals, network equipment, communications equipment, software, voice mail, E-Mail, documents, spreadsheets, calendar entries, appointments, tasks and notes which reside in part or in whole on any CDB electronic system or equipment.

Department Heads and supervisors have the authority to inspect the contents of any equipment, file(s), calendars, or electronic mail of their subordinates in the normal course of their supervisory responsibilities. IT staff shall extract information, files, documents, E-mail, phone reports, etc., when requested by authorized supervisory personnel. Such requests must be submitted to the IT Department in the BOSSDesk Service Desk System and approved by the requesting Department Head. Reasons for review include, but are not limited to system, hardware or software problems, general system failure, a lawsuit against the City of Delray Beach, suspicion of a crime or violation of policy or a need to perform work or provide service when the employee is not available. Employees should have no expectation of privacy in their E-Mail messages.

### **A. USE OF ELECTRONIC COMMUNICATION AND INFORMATION SYSTEMS**

Electronic systems, hardware, software, communications tools, and information are provided for the purpose of conducting business for the City of Delray Beach.

The following are the allowable uses of the City of Delray Beach's electronic communication and information systems:

- a. To facilitate performance of job functions.
- b. To facilitate the communication of information in a timely, efficient manner.
- c. To coordinate meetings of individuals, locations, and City resources.
- d. To communicate with Departments/Divisions throughout the City.
- e. To communicate with outside organizations as required to perform an employee's job functions.

Prohibited uses of electronic systems and information include, but are not limited to, the following:

- a. Illegal activities
- b. Threats
- c. Harassment
- d. Slander
- e. Libel
- f. Obscene or sexually suggestive messages, offensive graphical images, offensive pictures

- g. Political endorsements, except during an official, authorized City investigation
- h. Content that would likely offend someone on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability, or that may contribute to a hostile work environment.
- i. Commercial activities
- j. Using non-business software, including games or entertainment software
- k. Employees are not permitted to share their passwords. E-Mail access or message distribution by another employee is prohibited without authorization.

#### **B. EMAIL SPECIFIC GUIDELINES**

Email is provided by CDB for employees, contractors and Board members to conduct City-related business. The use of email for personal use during work time is prohibited. Personal use should be limited to breaks or before or after work. Abuse of this medium may result in disciplinary action, up to and including termination.

All Email users are to use email as they would any other type of official City communications tool. This implies that when any email is transmitted, both the reader and the sender should consider if the communication falls within the established guidelines. These guidelines include, but are not limited to, ensuring that the communication is not perceived to be a conflict of interest or unethical. Communication containing confidential information should be sent in an encrypted format. Exercise the same care in drafting email messages as if it were being read in public.

Communication by email is encouraged when it results in the most efficient and/or effective means of communication. The sender of email messages must retain the primary responsibility for seeing that the communication is received by those intended. Please remember that some personal information is NOT public information (i.e., Social Security Numbers of any City employee, home addresses and telephone numbers of Police Officers, Firefighters, Code Enforcement Officers, or family members residing in their households) and, therefore, should not be distributed. E-Mail messages sent within a Department shall not contain confidential and/or exempt documents as attachments. If there is a shared server within the Department, the sender of the E-Mail message shall reference the location of the document in the shared server for the recipient without attaching the document to the E-Mail message.

**NOTE:** Be aware that even after E-Mail has been "erased" or "deleted", it may still reside in back-up files and stored printouts.

Email regarding City business sent to or drafted by a representative of a public agency, including a local government, becomes a public record for that agency pursuant to Chapter 119, Florida Statutes and such e-mail must be retained in accordance with record retention requirements as set forth by the Florida Department of State.

Personal and private e-mails (not relating to City business) are NOT considered public record.



## **XIX. REMOTE ACCESS**

### **A. VPN OVERVIEW**

This remote access policy identifies the standards for remotely connecting to the City of Delray Beach network and applications, as well as the security standards for computers that can connect to the organizational network.

This Remote Access Policy specifies how remote users can connect to and the requirements for each of their systems before they can connect to the City of Delray Beach network. This will specify:

1. Anti-virus program remote users must use and how often it must be updated.
2. Personal firewalls to secure devices
3. Other protection against spyware or other malware.

### **B. VPN STANDARDS**

The purpose of this policy is to define standards for connecting to the City of Delray Beach's network using the Internet or any other public/private network, from a remote capable, City furnished, device. These standards are designed to minimize the potential exposure to the City of Delray Beach from damage which may result from a remote access connection. Damage includes the loss of sensitive or confidential data, damage to public image, damage to critical City of Delray Beach internal systems and to other hosts (i.e., other devices that are connected to the same local area network as the connected remote computer.)

This policy applies to all City of Delray Beach's employees, contractors, vendors, Commission members, CRA staff and any other individuals requesting remote access to the City's network. This policy applies to remote access connections granted to perform City work from remote locations including the home and when traveling. Simply accessing e-mail from home or when traveling can be accomplished via Office 365 email portal. This policy covers the situation where special access is granted to the network to access servers and systems located behind the firewall. Such access is required to work with City applications and ERP applications. The "normal" Outlook client is accessible as is the Internet via the City's Internet connection.

Remote access implementations that are covered by this policy include any transit of data between any client and City of Delray Beach systems and/or applications.

### **C. VPN POLICY**

1. Users granted the privilege of remote access must understand that all the regulations and restrictions that apply to computer usage within the City apply identically remotely. All Internet use is tracked, (for example), and there is no expectation of privacy.
2. The City of Delray Beach employee is responsible to ensure that only authorized users can use city-owned equipment. Family members are not allowed to use the remote access to



access the Internet, for example. The City of Delray Beach employee bears responsibility for the consequences if the access is misused.

3. Users must be familiar and understand the details of protecting information when accessing the City network via remote access methods and adhere to the acceptable use of City of Delray Beach's network.

#### **D. VPN PROCEDURE**

1. To be approved for accessing the City's network remotely, a Request for Remote Network Access Form must be filled out in the BOSSDesk Service Catalog and approved by the respective department head prior to the IT Department configuration.
2. Once approved, remote access hardware will be configured (on City owned device) or user will be advised of any required configuration and/or setup. The IT Department will work with user on testing the approved access.

#### **E. VPN REQUIREMENTS**

1. Secure remote access must be strictly controlled. Control will be enforced via password authentication and host identification (workstation/laptop/tablet/smartphone).
2. At no time should any City of Delray Beach employee provide their login or email password to anyone, not even supervisors or family members.
3. Remote access users must ensure that their City-owned personal computer or workstation, which is remotely connected to the City of Delray Beach's corporate network, is not connected to any other network at the same time. In other words, when connected via an air card or other Internet connection for the purpose of remote access, the user must not connect to the web via wireless, for example, for simultaneous browsing. The City owned PC must never be connected to a personal network.
4. Non-city-owned hardware can access city applications and systems via approved client software and programs. However, City IT Department support will be limited to application usage, as outlined in bullet 9 below.
5. City of Delray Beach employees and contractors with remote access privileges to the city's corporate network must not use non-City of Delray Beach email accounts (i.e., Gmail, Hotmail, Yahoo, AOL), or other external resources to conduct City of Delray Beach business, thereby ensuring that official business is never confused with personal business.

6. Once the remote access is authenticated and connected, all Internet transmissions will be conducted over the City of Delray Beach Internet connection. As such, all usage will be regulated as per the End User Computing Policy.
7. Reconfiguration and/or setup of a home user's equipment for the purpose of remote access, split-tunneling or dual homing is not permitted at any time.
8. Non-standard hardware configurations and non-standard remote access solutions are not permitted at this time.
9. Vendors temporarily allowed access to the network for application software installation or remote debugging must also ensure that they have their operating systems up to date and must use the most up-to-date anti-virus software.
10. In terms of support, the IT Department's responsibility will be to configure and test the city-owned devices. IT can only advise on the standard practices used to connect using external internet access, such as cable modems, DSL, etc. The only fully supported remote access solution is a City-owned laptop configured with a City-issued broadband access air card.

#### **F. VPN ENFORCEMENT**

Violations in policy could result in progressive disciplinary action dealt with through normal disciplinary processes within each department.

While monitoring, any computers/connections found not to be in compliance will be disconnected from the network until they can be properly configured.



## **XX. SECURITY EDUCATION TRAINING AND AWARENESS (SETA) POLICY**

### **A. PURPOSE STATEMENT**

To establish a formal, Security, Education, Training, and Awareness (SETA) program for the City of Delray Beach. A strong information SETA program requires all users to be proficient in understanding security policies, procedures, and technical security controls. All City staff members need to have the necessary skills to carry out their assigned duties in a safe and secure manner. This policy promotes continuous employee training around data security and privacy education. The City of Delray Beach utilizes KnowBe4 for Phishing Campaigns and Security Training.

### **B. POLICY PURPOSE**

The purpose of this policy is to help ensure that all City staff are aware, understand, and apply security awareness in order to protect the City's information systems, Personally Identifiable Information (PII), and other sensitive information by ensuring information confidentiality, integrity, and availability (CIA) of data. The quality and integrity of the City's SETA program ensures that all City staff, understand the security implications of their actions and increases the likelihood that information system security will not be breached, either intentionally or unintentionally, through technical measures (such as hacking) or non-technical measures (such as social engineering). The goal of this policy is to ensure that all City staff understand the risks of using information technology, how to defend against malicious threats, and how to react to information security events or incidents, whether at work or at home. Without such training, information systems users have an increased likelihood of breaching security and have lower individual fault should they breach security.

### **C. POLICY SCOPE**

This policy applies to all City employees, including full-time staff, part-time staff, vendors, contractors, freelancers, and other agents who utilize City or personally owned systems to access the organization's data and networks. This Security Awareness Training Policy applies to all users of all information systems that are the property of City of Delray Beach. Specifically, it includes:

- All employees, whether employed on a full-time or part-time basis by City of Delray Beach,
- All contractors and third parties that work on behalf of and are paid directly by City of Delray Beach,
- All contractors and third parties that work on behalf of City of Delray Beach but are paid directly by an alternate employer,
- All employees of partners and clients of City of Delray Beach that access City non-public information systems.
- 

### **D. CJIS SECURITY POLICY RELATIONSHIP TO LOCAL POLICY**

The Criminal Justice Institute Services Security Policy herein known as the CJIS Security Policy may be used as the sole security policy for the municipality. The local municipality and/or local



agency may complement the CJIS Security Policy with a local policy; however, the CJIS Security Policy shall always be the minimum standard; however, the local policy may augment, or increase the standards, but the local policy shall not detract from the CJIS Security Policy standards.

**E. DEFINITIONS**

<b>Terms</b>	<b>Definitions</b>
Security Education Training & Awareness Training (SETA)	A formal process for educating employees about computer security.
Breach	Any incident that results in unauthorized access of data, applications, services, networks, and/or devices by bypassing their underlying security mechanisms.
Personal Identifiable Information (PII)	Any sensitive data that could potentially identify a specific individual.
Confidentiality	A set of rules and controls that limits access to information.
Integrity	An assurance that information is trustworthy and accurate.
Availability	A guarantee of reliable access to information by authorized people.
Security Audit	A systematic evaluation of the security of a company's information system by measuring how well it conforms to IT policies.

**F. POLICY**

**1. BASIC SECURITY REQUIREMENTS**

- The City of Delray Beach will ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.
- All City department heads, or directors and mid-level managers must ensure that all City staff within each respective department are adequately trained to carry out their assigned information-security-related duties and responsibilities.
- Periodic security audits shall be performed by the IT department to verify compliance and assess effectiveness of training.

## 2. DERIVED SECURITY REQUIREMENTS

- Security awareness training will be provided to ensure all parties within the scope of this policy can recognize and report potential indicators of all physical and logical threats.
- Upon completion of security awareness training, all employees will be required to sign a declaration that they have completed training, understand the purpose of the training and the specific procedures taught, and that they intend to abide by City of Delray Beach's security policies.
- All City employees are required to complete security awareness training within 30 days of starting work or the deployment of a new or significantly updated/revised information system and thereafter on an annual basis. Upon completion of security operations training, all employees will be required to sign a declaration that they have completed the training, understand the purpose of the training and the specific procedures taught, and that they intend to abide by City of Delray Beach's security policies.
- Security awareness and training will be ongoing at the City of Delray Beach via monthly Phishing, Vishing, and/or Smishing campaigns, bi-annual Cybersecurity awareness training campaigns, monthly newsletter and weekly email news blasts, and training on existing City-wide policy and procedures. All City employees will be kept up to date on new improvements or threats of which to be aware. These can be distributed by email, posters, work newspapers, or meetings.

### G. NON-COMPLIANCE

Violations of this policy will be treated like other allegations of wrongdoing at the City of Delray Beach.

Any user under scope of this policy and procedures must adhere to the stipulated requirements. Any user that is in violation of the parameters of this policy or procedure will be considered non-compliant and will require enforcement actions according to the severity and nature of the incident. Users may be considered non-compliant if:

- A user fails to complete Annual awareness training within 30 days,
- A user fails to complete remedial training within 7 days,
- A user fails periodic assessments,
- A user continually fails to carry out expected actions from awareness and training.

Non-compliant users email account and network access will be suspended, and their supervisor notified. Email account and network access will be restored upon successful completion of the assigned semi-annual or remedial training.

Any user under scope of this policy who fails to adhere to the policy may be subject to disciplinary action up to and including termination. Violation of any of the constraints of these policies or procedures will be considered a security breach and depending on the nature of the violation, various sanctions will be taken.



## **XXI. INTERNET**

Use of the Internet is becoming increasingly necessary for CDB employees to provide superior customer service. The efficient utilization of the Internet for communications and research can improve the quality, productivity, and general cost effectiveness of the City's work force. The effective performance of computer and telecommunications networks, whether local or global, relies upon users adhering to established standards of proper conduct. The purpose of this policy is to ensure the proper use of this resource via the City's Internet account.

Regardless of the user's location when using the City's Internet account, during work time only City business is to be conducted via that access. In general, such access requires appropriate, efficient, ethical, and legal utilization of network resources.

### **A. INTERNET USE GUIDELINES**

- a. Employees are expected to exercise good judgment while using the Internet.
- b. Access to the Internet via the City's account is to be used for City business and must be supportive of organizational objectives and be consistent with the mission of the City of Delray Beach.  
Use of City access to the Internet by employees for personal use during work time can constitute neglect of job duties, which will result in disciplinary action up to and including dismissal. City employees shall be responsible for any personal charges arising from use of the City's Internet account.
- c. It is the responsibility of each Internet user to ensure they follow all City policies, including computer security and virus detection.
- d. Avoid uses of the Internet that reflect poorly or unprofessionally on the City.
- e. CDB employees should take the proper precautions and virus scan all files which are downloaded from the Internet.



## **XXII. HARDWARE, SOFTWARE AND DATA RESOURCES**

Each department is responsible for the implementation of and compliance with the following guidelines:

- a. Only IT approved hardware and software are to be used.
- b. IT is the only Department to authorize the installation of hardware and/or software.
- c. IT will not provide support to non-authorized hardware and/or software.
- d. All relocation of hardware or software resources will be authorized by and coordinated through the IT Department.
- e. Password security is to be treated the same as and regarded as sensitive information.
- f. Surge protection will be used on all hardware devices.
- g. Only approved department/division personnel or personnel approved by IT and HR shall have access to IT resources.
- h. All data shall reside on the City network.
- i. All hardware and software are to be kept in a safe and secured physical location.
- j. Hardware and optical / magnetic media are to be kept clean and not exposed to magnetic fields or extreme temperatures.
- k. Drinks and food should be kept away from any hardware and storage media.
- l. Use of resources outside CDB's facilities must be approved by Department Heads and/or the City Manager. Resources include but are not limited to software, Laptops, and/or other devices used for official city business.
- m. All software that is developed by an employee of the City is the property of the City of Delray Beach.
- n. Personal software shall not be installed nor is it permitted on any equipment owned by the City. All software that has not been acquired by the City is considered unauthorized and is not permitted on any City equipment.

## XXIII. TECHNOLOGY REPLACEMENT AND UPGRADE POLICY

### A. REPLACEMENT PURPOSE

Adequate computer and network hardware and software are essential to the delivery of City services, including Public Safety, Community Development and Improvement, and Parks and Recreation, and to the efficient and effective management of the City. Rapid changes in technology require that a well-managed City have a systematic plan for upgrading and replacing technology to ensure that it offers access to the most basic services.

Outside threats from those who would do harm to City infrastructure to disrupt government and public order requires that the City replace equipment and software in order to accommodate the latest defense mechanisms.

This document defines City of Delray Beach policy regarding the replacements of all City-owned technology equipment at the end of its life cycle and upgrades of City-wide software.

### B. REPLACEMENT SCOPE

This Policy applies to all City-owned workstations, laptop computers, iPads, desktop peripherals (printers, scanners, projectors, and interactive whiteboards), network hardware (servers, switches, routers, bridges, and other key network devices), cable plant and physical infrastructure, and the City-wide software (Microsoft Operating System, Microsoft Office Suite including Office 365, Tyler Technologies, Central Square/Superion, CityWorks, and other site-licensed desktop applications) running on those devices.

### C. REPLACEMENT ROLES AND RESPONSIBILITIES

**Administration/Department Heads** - Each department head is responsible for identifying any exceptions (earlier or delayed replacements/upgrades) necessary to ensure an employee can effectively perform his/her job duties. The Director of each department is responsible for reviewing and approving requested exceptions and divisional budgets and escalating those requirements to Information Technology for inclusion into the City budget.

**Information Technology Department** - This group is responsible for generating and monitoring inventories, budgeting for replacements and upgrades and executing equipment replacements and upgrades to City-wide hardware and software according to the replacement cycle. This group also makes technical decisions on equipment and software standards and upgrades and replacements based on industry trends, software development cycles, costs, and risks to systems stability.

### D. REPLACEMENT POLICY STATEMENT

The City of Delray Beach will maintain modern computer and network hardware and software capable of supporting Public Safety, and other City objectives and business activities. The risk of exploitation and penetration of these systems that could affect the public interest is mitigated by prudent, systematic replacement and upgrades of systems and software.



To accomplish this, technology hardware will be budgeted for replacement through the City IT budget and replaced and upgraded according to the schedule below.

<b>Category</b>	<b>Description</b>	<b>Replacement Timeframe</b>
High-performance Servers	This category encompasses all high performance and high-use servers. These servers perform mission critical activities and/or provide access to critical services daily. Storage Arrays without Spinning Disks are considered High Performance Servers. Primary financial systems, systems that manage telephone systems and Police E911 systems are explicitly included in this category.	Fiscal year immediately after 4th year of use
Laptop Computers	This category encompasses all laptop systems and includes all associated docking stations and monitors as a single unit.	Fiscal year immediately after 4 <sup>th</sup> year of use
Workstation Computers	This category encompasses all desktop computer systems and includes the CPU and monitor as a single combined unit.	Fiscal year immediately after 5 <sup>th</sup> year of use
General Use Servers	This category encompasses all servers not classified as "high-performance". These servers provide mission-essential services and perform activities supporting the service and business goals of the institution. Storage Arrays with spinning disks are considered General Use Servers.	Fiscal year immediately after 5 <sup>th</sup> year of use
Network Hardware	Network hardware includes repeaters, routers, switches, bridges, access points and other communication devices.	Fiscal year immediately after 5 <sup>th</sup> year of use
Surveillance Cameras	All Surveillance Cameras mounted inside or outside.	Fiscal year immediately after 3 <sup>rd</sup> year of use.
Desktop Peripherals	Desktop peripherals include printers, scanners, projectors, and interactive whiteboards.	Fiscal year immediately after 7 <sup>th</sup> year of use
Cable Plant and Physical Infrastructure	The copper and fiber optic wires that connect data/information stations together and comprise the network infrastructure are the components identified in this last category.	Fiscal year immediately after 10 <sup>th</sup> year of use

If a hardware item is determined to be irreparable by IT or if the cost to repair exceeds the current market value of the item, the item may be replaced earlier than indicated in the table above with all costs for replacement covered by the City IT Repair and Replacement budget. If a department elects to replace an item earlier than the identified replacement cycle, the City

Manager, IT, the budget officer, and Department Head over the reporting line must approve the request and the electing department assumes all costs for replacing the item.

**E. REPLACEMENT RISK MITIGATION**

If any hardware or software is determined to present a risk to the IT infrastructure of the City, it will be replaced with all costs for replacement covered by the City IT Repair and Replacement budget or in accordance with Risk Management guidelines.

**F. REPLACEMENT SOFTWARE UPGRADES**

Related to software, all systems should be running the current version or most recent prior (current -1) version of manufacturer-released software packages. If a City-owned system is found to be running an older version (current -2 or older) of any institution-wide software package (Microsoft Operating System, Microsoft Office Suite, or other site-licensed desktop application), it will be upgraded to the most recent version as soon as possible.

**G. REPLACEMENT REQUIREMENTS**

All replacements will adhere to a single standard for each equipment type. Departments must surrender a like device (computer, peripheral, etc.) for each device replaced. Departments may not repurpose existing devices to expand the number of technology devices supported. All enhancements to or changes from the standard resulting in a cost-higher than that of the standard will be charged to the requesting department's budget.

If a department keeps or maintains any special-purpose software or peripherals, they must be compatible with the new equipment and all institution-wide software packages. Otherwise, the department is required to purchase the software or peripheral upgrade.



## **XXIV. PRINT SERVICES GOVERNING PRINCIPLES**

### **A. UTILIZATION/PRACTICES**

- We communicate electronically and print only when necessary.
- We will simplify output processes by leveraging technology to realize productivity gains through workflow and print process automation.
- We will focus on reengineering paper intensive processes to facilitate the electronic movement information through our environment.
- Workflow solutions should be simple for our users to utilize and stable to support.

### **B. DEPLOYMENT AND CONFIGURATION**

- Print devices will be shared resources on the network.
- Print resources will be standardized across the managed fleet as much as possible.
- Duplex printing can be our standard device default setting where appropriate.
- Where multiple input trays are being used for special stocks in current state, this configuration must also be available in the rationalized state and within the distance parameters.
- Special features such as tabloid size trays will be specified only when required.
- All MICR check printing devices will remain in their respective locations.

### **C. SECURITY AND COMPLIANCE**

- Device configurations will be password protected.
- Secure printing capabilities will be available.
- Badge access will be required for print and copy jobs.

### **D. FINANCIAL MANAGEMENT**

Usage will be monitored at the device level. CDB IT team will administer the reporting for all print output device usage.

### **E. CONNECTIVITY AND DRIVER DEPLOYMENT**

Print queues will be the standard for connectivity with the managed fleet.

Queues provide/enable:

- Ease of connecting to a device without administrative rights.
- Policy enforcement (duplex, color, etc.)
- User utilization tracking.
- Print driver management.
- Printer naming convention will be the fully qualified DNS name.

### **F. PRINTER / COPIER DEVICE PLACEMENT PRINCIPLES**

End-users must not have to use stairs, pass into or out of a secure area, or pass-through doors

to access their primary mono letter printer.

- The preferred user to device distance for a primary monochrome device should be approximately 100 radial feet where facility layout permits.
- Providing standard capabilities and placement is intended to minimize device moves required in response to individuals' moves.
- Color will be produced on laser devices, which will be centrally located in each building/work area where possible or specifically where color-enabled devices are needed.
- MICR check printers will remain in their respective areas as necessary.

Note: Specific business process requirements or end-user accessibility considerations may necessitate exceptions to these guidelines.

#### **PRINTER / COPIER ON-GOING MANAGEMENT PROCEDURES**

##### **G. STRATEGIC DEPARTMENT CONSOLIDATION (DEPARTMENT BY DEPARTMENT)**

This process utilizes our baseline information and future-state design. Many aspects of consolidation have been taken into consideration including:

- 1) TCO of the devices
- 2) Service call history and age
- 3) Business processes and proximity to users
- 4) Age of the devices
- 5) Compatibility with print behavior modification software

This will be an initiative that will "attack" high-cost devices and those that are underutilized to achieve a more cost effective footprint of devices. Inherent in this model, print volume will be migrated to those shared devices with lower cost of ownership. Therefore, you will have a "rolling" rationalization project, where the designed future-state will be achieved through an initial implementation process and where the IT Department will continuously improve the printing environment over the life of the partnership as laid out in the print policy.

##### **H. TACTICAL DEVICE CONSOLIDATION (DEVICE BY DEVICE)**

This process will also utilize our baseline information and future-state design. We will use reports such as (but not limited to):

- 1) Top 20/Bottom 20 devices by Usage
- 2) Top 20/Bottom 20 devices by Utilization
- 3) Excessive Service Calls
- 4) Top Expensive Devices
- 5) Oldest Deployed Printer Models

This approach will not follow a process whereby the IT Department will "Right-size" a department at one time as during the initial implementation of the future-state design but will use the data provided in the management reports to cull the environment over time. The goal



of this activity will be similar to the strategic consolidation but will look to remove devices on a monthly basis based on that device's use and per the print policy to continuously drive down costs and improve the printing environment.

#### **I. PLANNING AND ACQUISITION**

- City of Delray Beach has standardized with Canon USA on a limited number of output devices by type and manufacturer. These are pre-determined in the procurement process.
- All new acquisitions requests will be submitted through City of Delray Beach IT to the Canon USA team. The Canon USA team will determine the feasibility of the acquisition and decide of its level of adherence to the print policy, the needs of the individual or department and TCO of the investment.
- Additional standard printers, beyond the corporate infrastructure provided, must be requested through a defined exception process. Upon receipt of an approved request, City of Delray Beach IT and Procurement office will coordinate the acquisition and deployment of such requested hardware.
- Employees may not purchase printers, supplies or maintenance outside of the defined process.
- The IT Department will budget for Lease amount and usage per page cost. These will be expensed out of the IT Department budget through monthly invoices.

#### **J. MAINTENANCE AND SUPPORT**

- Support of all printer or multifunctional equipment must be requested through the City of Delray Beach IT Department work order system.
- City of Delray Beach IT will contact Canon USA for support.
- Canon USA's off-site managed services center will manage maintenance and service calls of all print output equipment.
- Canon USA's off-site managed services center will monitor device status and provide real-time support.
- Consumable's fulfilment will be completed by Canon USA's off-site managed services center. The workflow for end-users will be the same as today when service is placed on any copier.
- All support processes will be standardized and mapped to business need to enable best in class customer service.
- Each device will have a defined criticality level.
- All consumable items will be recycled where appropriate.
- Training regarding the use and features of copiers is always available to end-users and supported by the CDB IT team.

**K. RETIREMENT AND DISPOSAL**

- Technology will be refreshed based on a lifecycle of 48 months.
- The CDB IT team will be responsible for removal, refresh, and disposal of all leased copier assets.
- The CDB IT team will be responsible for removal, refresh, and disposal of all City of Delray Beach owned printer assets.

**L. PRINTER / COPIER EXCEPTION APPROVAL PROCESS**

- All exceptions to processes outlined in this policy document must receive approval.
- Any purchase exceptions to the policy must have approval prior to purchase.
- Retention of any existing device outside of the scope of this policy must receive approval at the time of rationalization recommendation.
- All exceptions must be approved, in writing, by the City of Delray Beach IT and Procurement departments.



## **XXV. THIRD PARTIES AND THIRD-PARTY PERSONNEL**

### **A. THIRD PARTY PERSONNEL USER IDS**

All requests for new or changes to access privileges on CDB systems or networks for Third Party Personnel must follow the same request and authorization process as for CDB workers. The service request must be submitted to the IT Service Desk. The access for Third Party Personnel will be set to expire after 3 months by default, however the privileges of these non-employees must be immediately revoked by IT when the project is complete, or when the non-employees stop working with CDB. The relevant project manager must review the need for the continuing privileges of non-employees every three months.

### **B. THIRD PARTY PERSONNEL REMOTE ACCESS**

Inbound dial-up, inbound Internet, remote desktop or virtual private network privileges must not be granted to third-party vendors unless the relevant project manager determines that these vendors have a legitimate business need for such access provided that these privileges are enabled for specific individuals and only for the period required to accomplish approved tasks.

### **C. THIRD PARTY COMPLIANCE AND NON-DISCLOSURE AGREEMENTS**

Acknowledgment and compliance for Third Party Personnel shall be accomplished by inclusion of applicable reference language in contracts and agreements with Third Parties. All disclosures of confidential or critical CDB information to third parties must be accomplished through a signed Non-Disclosure Agreement that includes restrictions on the subsequent dissemination and usage of the information.

### **D. NETWORK CONNECTED THIRD PARTY SYSTEMS**

To gain access to the CDB computer network, every Third-Party Personnel must secure its own connected systems in a manner consistent with CDB requirements including, but not limited to, virus and spam control measures, the right to audit the security measures on these connected systems without prior warning, as well as the right to immediately terminate network connections with all third-party systems if considered necessary by IT.

## **XXVI. BOSSDESK SERVICE DESK**

### **A. PURPOSE**

The City of Delray Beach IT Department utilizes the BOSSDesk Service Desk tool for all work orders following ITIL and ITSM conventions. There are sections following in this manual for specific ITIL processes.

- Incident Management
- Request Management
- Problem Management
- Change Management

BOSSDesk is configured with a Service Catalog depicting all the services offered to City of Delray Beach employees. Use of the incident and request modules within the Service Catalog expedites IT services with pre-programmed workflows and solutions. BOSSDesk also includes a Knowledge Base with self-service solutions and End user instructions for common issues.

Service Catalog items have been created for Police Department and Fire Department which are only visible to those Departments. Those tickets are automated with workflow to be assigned to Police and Fire IT personnel.

### **B. APPROVALS**

BOSSDesk utilizes a digital approval process for requests of User Add/Remove, equipment, ERP access change and Change Management. When a request is entered which requires an approval, an email is sent to the approval board and the ticket remains on hold until acted upon and the approval has been sufficed. All approvals are logged in the BOSSDesk system and can be printed out or saved to pdf file.

### **C. EMPLOYEE RELATED REQUESTS**

All requests for Employee – New Hire, Employee – Termination, and Employee – Job Change / Name Change should be entered by the requesting Department. The Department would have all of the required information for the employee filled out in the request. There is automated workflow configured into the BOSSDesk tickets to request the appropriate approvals from the HR team prior to any work commencing on the ticket.

Requests also need to be entered for any outside agencies or contractors / vendors requiring access to the City network, applications, or data resources. UserIDs are setup on a named user basis and not Generic for a position.

### **D. IT DEPARTMENT USE OF BOSSDESK**

The IT Department has Created Service Catalog items solely for use of the IT Team.

- IT Vacation Requests are tracked and approved in the BOSSDesk system.
- Change Management and Server Patching requests are tracked and approved in the BOSSDesk system.



- Daily Tasks are Scheduled for General IT, Infrastructure and Security Tasks.
- IT Documentation requests
- New Server and Decommission Server tasks as well as Infrastructure Modifications.

All Data Backup jobs are logged into the BOSSDesk system. Successful jobs are automatically closed while Failures remain open to be verified by an Engineer and restarted if required. Custom fields have been added to Employee access tickets and Computer tickets as check boxes to verify all work has been completed. Tasks have been automated for Employee access tickets for ERP and phone access.

## **XXVII. BOSSDESK INCIDENT MANAGEMENT**

### **A. PURPOSE**

The purpose of the Incident Management Policy is to establish standards and best practices on how to respond effectively to all support incidents. This policy will ensure consistent and coordinated approach to restore normal service operation as quickly as possible and minimize adverse impact on business operations, ensuring that the agreed upon availability is maintained for incidents.

### **B. SCOPE**

The Incident Management policy will govern the decisions and actions taken in the course of City of Delray Beach (**CDB**)'s IT Infrastructure standard services failures which causes, or may cause, an interruption to, or a reduction in, the quality of that service. The scope of this policy applies to all incidents reported by CDB's IT analysts or engineers, to include vendors & third-party contract personnel (consultants/contractors) regarding IT Infrastructure hardware, software, system components, virtual components, cloud components, networks, services, documents, and processes.

### **C. ROLES AND RESPONSIBILITIES**

The Incident Management process is the responsibility of all analysts in the IT Operations organization, including vendors and third parties that support, manage and/or operate IT Infrastructure devices and services for CDB. The CDB IT organization will use the concept of roles to remain flexible across its process framework. These management processes include a Service Desk Operator / Analyst, an Incident Manager or process owners and the process support staff. The CDB's Service Desk is the owner and driver of the Incident Management process and the process participants support the activities and tasks of the process. It is acceptable that the Service Desk Incident Manager or process owner and process participants may play other roles in the IT organization. The following roles are identified as part of the Incident process:

#### **1. INCIDENT MANAGERS**

The Incident Managers are responsible for managing the activities of the Incident Management process for the IT organization. These individuals focus on the process more than on any individual Incident. However, the Incident Managers are involved in every step of the process—from receipt of the Incident to its successful resolution.

- Drive the efficiency and effectiveness of the Incident Management process
- Produce management information and metrics.
- Manage the work of the Incident Management process participants.
- Monitor the effectiveness of the Incident Management process and make recommendations for improvements.
- Monitor the status and progress towards resolution of all open Incidents.
- Keep affected users informed about the progress.



- Escalate the Incident to management for decision-making.

## **2. SERVICE DESK OPERATOR**

The Service Desk Operator oversees receiving and registering the Incidents per the corresponding Incident Management process. This role will also attempt to resolve the incident as a first line of support. The responsibilities of the role are to:

- Receive and register Incidents submitted via self-service support website, telephone, email or automation of alerts.
- Classify the Incident and act as the first line of support to resolve the ticket
- Resolve and close the Incident (if possible)
- Escalate the Incident to second line of support or specific resolver queue for further resolution if required

## **3. SECOND-LINE SUPPORT**

The responsibilities of second line of support technicians will be to:

- Receive and further document Incident details.
- Investigates and diagnoses Incident.
- Identify potential Problems and/or Changes required.
- Resolve and close Incidents.

## **4. THIRD-LINE SUPPORT**

The responsibilities of third line of support technicians will be to:

- Refer to third-party or outsource support.
- Receive and further document ticket details.
- Investigate and diagnose Incident.
- Detect potential Problems and/or Changes required.
- Resolve and close Incident.

## **D. REVISION CONTROL**

This Incident Management policy document is subject to the same revision control procedures as all other CDB IT policies, procedures, and guidelines. The revision record clearly identifies the date, purpose and content changed, as well as those responsible for its modification, review, and management approval.

No change shall be made to this document, once approved for initial distribution, without the formally documented request, review and management approvals process defined in the Change Management Guidelines, Policies and Procedures.

#### E. COMMUNICATION OF POLICIES

Effective communication of the policies contained in this document is essential for an efficient management and internal controls process and to the successful protection of CDB's Information Resources. To facilitate this communication, a link to the repository of all IT policies will be added to the CDB's document repository tool for easy access and reference by all employees and a notice of changes will be issued whenever modifications to these policies are updated and approved.

### INCIDENT MANAGEMENT

#### F. INCIDENT MANAGEMENT PROCESS

The Incident Management process shall include namely the following activities:

- **Incident Detection and Recording:** This activity records basic details of the Incident, alerts the appropriate support staff, and start procedures for handling the request
- **Classification and Initial Support:** This activity classifies Incidents, matches the Incident against known errors and Problems, assigned impact and urgency, assess configuration details, and provides initial support or closes the Incident.
- Investigation and Diagnosis: This activity involves:
  - assessing the Incident details.
  - collecting and analyzing all related information including workarounds.
  - matching the Incident against known errors, Problems, solutions, planned Changes or Knowledge databases.
  - documenting any potential solutions.
- **Resolution and Recovery:** This activity involves resolving the Incident using a planned solution or a work around and taking recovery actions.
- **Incident Closure:** This activity involves:
  - updating Incident details.
  - contacting Requestor(s).
  - determining closure procedures.
  - closing the related Incident.
  - Incidents maybe closed by the Support Team (Administrative Close) after 1 week and 3 unsuccessful attempts to contact the requester.
- **Ownership, Monitoring, Tracking and Communication:** The Service Desk regularly monitors the status and progress of the Incident and keep end-user informed of progress.



**G. SERVICE DESK**

CDB's IT Service Desk can be contacted via the BOSSDesk Service Desk icon on your desktop, email at [itsupport@mydelraybeach.com](mailto:itsupport@mydelraybeach.com), telephone extension 7191. The Service Desk operates 24 hours a day, 365 days a year, but is staffed Monday – Friday, 8:00AM – 5:00PM.

**SERVICE LEVELS AND METRICS**

**H. INCIDENT PRIORITIZATION**

The CDB's IT organization determines the priority of an Incident by cross referencing and evaluating the impact on the business or service operations against the urgency by which a resolution or workaround is required.

Incident Impact and Urgency are defined as follows:

**1. BUSINESS IMPACT CHART**

<b>Impact</b>	<b>Impact Scope</b>
<b>High</b>	The ability to conduct business or services has stopped. Examples: Server, network, database, or application down.
<b>Medium</b>	Business or Services is moderately affected but can continue its operation via a short-term work around or with incremental resources for a short period of time before business is seriously degraded.
<b>Low</b>	Business or Services have not been interrupted but a problem is identified. A work around solution is available in case the Customer experiences work interruptions. No loss of productivity is present.

**2. URGENCY CHART**

<b>Urgency</b>	<b>Urgency Scope</b>
High	Must be executed as soon as possible.
Medium	Must be executed before a particular deadline.
Low	Not required to be executed at a particular deadline or timeframe.

**3. IMPACT/URGENCY CHART**

The chart below describes the priority classification level given to Incidents based on the Impact and Urgency described above. For example, a High-Urgency Incident with impact labeled as High will be given a priority 1. A priority one (1) Incident calls for an immediate response time from the Service Desk and requires an 'immediate' resolution. Such Incident if needed is immediately escalated to the 2<sup>nd</sup> level support and may require multiple resources to resolve.

		Urgency		
		High	Med	Low
Impact	High	1	2	3
	Med	2	3	4
	Low	3	4	5

Priority →

**I. INCIDENT RESPONSE TIMES**

The CDB's IT organization regards a response time when an Incident is recorded, classified, prioritized, and escalated to be resolved based on the Incident Management process outlined. The Incident Response Time chart contains the response and resolution time goals:

Priority	Response Time	Resolution Goal	First Escalation	Second Escalation	Third Escalation (Depends on third-party SLA)
1	<3 hours	<2 business days	1 hour	3 hours	6 hours
2	<6 hours	<5 business days	6 hours	12 hours	24 hours
3	<2 days	<10 business days	12 hours	24 hours	36 hours
4-5	<3 days	<30 business days	20 hours	48 hours	96 hours

An overall performance target percentage per quarter will be defined to measure the overall performance in achieving response times.

**J. ESCALATION MANAGEMENT**

The CDB's IT organization's Service Desk shall receive all inbound service request calls, emails, and self-service incident tickets to escalate them to the proper support staff. The escalation to the next level of support will occur per the Incident Response timeline or until the incident has been resolved.



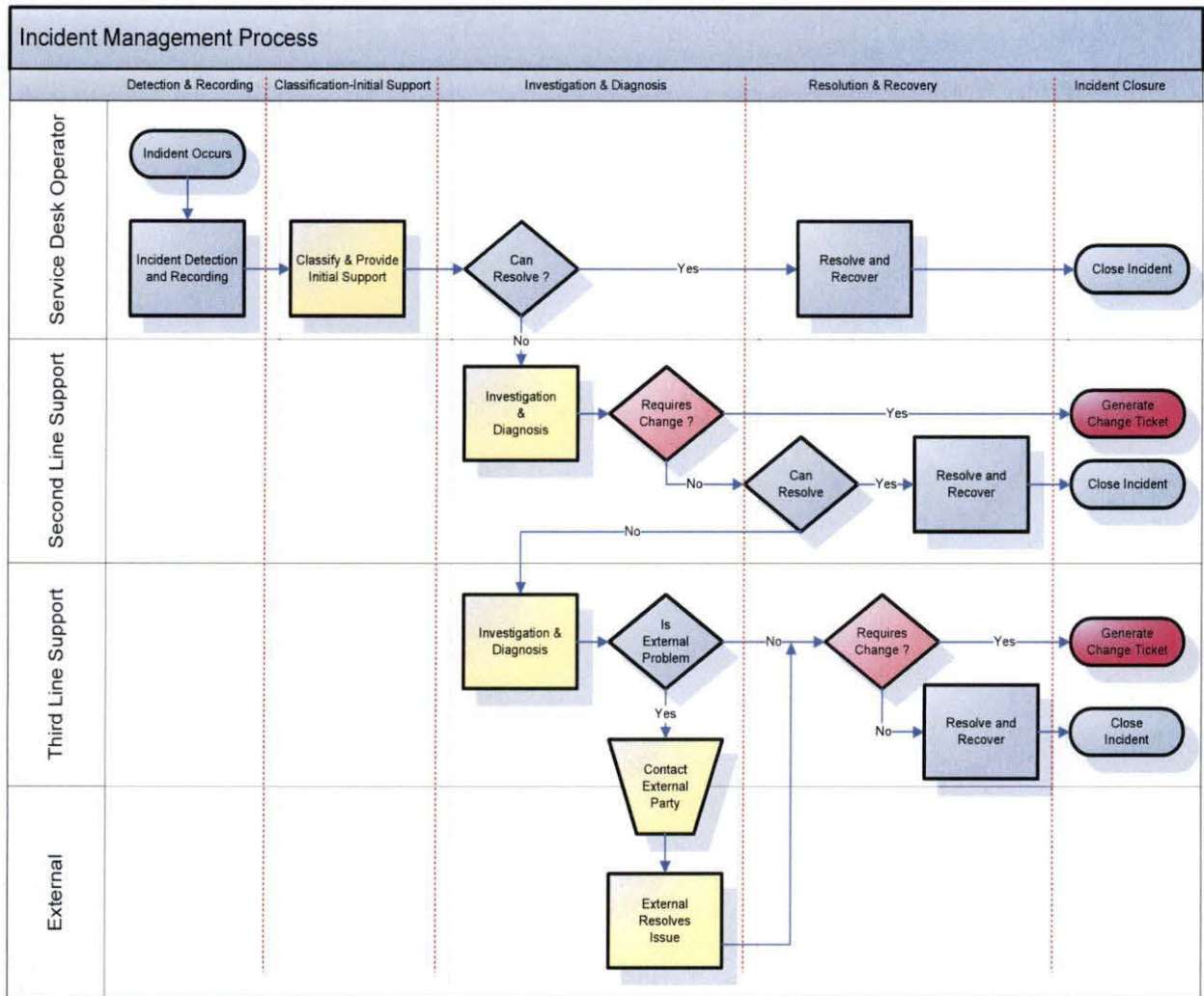


Figure 1: Incident Management Process Activities

## **XXVIII. BOSSDESK REQUEST MANAGEMENT**

### **A. PURPOSE**

The purpose of the Request Management Policy is to establish standards and best practices on how to respond effectively to all requests for service. This policy will ensure consistent and coordinated approach to fulfill requests of standard services within defined Service Levels and required quality.

### **B. SCOPE**

The Request Management policy will govern the decisions and actions required to source and deliver the components of requested standard services for IT Operations. The scope of this policy applies to all requests issued by City of Delray Beach (**CDB**)'s users, to IT analysts or engineers, (include vendors & third-party contract personnel (consultants/contractors)) regarding IT Operations hardware, software, system components, virtual components, networks, services, documents, and processes.

### **C. ROLES AND RESPONSIBILITIES**

The Request Management processes are the responsibility of all analysts in the IT Operations organization, including vendors and third parties that support, manage and/or operate IT devices and services for CDB's. The CDB IT organization will use the concept of roles to remain flexible across its process framework. These management processes include a Service Desk Operator / Analyst, a Request Manager or process owners and its process support staff. The CDB's Service Desk is the owner and driver of the Request Management process and the process participants support the activities and tasks of the process. It is acceptable that the Service Desk Incident Manager or process owner and process participants may play other roles in the IT organization. The following roles are identified as part of the Request Management process:

#### **1. REQUEST MANAGERS**

The Request Managers are responsible for managing the activities of the Request Management process for the IT organization. These individuals focus on the processes more than on any individual Request. However, the Request Managers are involved in every step of the process—from receipt of the Request to its successful fulfillment.

- Drive the efficiency and effectiveness of the Request Management processes
- Produce management information and metrics.
- Manage the work of the Request Management processes participants.
- Monitor the effectiveness of the Request Management processes and make recommendations for improvements.
- Monitor the status and progress towards resolution of all open Requests.
- Keep affected users informed about the progress.
- Escalate the Request to management for decision-making.

#### **2. SERVICE DESK OPERATOR (TICKET CREATOR)**

The Service Desk Operator oversees receiving and registering the Requests per the corresponding Request Management process. This role will also attempt to fulfill the request as a first line of support. The responsibilities of the role are to:

---



- Receive and register Requests submitted via self-service support website, telephone or email.
- Classify the Request and act as the first line of support to resolve the ticket
- Resolve and close the Request (if possible)
- Escalate the Request to second line of support or specific resolver queue for further fulfillment if required

### 3. RESOLVER GROUP (S)

The responsibilities of Resolver Group technicians will be to:

- Receive and further document Request details.
- Investigates and fulfills the Request.
- Refer to third-party or outsource support.
- Identify Changes required
- Resolve and close Request.

#### D. REVISION CONTROL

This Request Management policy document is subject to the same revision control procedures as all other CDB's policies, procedures, and guidelines. The revision record clearly identifies the date, purpose and content changed, as well as those responsible for its modification, review, and management approval.

No change shall be made to this document, once approved for initial distribution, without the formally documented request, review and management approvals process defined in the Change Management Guidelines, Policies and Procedures. See Document Revision Record page for additional information.

#### E. COMMUNICATION OF POLICIES

Effective communication of the policies contained in this document is essential for an efficient management and internal controls process and to the successful protection of CDB's Information Resources. To facilitate this communication, a link to the repository of all IT policies will be added to the CDB's document repository tool for easy access and reference by all employees and a notice of changes will be issued whenever modifications to these policies are updated and approved.

## REQUEST MANAGEMENT

### F. REQUEST MANAGEMENT PROCESS

A Service Request is a request to provide a new product or service or to grant access to a current product or service being by a service provider. It usually involves a low-risk modification to an IT infrastructure which is accomplished through the invocation of a set of well established procedures (see *Figure 1: Request Management Process diagram* on page 6).

**- Request Recording and Classification:** This activity records the basic details of the request,

---

any parameters or properties that may be required for the fulfillment, assigns the appropriate request area to the ticket, alerts the appropriate support staff, and start procedures for handling the request. In some cases, the request may require specific approvals (access, financial, compliance, etc.) in order for the fulfillment process to be initiated.

- **Request Fulfilment:** The actual fulfilment activity will depend upon the nature of the Service Request. Some simpler requests may be completed by the Service Desk, acting as first line of support, while others will have to be forwarded to specialist groups and/or suppliers for fulfilment. The Service Desk should monitor, track progress, and keep users informed throughout the lifetime of the request, regardless of the actual fulfilment source.

- **Request Closure:** Update ticket with details of the fulfillment, contact Requestor and validate that the user is satisfied with the outcome, update any Configuration Items that require documentation and resolve the request. Incidents may be closed by the Support Team (Administrative Close) after 1 week and 3 unsuccessful attempts to contact the requester.

- **Ownership, Monitoring, Tracking and Communication:** The Service Desk regularly monitors the status and progress of the request and keep end-user informed of progress.

#### G. IT OPERATIONS SERVICE DESK

CDB's IT Service Desk can be contacted via the BOSSDesk Service Desk icon on your desktop, email at [itsupport@mydelraybeach.com](mailto:itsupport@mydelraybeach.com), telephone extension 7191. The Service Desk operates 24 hours a day, 365 days a year, but is staffed Monday – Friday, 8:00AM – 5:00PM.

#### H. REQUEST CLASSIFICATION

The request ticket will be classified according to the nature of the product or service being requested. The properties, approvals or additional documentation required will also be defined specifically per type of request. This information will be re-determined with the business.

#### I. REQUEST SERVICE TYPES

The target goal for resolution of requests is also predetermined during the definition and setup of the service management tool. The goal is normally defined in hours or days and will be the service level agreement tied to the service request classification.

#### J. ESCALATION MANAGEMENT

The CDB's IT organization's Service Desk shall receive all inbound service request calls, emails, and self-service incident tickets to escalate them to the proper support staff. The escalation to the next level of support will occur per the **Service Type** timeline or until the **request** has been resolved.

---



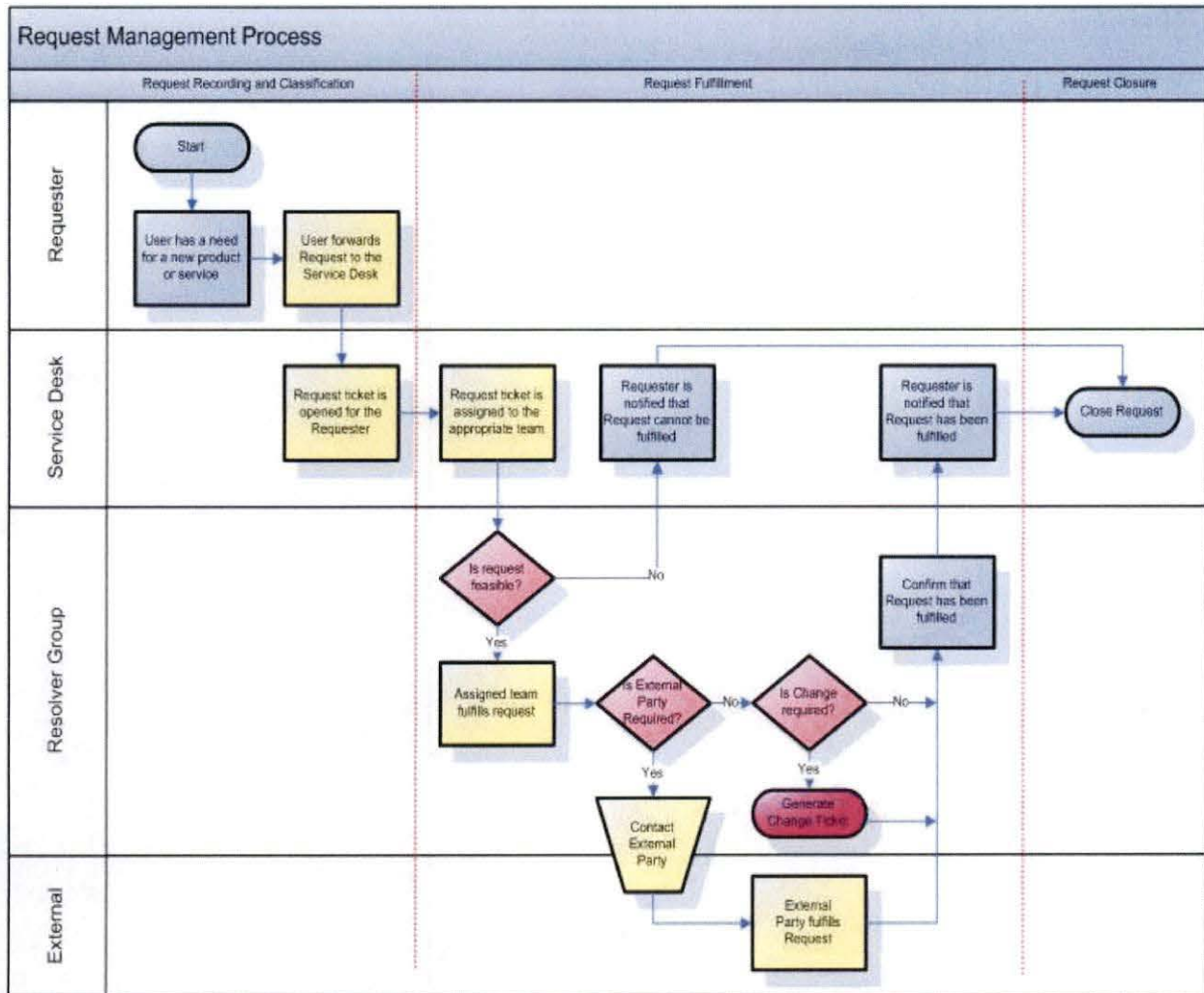


Figure 1: Request Management Process Activities

## **XXIX. BOSSDESK PROBLEM MANAGEMENT**

### **A. PURPOSE**

The purpose of this document is to define City of Delray Beach (**CDB**)'s approach to Problems, related to CDB's infrastructure.

A Problem is defined by ITIL as the unknown cause of one or more incidents, often identified because of multiple similar incidents.

### **B. SCOPE**

The scope of the Problem Management Policy applies equally to all resources in the CDB's IT infrastructure and includes management of the events that are not part of the standard operation of a service and cause or may cause an interruption to or a reduction in, the quality of service provided by the IT infrastructure.

The process and procedures in Problem Management are applied to:

- Service Desk calls and emails which require the involvement of Problem Management.
- First (Service Desk), Second (Engineers), and third-line support
- Escalation
- Priority
- Relationship between Incidents, Problems and Requests for Change

Out of scope items for this process include:

- Request for additional service(s)
- Requests that fall under the Request Management Process or Standard Change Process
- Development of standard Service Level Management procedures for handling Problems

### **C. ROLES AND RESPONSIBILITIES**

The Problem Management processes are the responsibility of all resources and/or services in the IT Operations organization, including vendors and third parties that support, manage and/or operate IT devices and services for CDB's.

The CDB IT organization will use the concept of roles to remain flexible across its process framework. These management processes include a Service Desk Analyst, a Problem Manager or process owners and its process support staff. The CDB's Problem Manager is the owner and driver of the Problem Management process, and the process participants support the activities and tasks of the process. It is acceptable that the Service Delivery Manager or process owner and process participants may play other roles in the IT organization.

#### **1. PROBLEM MANAGER**

The Problem Manager is responsible for managing the activities of the Problem Management process for the CDB's IT organization; this role is responsible for managing the lifecycle of all Problems.

The primary objectives of this role are to prevent Problems from happening, and to minimize the impact of Incidents that cannot be prevented (and then cause Problems); for this purpose, the Problem Manager maintains information about Known Errors and Workarounds.



## **2. PROBLEM TICKET REQUESTER**

This is an IT resource that could request the creation of the problem ticket. This includes a Problem Analyst, Problem manager, Service desk or any resource in the CDB's IT organization.

## **3. PROBLEM ANALYST**

The Problem Analysts, par to the CDB's IT teams, provide skills and knowledge in a particular domain, technical or operational. The Problem Analyst will use this expertise to facilitate root cause analysis of assigned problems, and the development of workarounds and/or permanent solutions. The main responsibility includes gathering data and resolving Problems through a permanent of workaround solution. Additionally, the Problem Analyst will facilitate the development and testing of permanent solutions.

## **4. SERVICE DESK**

The Service Desk is a single point of contact for users when there is a service disruption, for service requests, or even for some categories of requests for change. The Service Desk provides a point of communication to users and a point of coordination for several IT groups and processes. The main role of the Service Desk is to identify and document all relevant incidents details, allocating categorization and prioritization codes, that might prompt a Problem creation.

### **D. POLICY**

Problem management shall be performed in accordance with an established Problem Management process and set of procedures. The process and procedures must cover:

- Proactive Problem Management
- Root Cause Analysis
- Trending analysis
- Workarounds
- Interfaces (e.g., Incident, Change, Service Desk, etc.)

Problem Management activities must be based on the established process and set of procedures referenced in this document. They include:

- Proactive Problem Management
- Detection and Logging
- Classification
- Investigation and Diagnosis
- Error Control
- Problem Closure
- Continuous Process Improvement

The Problem Manager has the authority to assign Problem Records to the appropriate service support teams.

- Problems must be addressed in a timeframe agreed upon between Problem Manager and the affected parties.
- Problem Management has the authority to escalate any non-responsiveness for problem assignments to the CDB's IT management.

#### E. GOAL

The goal of problem management is to contribute to the mission of the organization by providing the highest possible levels of IT Service availability through minimization of the impact of Incidents and Problems within the environment by:

- Proactive prevention of Incidents and Problems
- Elimination of recurring Incidents
- Understanding the root cause of Incidents so that corrective action can be undertaken.

To achieve this goal, Problem Management seeks to establish the root cause of incidents and then initiate actions to improve or correct the situation.

The objectives of Problem Management are to:

- Identify and take ownership of problems affecting infrastructure and service.
- Take steps to reduce the impact of incidents and problems.
- Identify the root cause of problems and initiate activity aimed at establishing workarounds or permanent solutions to these identified problems.
- Using recorded problem and incident data, perform trend analysis to predict future problems and enable prioritization and implementation of problem management activity.

The Problem Management process has both reactive and proactive aspects. The reactive elements provide direct support to the day-to-day operational activities of other service management functions, such as incident management, and are concerned with initiating activity aimed at resolving problems in response to one or more incidents currently causing issues. Proactive Problem Management is concerned with identifying and mitigating problems and known errors before incidents occur.

#### F. PROBLEM MANAGEMENT PRINCIPLES

These principles are established to ensure that the process identifies the desired outcomes or behaviors related to the adoption for the IT Cloud operations.

- A single Problem Management process that is separate from the Incident Management and Change Management processes shall be used throughout the IT Operations.
- Clear criteria shall be established to define what constitutes a problem and how problems will be prioritized.
- All problems, known errors and relevant progress and resolution information shall be recorded in a common repository that is linkable to Incident and/or a Change Management records
- A known error shall be raised as soon as useful knowledge is available, even before a permanent resolution is found.
- Problem investigation & diagnosis shall employ standard analysis techniques & methodologies leveraging industry best practices.



## **XXX. BOSSDESK CHANGE MANAGEMENT**

### **A. PURPOSE**

The purpose of this policy is to ensure that the City of Delray Beach's (CDB) Information Technology (IT) organization and external personnel follow consistent best business practices, in relation to configuration changes of CDB infrastructure. The result of adhering to this policy will be enhanced customer service, higher systems integrity, and higher systems availability.

### **B. SCOPE**

The Change Management policy will govern the decisions and actions taken while changing IT infrastructure for all CDB operations. The scope of this policy applies to all changes made by CDB's IT analysts or engineers, to include vendors & third-party contract personnel (consultants/contractors) to IT hardware, software, system components, virtual components, cloud components, networks, services, documents, and processes that could affect the IT environment.

### **C. ROLES AND RESPONSIBILITIES**

#### **1. CHANGE REQUESTER**

The Change Requester initiates a change by submitting a Request for Change (RFC) through the BOSSDesk Service Catalog. All IT Team Members are authorized to initiate an RFC. The Change Requester may also be the Change Requester throughout the life cycle of the Change.

The Change Requester is responsible for completely filling out the RFC form, which includes the reason for the RFC, the requested implementation date, risks, benefits, and the systems and personnel affected by the change. This person is notified whether the change was approved and is kept up to date on the status of the RFC throughout the change process.

The Change Requester assists the Change Manager and Change Advisory Board (CAB) in determining the RFC priority and, at the conclusion of the change, participates in the post-implementation review.

#### **2. CHANGE ASSIGNEE**

The Change Manager may delegate or assign some of his or her duties to an individual to be the Change Assignee for a particular change. The Change Assignee is responsible for planning and implementing a change in the IT environment. The Change Assignee assumes responsibility upon receiving an approved RFC from the Change Manager or the CAB. The Change Assignee is required to follow the Change schedule approved by the CAB. The Change Assignee should routinely provide project status feedback to the Change Manager and identify any problems as they arise. The Change Assignee presents all formal updates and proposals to the CAB.

#### **3. CHANGE MANAGER**

The Change Manager is responsible for managing the activities of the Change Management process for the IT organization. This individual focuses on the process more than on any individual change. However, the Change Manager is involved in every step of the process—from receipt of

an RFC to the implementation of the change in the IT environment—and is ultimately responsible for the successful implementation of any change to the IT environment.

The Change Manager's responsibilities include:

- Receiving RFCs and ensuring that they are properly recorded in the change log.
- Selecting CAB members and facilitating CAB meetings.
- Preparing CAB meeting agendas and providing all necessary review information to the CAB members prior to the meetings.
- If necessary, assigning teams to conduct RFC impact analyses and risk assessments.
- Analyzing and prioritizing RFCs.
- Categorizing, assigning Change Owners, and scheduling RFCs, subject to approval by the CAB.
- Approving requests of type Standard. Normal changes (minor) do not require approvals, as their scope is too small, and may not require the creation of change documentation. Emergency changes, by their nature, do not require a previous approval.
- Providing change notification to Change Initiator and other affected parties.
- Monitoring the successful completion of all RFC's, including the Change implementation activities and steps, and ensuring that they follow the change schedule.
- Reviewing and evaluating the Change Management process.

#### **D. CHANGE ADVISORY BOARD (CAB)**

The Change Advisory Board (CAB) is comprised of all Change Approvers, who evaluate and approve significant/major/urgent changes to the production environment. The CAB reviews and evaluates impact to the business, cost of the change, financial impact to the business if the change is not done, and the benefits in terms of efficiency and revenue the Change could bring into the organization. The CAB shall also review the status of a change throughout the change process, assess progress with respect to the approved schedule, determine how to correct any identified problems, and communicates findings to appropriate business managers and stakeholders. The CAB shall meet on a periodic basis.

#### **E. REVISION CONTROL**

This Change Management policy document is subject to the same revision control procedures as all other CDB's policies, procedures, and guidelines. The revision record clearly identifies the date, purpose and content changed, as well as those responsible for its modification, review, and management approval.

No change shall be made to this document, once approved for initial distribution, without the formally documented request, review and management approvals process defined in the Change Management Guidelines, Policies and Procedures. See Document Revision Record page for additional information.



## CHANGE MANAGEMENT

### F. CHANGE MANAGEMENT PROCESS ACTIVITIES

The Change Management process will include the following activities.

**- Recording and Classification:** This activity includes the proper recording and classification of the RFC. RFCs are categorized, prioritized, and assigned. This activity shall be performed by the Change Initiator, Change Owner, or Change Manager. The Change Initiator, Change Owner, or Change Manager evaluates and analyzes the Change, so its category, type, and priority are properly selected and recorded.

**- Approval:** This activity involves the documentation of all the necessary information for Changes to be submitted for approval through the Change Advisory Board. The information required includes the Change detail description, business impacts, costs, risks, and benefits. This activity shall be performed by the Change Manager. All changes must be approved by two (2) members of the CAB.

**- Implementation or Release:** This activity involves documenting the various tasks on how the Change is going to be accomplished, a technical authorization by the Change Manager and the implementation or release of the affected Configuration Item (CI) into production. Changes that are vendor related are submitted to the vendor(s) for implementation, however, the Change Owner and/or Change Manager will authorize the release of the Change into production.

**- Closure:** This activity involves the review and assurance of the Change solution and implementation by the Change Owner and/or Change Manager before the Change can be properly closed. In addition, customers, suppliers, partners, or multiple sites should be involved in testing the Change, accepting it, and authorizing its release. The release of a Change is responsibility of the Release Management process and team. A post-implementation review of Significant, Major, Urgent, or Emergency Changes shall be conducted at the discretion of the Change Owner and/or Change Manager, to follow up on the results and impact of the Change.

### G. ADVISORY BOARD MEETINGS

Change Advisory Board meetings shall be scheduled regularly every month depending on the volume and complexity of Changes proposed. The meetings will provide for a formal review and sign-off of approved Changes. The CAB agenda shall include a review of:

- Failed Changes, backed-out Changes, or Changes applied without reference to the CAB by Incident Management, Problem Management or Change Management.
- RFC's to be assessed by CAB members.
- RFC's that have been assessed by CAB members.
- Change reviews.
- The Change Management process, including amendments made to it during the period under discussion, as well as proposed Changes.
- Change Management wins/accomplishments for the period under discussion, i.e., review of the business benefits accrued by way of the Change Management process.



#### H. FORWARD SCHEDULE OF CHANGES

The Change Manager shall coordinate the production and distribution of a Forward Schedule of Changes (FSC). The FSC shall contain details of all the Changes approved for implementation and their proposed implementation dates. These shall be agreed with the relevant Customers \ users within the business, with Service Level Management, with the Service Desk and with Availability Management. Once agreed, the Service Desk shall communicate any planned additional downtime to the user community at large, using the most effective method available.

#### I. CHANGE REVIEWS

The Change Manager shall review all implemented Changes after a predefined period has elapsed. This process may involve CAB members. The purpose of such reviews is to establish that:

- The Changes have had the desired effects and met their objectives.
- Users and Customers are content with the results, or to identify any shortcomings.
- There have been no unexpected or undesirable side-effects to functionality, availability, capacity/performance, security, and maintainability.
- The resources used to implement the Change were as planned.
- The implementation plan worked correctly (so include comments from the implementation)
- The Change was implemented on time and to cost.
- The back-out plan functioned correctly, if needed.

#### J. RELATIONSHIP TO OTHER SERVICE MANAGEMENT FUNCTIONS PROCESSES

There is a close relationship between Change Management, Configuration Management, and Release Management. All releases into production environments will be controlled by Requests for Changes (RFC's). All changes to configurations will also be documented through an RFC including updates to the Definite Software Library (DSL), Definite Hardware Store (DHS), release packages and all Configuration Items (CI).

Change Management ensures that only approved changes are deployed, and all tracking of the authorization process is complete. Release Management updates the Configuration Management Database (**CMDB**, the database where all the Configuration Items' records are kept) with the release package after deployment.

The Change Manager must ensure that all CIs affected by a Change are up-to-date. The accuracy of the information stored in the CMDB is crucial to the success of the Change Management and other service management processes. A review process that ensures that the database accurately reflects the production IT environment needs to be established. Refer to the Configuration Management policy and procedure for further information.

Note: A more fundamental review should also be carried out at periodic intervals to establish whether the information in the CMDB is relevant to the business and is being managed at the correct level of detail.



#### K. CHANGE CATEGORIES

Changes should be assigned a category to identify what area of the Technology is being affected. This facilitates the reporting and assignment of Changes. Below is a suggested list of Categories that can be used with a Service Desk or manual tool:

- Software
- Hardware
- Network
- Documentation
- Training
- Mail / messaging
- ERP (Enterprise Resource Planning)
- Reporting system

#### L. CHANGE TESTING AND BACK OUT

Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) prior to implementation to minimize the effect on the relevant business process, to assess its impact on operations and security, and to verify that only intended and approved changes were made.

Procedures for aborting and recovering from unsuccessful changes shall be documented in the change documentation. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert to what they were prior to implementation of changes.

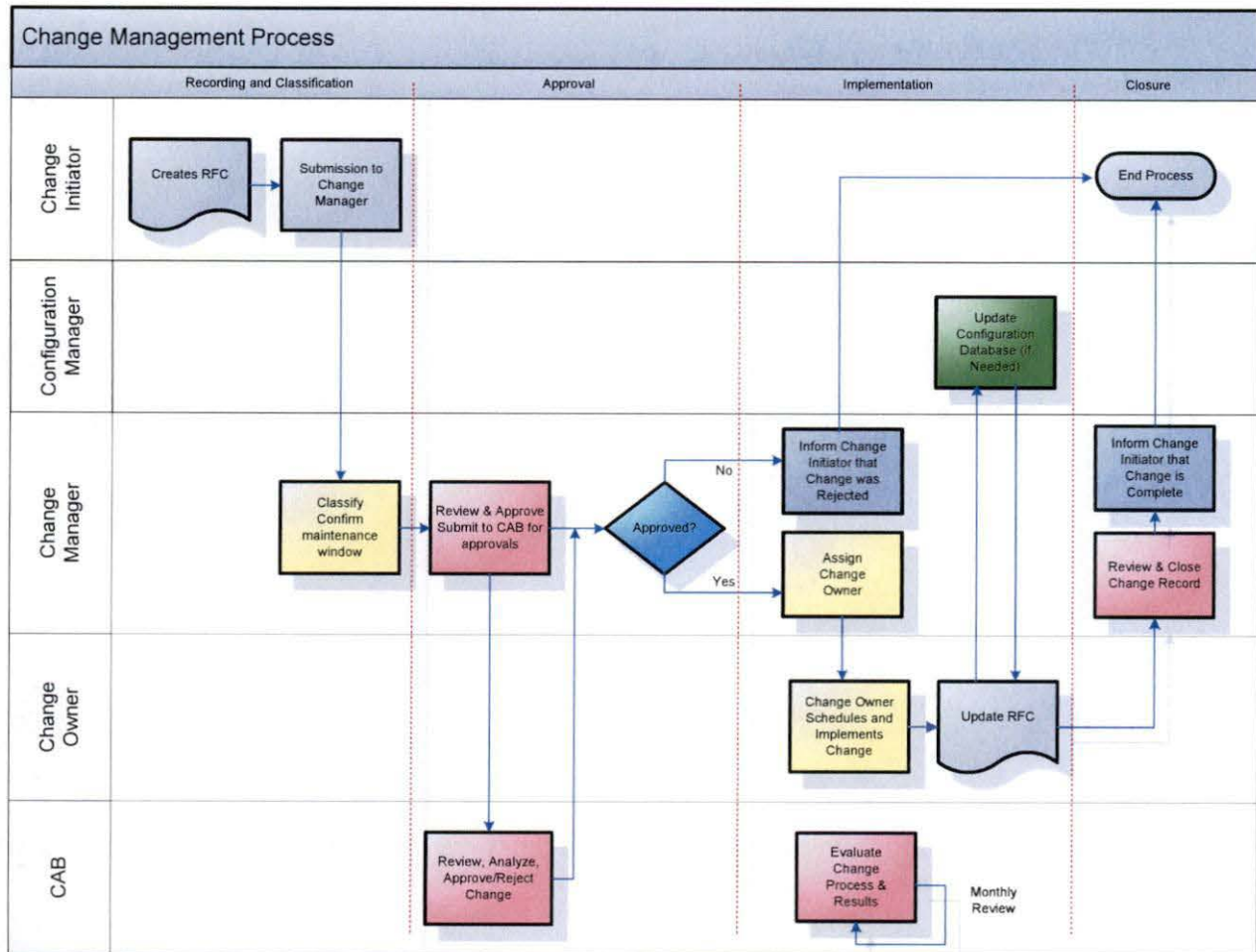


Figure 1: Change Management Process Activities



## **XXXI. PUBLIC WI-FI**

The City of Delray Beach has installed Wi-Fi Access Points in some City Buildings, but not all. Wi-Fi is utilized for City staff and not necessarily for general public access to the Internet. City Staff utilizing Public Wi-Fi must VPN back into the City Network for access to any Network data resource or application.

### **A. DISCLAIMER**

Please read the following usage disclaimer before continuing.

You are about to access Internet content that is not under the control of the City of Delray Beach. This service (the "Service") is an open network provided for your convenience, and ITS USE IS AT YOUR OWN RISK. It is available to the general public and is NOT INHERENTLY SECURE. The City cannot and does not guarantee the security, privacy or confidentiality of your data and communication while using the Service. The City does not warrant that the Service will be uninterrupted, error-free, or free of viruses or other harmful components.

The City of Delray Beach is not responsible for any of these sites, their content, or their privacy policies. The City of Delray Beach and its staff do not endorse nor make any representations about any of these sites, or any information, software or other products or materials found there, or any results that may be obtained from using them. If you decide to access any Internet content, you do so entirely at your own risk, and you are responsible for ensuring that any accessed material does not infringe on the laws governing copyright, trademark, pornography, defamation, or slander.

### **B. PROHIBITED**

THE USE OF THIS SERVICE FOR THE FOLLOWING ACTIVITIES IS PROHIBITED:

Spamming and Invasion of Privacy of Others, Violating Intellectual Property Law, Transmitting Obscene or Indecent Speech or Materials, Transmitting Defamatory or Abusive Language, Hacking or Distribution of Internet Viruses, Worms, Trojan Horses or Other Destructive Activities.

### **C. CONDITIONS**

By using the Service, you also agree to the following conditions:

Release and Indemnity. Under no circumstances shall the City, its officers, employees or agents, be liable for any direct, indirect, incidental, special, punitive or consequential damages or lost profits, whether foreseeable or not, that result in any way from user's use of or inability to use the Service or to access the Internet or any part thereof, or user's reliance on or use of information, services or merchandise provided on or through the Service, or that result from mistakes, omissions, interruptions, deletion of files, errors, defects, delays in operation or transmission or any failure of performance. You agree to release the City, its officers, employees and agents, and to indemnify and hold harmless the same, from any claim, liability, loss, damage, cost or expense (including, without limitation, reasonable attorney's fees) incurred by you or any third party arising out of or related to your use of or inability to use the Service, any materials downloaded or uploaded through the Service, any actions taken by you in connection with your use of the Service, any violation of any third party's rights or any violation of law or regulation or any breach of this agreement.

The Service and any products or services provided on or in connection with the Service are provided without warranties of any kind. All warranties, conditions, representations, indemnities and guarantees with respect to the content or Service and the operation, capacity, speed, functionality, qualifications or capabilities of the services, goods or personnel resources provided hereunder, whether express or implied, arising by law, custom, prior oral or written statements or otherwise (including, but not limited to any warranty of satisfactory quality, merchantability, fitness for particular purpose, title and non-infringement) are hereby overridden, excluded and disclaimed.



## XXXII. SECURITY INCIDENT RESPONSE POLICY

### A. PURPOSE

This document describes the City of Delray Beach's overall plan for preparing and responding to both physical and electronic information security incidents. It defines the roles and responsibilities of participants, characterization of incidents, relationships to other policies and procedures, and reporting requirements. The goal of this Security Incident Response Plan is to prepare for, detect, and respond to security incidents. It provides a framework by which the Incident Response Team (IRT) shall determine the scope and risk of an incident, respond appropriately to that incident, communicate the results and risks to all stakeholders, and reduce the likelihood of an incident from occurring or reoccurring.

### B. SCOPE

This plan applies to all physical locations, information systems, all Criminal Justice Information (CJI) data, Protected Health Information (PHI) data, Cardholder data, Personally Identifiable Information, and any other sensitive data type stored by the city, and networks of The City of Delray Beach and any person or device that gains access to these systems or data.

### C. MAINTAINING CURRENCY

It is the responsibility of the Chief Technology Director to maintain and revise this policy to ensure that it is always in a ready state.

### D. DEFINITIONS

**Event** – An event is an exception to the normal operation of infrastructure, systems, or services. Not all events become incidents.

**Incident** – An incident is an event that, as assessed by the staff, violates the policies of the City of Delray Beach as related to Information Security, Physical Security, or Acceptable Use; other City of Delray Beach policies, standards, or code of conduct; or threatens the confidentiality, integrity, or availability of information systems or CJI event.

Incidents will be categorized according to their potential for the exposure of protected data or the criticality of the resource, using a four (4) level system of:

- 0 – Low
- 1 – Medium
- 2 – High
- 3 – Critical

Incidents can include, but are not limited to:

- Malware/viruses/Trojans
- Ransomware
- Phishing
- Unauthorized electronic access
- Account compromise
- Breach of information
- Unusual, unexplained, or repeated loss of connectivity
- Unauthorized physical access
- Loss or destruction of physical files, etc.
- Denial of Service

**Criminal Justice Information (CJI)** – CJI is as defined in the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy and by the Florida Department of Law Enforcement.

**Protected Health Information (PHI)** – The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

**Cardholder Data** – The PCI Security Standards Council (PCI SSC), the body that administers the PCI DSS, defines cardholder data as “At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code [found on the magnetic stripe]. Sensitive Authentication Data are additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.”

#### E. EVIDENCE PRESERVATION

The goal of any incident response is to reduce and contain the impact of an incident and ensure that information security related assets are returned to service in the timeliest manner possible. The need for a rapid response is balanced by the need to collect and preserve evidence in a manner consistent with state and federal laws, and to abide by legal and administrative requirements for documentation and chain-of-custody.

#### F. INCIDENT RESPONSE

In accordance with the FBI CJIS Security Policy, based off the National Institute of Standards and Technology (NIST) Special Publication 800-61 rev. 2, the Incident Response Life Cycle consists of a series of phases—distinct sets of activities that will assist in the handling of a security incident, from start to finish.



## 1. PREPARATION

Preparation includes those activities that enable the City of Delray Beach to respond to an incident. These include a variety of policies, procedures, tools, as well as governance and communications plans.

The City of Delray Beach utilizes several mechanisms to prevent, and prepare to respond to, an incident.

- **Security Awareness Training:** The City of Delray Beach requires regular security awareness training provided through KnowBe4. This training covers additional ongoing threats to systems such as malware, phishing, social engineering, ransomware, and other threats as they become known. This training also performs regular phishing campaigns to evaluate the city's security posture for this attack vector. All personnel with access to CJI data are required to take FBI CJIS Security Policy-compliant Security Awareness Training. This training must be updated at a minimum of every two years.
- **Malware/Antivirus/Spyware Protections:** All information system terminals, as well as key information flow points on the network are protected by continuous defense against malware/antivirus/spyware and other known malicious attacks. These defense mechanisms are kept up to date without the need for end user intervention, and end users are restricted from accessing, modifying, disabling, or making other changes to the defense mechanisms.
- **Firewalls:** Multiple firewalls are in place within the network to provide the necessary depth of defense. The city's IT Department keeps all firewalls up to date with the latest security patches and other relevant upgrades, as well as maintain an active backup of the latest security configuration.
- **Personnel Security Measures:** All CDB personnel with access to CJI or those areas in which CJI is accessed, stored, modified, transmitted, or maintained have been cleared to the required Personnel Security standards set forth in FBI CJIS Security Policy section 5.12.1 and FDLE requirements.
- **Physical Security Measures:** All locations within the City of Delray Beach that house CJI or CJI-related information systems are secured to the required criteria set forth in FBI CJIS Security Policy section 5.9. Access to these secured areas and information systems are a need-to-know/need-to-share basis and required agency authorized credentials for access and are under the direct control and management of the City of Delray Beach.
- **Event Logs:** Event logging is maintained at all applicable levels, capturing all the required events and content specified for CJI through FBI CJIS Security Policy sections 5.4.1.1 and 5.4.1.1.1, retained for the specified period, and reviewed weekly.

- Patching/Updating: Systems shall be patched and updated as new security patches and hot fixes are released. Any software or hardware product that reaches the end of the manufacturers service and support life for patching will be deemed out-of-compliance and replaced.

## **2. STAFFING**

The City of Delray Beach, Chief Technology Director will strive to maintain adequate staff levels and third-party support to investigate each incident to completion and communicate its status to other parties while it continues to monitor the tools that detect new events.

## **3. TRAINING**

No incident response capability can be effectively maintained over time without proper and ongoing training. The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested, and translated into recommendations for enhancements. All pertinent City staff will be trained on a periodic basis in security awareness, procedures for reporting and handling incidents to ensure a consistent and appropriate response to an incident, and that post-incident findings are incorporated into policy and procedure.

# **G. DETECTION AND ANALYSIS**

## **1. DETECTION**

Detection is the discovery of an event with security tools or through notification by an inside or outside party about a suspected incident. The detection of an incident requires the immediate activation of the IRT as listed in Appendix A. The determination of a security incident can arise from one or several circumstances simultaneously.

Means by which detection can occur include:

- Trained personnel reviewing collected event data for evidence of compromise.
- Software applications analyzing events, trends, and patterns of behavior.
- Intrusion Protection/Intrusion Detection devices alerting to unusual network or port traffic.
- The observation of suspicious or anomalous activity within a [agency name] facility or on a computer system.

It is critical in this phase:

- To detect whether a security incident has occurred.
- To determine the method of attack.
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident.
- To obtain or create intelligence products regarding attack modes and methods.

## **2. ANALYSIS**

Analysis of the incident indicators will be performed in a manner consistent with the type of



incident. In the event of a physical incident, appropriate steps will be taken to determine weaknesses in either the physical security of the facility, its monitoring tools, or its training programs to assess areas for process improvement or change. For an electronic incident, the City will utilize the City IT Department, its tools, vendors, and contractors to perform static and dynamic analysis of malicious code within their capability, a review of information system boundary protections, determination of source code if applicable, the depth and breadth of the attack, if the attack has migrated to other systems on or off the network, and any other tasks appropriate to the type of incident experienced. These analyses can be performed either manually or utilizing automated tools dependent upon the situation, timeliness, and availability of resources.

### 3. INCIDENT CATEGORIES

An incident will be categorized as one of four severity levels. These severity levels are based on the impact to The City of Delray Beach and can be expressed in terms of financial impact, impact to services and/or performance of our mission functions, impact to the city's image, or impact to trust by the City's customers and citizens, etc. The below table provides a listing of the severity levels and a definition of each severity level.

Severity Level	Description
0 – Low	Incident where the impact is minimal. Examples may be e-mail SPAM, isolated virus infections, etc.
1 – Medium	Incident where the impact is significant. Examples may be a delayed or limited ability to provide services, meet the city's mission, delayed delivery of critical electronic mail or data transfers, etc.
2 – High	Incident where the impact is severe. Examples may be a disruption to the services and/or performance of our mission functions. The city's proprietary or confidential information has been compromised, a virus or worm has become widespread and is affecting over 1 percent of employees, Public Safety systems are unavailable, or the city's Executive management has been notified.
3 - Critical	Incident where the impact is catastrophic. Examples may be ransomware, denial of service or a shutdown of all the city's network services due to natural or manmade causes. The city's proprietary or confidential information has been compromised and published in/on a public venue or site. Public safety systems are unavailable. Executive management must make a public statement.

#### 4. **INCIDENT REPORTING**

If an incident involves or is suspected of involving criminal justice information, the Information Security Officer (ISO) will be contacted and provided a CJIS-016 "Information Security Officer (ISO) Security Incident Report" and should work with the City's agency representatives for CJI compliance.

### H. **CONTAINMENT, ERADICATION, AND RECOVERY**

#### 1. **CONTAINMENT**

The Chief Technology Director is responsible for containment and will document all containment activities during an incident.

Containment activities for security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. This requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

#### 2. **ERADICATION**

The Chief Technology Director is responsible for eradication and will document all eradication activities during an incident.

Eradication efforts for a security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

#### 3. **RECOVERY**

The Chief Technology Director is responsible for recovery and will document all recovery activities during an incident.

Recovery efforts for incidents will involve the restoration of affected systems to normal operation. This is dependent upon the type of incident experienced but may include actions such as restoring systems from backups, rebuilding systems from an agency approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.



## I. POST-INCIDENT ACTIVITY

The Chief Technology Director is responsible for documenting and communicating post-incident activity.

Post-incident activities will occur after the detection, analysis, containment, eradication, and recovery from a security incident. One of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Important items to be reviewed and considered for documentation are:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What should be done differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Post-incident activities will be incorporated into future training opportunities for all parties involved in the incident, from victims to system administration personnel, to incident responders.

## J. ESCALATION

The escalation process will be initiated to involve other appropriate resources as the incident increases in scope and impact. Incidents should be handled at the lowest escalation level that can respond to the incident with as few resources as possible to reduce the total impact and maintain limits on cyber-incident knowledge. The table below defines the escalation levels with the associated team members involvement.

<b>Severity</b>	<b>Response Team Member Involvement</b>	<b>Description</b>
0 – Low	IT Technical Support Staff or vendor Local Agency Security Officer (LASO)	Normal Operations
1 – Medium	IT technical support staff or vendor LASO IT Director	The City is aware of a potential or actual threat and is responding to that threat
2 – High	IT technical support staff or vendor LASO IT Director City Management/Controller	An obvious threat has impacted business operations. Determine course of action for containment and eradication. Message staff of required actions and operational impacts if necessary
3 – Critical	IT technical support staff or vendor LASO IT Director City Management/Controller Finance Director Legal Contact Communications Director	Threat is widespread with significant impact. Determine course of action for containment, mitigation, and eradication. Message staff and officials. Prepare for legal action. Prepare for a public statement.

The Incident Response Team will consider several characteristics of the incident before escalating the response to a higher level. They are:

- How widespread is the incident?
- What is the impact to business operations?
- How difficult is it to contain the incident?
- How fast is the incident propagating?
- What is the estimated financial impact to the city?
- Will this negatively affect the city's image?



**K. APPENDIX A: INCIDENT RESPONSE TEAM**

Role	Leadership / Members	Contact Information
IT Director		
Key IT Staff		
LASO		
City Manager		
Communications Director		
Extended Team	FBI Field Office or DHS	
	MS-ISAC SOC	
	HHS (HIPAA Data)	
	Legal / General Counsel	
	Human Resources	
	Finance Director	
	Chief of Police	
	Chief of Fire	
	City Clerk	

**Other Numbers/Contacts:**  
 Major Software Vendors  
 Internet Circuit Providers  
 Backup Data Center  
 Other agency contacts

**L. APPENDIX B: INCIDENT RESPONSE PROCESS TREE**

This appendix discusses the steps taken during an activation of the incident response plan. To create the plan, the steps in the following example should be replaced with contact information and specific courses of action for your organization.

The person who discovers the incident will notify the internal security team or manager as appropriate – whichever is deemed the most expedient given the nature of the discovery. Reporters may be anyone in the city as well as contracted vendors or outside agencies. The city should ensure that all staff understand who they can report events or potential incidents to.

Those should include:

- a) Helpdesk
  - b) IT Manager
  - c) Any IT Staff Member
  - d) Any member of city management
- 1) If the person discovering the incident is a member of the IT department or affected department, they will proceed to step four (4).
  - 2) The Helpdesk/manager/IT Staff will refer to the IT emergency contact list or effected department contact list and call the designated numbers in order on the list. The Helpdesk will log:
    - a) The name of the caller
    - b) Time of the call
    - c) Contact information about the caller.
    - d) The nature of the incident.
    - e) When the event was first noticed, supporting the idea that the incident occurred.
  - 3) The IT staff member or affected department staff member who receives the call (or discovered the incident) will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the incident response manager using both email and phone messages. The staff member will log the information received in the same format as in the previous step. The staff member could possibly add the following:
    - a) Is the system affected business critical?
    - b) What is the severity of the potential impact?
    - c) Name of system being targeted, along with operating system, Internet Protocol (IP) address, and location.
    - d) IP address and any information about the origin of the attack.
  - 4) Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.
    - a) Is the incident real or perceived?
    - b) Is the incident still in progress?
    - c) What data or property is threatened and how critical is it?
    - d) What is the impact on the business should the attack succeed? Minimal, serious, or critical?
    - e) What system or systems are targeted, where are they located physically and on the network?
    - f) Is the incident inside the trusted network?
    - g) Is the response urgent?



- h) Can the incident be quickly contained?
  - i) Will the response alert the attacker and do we care?
  - j) What type of incident is this? Example: virus, worm, intrusion, abuse, damage.
- 5) An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:
- a) Category one - A threat to public safety or life.
  - b) Category two - A threat to sensitive data.
  - c) Category three - A threat to computer systems.
  - d) Category four - A disruption of services.
- 6) Team members will establish and follow one of the following procedures basing their response on the incident assessment:
- a) Ransomware procedure
  - b) Virus response procedure.
  - c) System failure procedure.
  - d) Active intrusion response procedure - Is critical or sensitive data (Personally Identifiable Information (PII), CJI, etc.) at risk?
  - e) Inactive Intrusion response procedure.
  - f) System abuse procedure.
  - g) Property theft response procedure.
  - h) Denial of service response procedure.
  - i) Database or file denial of service response procedure.
- 7) Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.
- 8) Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.
- 9) Upon management approval, the changes will be implemented.
- 10) Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
- a) Reinstall the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
  - b) Make users change passwords if passwords may have been sniffed.
  - c) Be sure the system has been hardened by turning off or uninstalling unused services.
  - d) Be sure the system is fully patched.
  - e) Be sure real time virus protection and intrusion detection is running.
  - f) Be sure the system is logging the correct events and to the proper level.
- 11) Documentation—the following shall be documented:

- a) How the incident was discovered.
  - b) The category of the incident.
  - c) How the incident occurred, whether through email, firewall, etc.
  - d) Where the attack came from, such as IP addresses and other related information about the attacker.
  - e) What the response plan was.
  - f) What was done in response?
  - g) Whether the response was effective.
- 12) Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond, in case of an appeal.
- 13) Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.
- 14) In the event of a loss or suspected loss of criminal justice information, work with the LASO to contact the FDLE Information Security Officer via the CJIS-016 Form.
- 15) Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
- 16) Review response and update policies—plan and take preventative steps so the intrusion cannot happen again.
- a) Consider whether an additional policy could have prevented the intrusion.
  - b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
  - c) Was the incident response appropriate? How could it be improved?
  - d) Was every appropriate party informed in a timely manner?
  - e) Were the incident response procedures detailed, and did they cover the entire situation? How can they be improved?
  - f) Have changes been made to prevent a reinfection? Have all systems been patched, systems locked down, passwords changed, antivirus dated, email policies set, etc.?
  - g) Have changes been made to prevent a new and similar infection?
  - h) Should any security policies be updated?
  - i) What lessons have been learned from this experience?



### **XXXIII. POLICY VIOLATIONS**

Non-compliance with these and other information security requirements or any attempt to violate the provisions of this policy will result in disciplinary action up to and including termination, regardless of the success or failure of the attempt. Depending on the severity of the offense, the action may result in the following:

In the case of CDB employees:

- Suspension of usage privileges,
- Verbal and/or written reprimands,
- Disciplinary action,
- Termination

In the case of Third-Party Personnel, Contractors or Temporary workers:

- Suspension of usage privileges,
- Verbal and/or written reprimands,
- Termination of access and/or contract.

Specific actions will be taken at the discretion of CDB Management.

**PROCEDURE: (if applicable)**