RESOLUTION NO. 7370

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF REDLANDS ADOPTING A COMPUTER SECURITY INCIDENT RESPONSE PLAN

WHEREAS, Civil Code section 1798.29, California's security breach notification law, requires state agencies and businesses to notify residents, as quickly as possible and without delay, when the security of their personal information has been breached; and

WHEREAS, in 2013, the state legislature enacted Assembly Bill No. 1149 and Senate Bill No. 46 to extend the state's security breach notification law to local public agencies and to expand the scope of personal information that prompts a disclosure of a security breach; and

WHEREAS, staff of the City's Department of Innovation and Technology and Human Resources Department have collaborated to develop a Computer Security Incident Response Plan to establish roles and responsibilities in the event of a breach of security associated with the City's information technology systems; and

WHEREAS, the Computer Security Incident Response Plan establishes protocols for compliance with the state's security breach notification law; and

WHEREAS , it is the desire of the City Council of the City of Redlands to ensure that the City's residents will be promptly and fully notified of any breach of security with respect to their personal information maintained in connection with the City's information and technology systems;

NOW, THEREFORE, BE IT RESOLVED by the City Council of the City of Redlands as follows:

Section 1. The Computer Security Incident Response Plan attached hereto as Exhibit "A" is hereby adopted.

ADOPTED, SIGNED AND APPROVED this 18th day of March, 2014.

Pete Aguilar, Mayor

ATTEST:

Sam Irwin, City Clerk

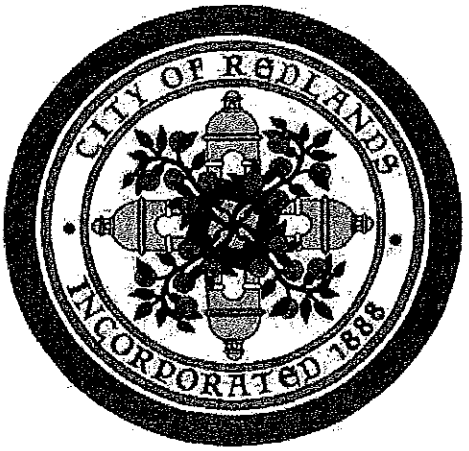
I:\cclerk\Resolutions\Res 7300-7399\7370 Computer Security Incident Response.doc

I, Sam Irwin, City Clerk, City of Redlands, hereby certify that the foregoing resolution was duly adopted by the City Council at a regular meeting thereof held on the 18th day of March, 2014, by the following vote:

AYES: Councilmembers Harrison, Foster, Gardner, Gilbreath; Mayor Aguilar
NOES: None
ABSTAIN: None
ABSENT: None

Sam Irwin, City Clerk

Exhibit "A"



City of Redlands
Computer Security Incident Response Plan

March 2014

TABLE OF CONTENTS

1. Overview

1.1 Purpose of Plan

This plan is established to specify roles and responsibilities in the event of a computer security incident, and to comply with California Civil Code section 1798.29.

The goal of the City of Redlands is to minimize and prevent incidents by ensuring that systems, networks, and applications are sufficiently secure, and this plan has been established to ensure the City is prepared to respond and disclose in the event of a security incident.

The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c) of California Civil Code section 1798.29, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

1.3 Scope

Any incidents that originate from, are directed towards, or transit the City's controlled computer or network resources, fall under the scope of this Incident Response Plan.

1.2 Definition of Computer Security Incident

An incident is defined as an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information; or any event that has actual or potential adverse effects on City computer or network resources such as loss or damage of property. If personal information was, or is reasonably believed to have been, acquired by an unauthorized person, the City shall notify the owner or licensee of such information of any breach of the security of the data immediately following discovery.

While the City should be prepared to handle any incident, it should focus on being prepared to handle incidents that use the following common attack vectors:

- External/Removable Media: An attack executed from removable media (e.g., USB flash drive, CD) or a peripheral device.
- Attrition: An attack that employs brute force methods to compromise, degrade, or destroy the City's systems, networks, or services.
- Web: An attack executed from a website or web-based application.
- Email: An attack executed via an email message or attachment.
- Improper Usage: Any incident resulting from violation of the City's acceptable usage policies by an authorized user, excluding the above categories.
- Loss or Theft of Equipment: The loss or theft of a computing device or media used by the City, such as a laptop or smart phone.
- Personal Information: A user name or email address, in combination with a password or security question and answer that would permit access to an online

account; or an individual's first name or first initial and last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social Security number
- Driver's License number or California ID Card number
- Account number, credit or debit card number, in combination with any required security code, access code, or password that permits access to an individual's financial account.
- Medical information: Any information on an individual's medical history, condition, treatment, or diagnosis.
- Health insurance information: an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
- Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

- Other: An attack or suspected malicious activity that does not fit into any of the other categories.

1.4 Structure of Plan

1. Overview
2. Incident Responsibilities
3. Incident Preparation
4. Computer Security Incident Response

2. Incident Responsibilities

2.1 Responsible Executive

If the incident affects multiple departments, the City Manager, or his or her authorized designee shall be the Responsible Executive. If a single department is impacted, the department director responsible for that department shall fill this role. The responsibilities of the Responsible Executive include, but are not limited to:

- Receiving initial notification and status reports from the Incident Response Manager.
- Consulting with other department directors on public notification, involvement of the City Attorney, and notification of law enforcement.
- Consulting with Human Resources (for cases involving employees violating the City's acceptable usage policies).
- Written Notice, in plain language
  - Identification of a contact person at the City who can provide further information;
  - A list of the types of personal information that may have been the subject of the security breach;

  - If determined, the actual or estimated date or dates during which the security breach occurred;
  - Whether there was any delay in notification as a result of a law enforcement investigation;
  - A general description of the breach incident; and
  - The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number, or a driver's license number, or California identification Card number.
  - At the discretion of the City, the notice may also include information about what the City has done to protect individuals whose security has been breached, and advice on what steps persons might take to protect themselves as a result of the security breach.
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
- Substitute notice, if the City determines that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the City does not have sufficient contact information. Substitute notice shall consist of all of the following:
  - E-mail notice when the City has an e-mail address for the subject persons.
  - Conspicuous posting of the notice on the City's Web site page.
  - Notification to major statewide media.

- Advising the Incident Response Manager on priorities.
- Authorizing resources required for incident response.
- Consulting with other department directors, the Emergency Operations Manager and appropriate staff on priorities for response and recovery.
- Delegating Incident Commander responsibility to the Incident Response Manager in accordance with the City's Emergency Operations Plan.

In the specific case where the security breach involves personal information relating only to access to an online account, the City may provide notice in electronic or other format that directs the person whose personal information was breached to promptly change his or her password or security question, as applicable, or to take other appropriate steps to protect online accounts. If the online account is established by the City and the City has provided the person whose security was breached with log-in credentials, then certain additional notification requirements exist as provided in California Civil Code section 1798.29.

2.2 Incident Response Manager

The City designates the Chief Innovation Officer with the responsibility for preparing for and coordinating the response to a computer security incident. Responsibilities of the Incident Response Manager include, but are not limited to:

- Training users to recognize and report suspected incidents.
- Developing and testing response plans.
- Develop and maintain incident classification scheme.
- Being the point of contact should any employee or official believe an incident has occurred.
- Involving and organizing appropriate technical support to address the incident.
- Notifying the City Manager, department directors and appropriate staff that an incident has occurred.
- Advising the City Manager, department directors and appropriate staff regarding notification of law enforcement and the City attorney if appropriate.
- Communicating and coordinating with other external stakeholders, such as the City's Internet Service Provider (ISP), software vendors, governmental computer security organizations and other affected external parties.
- Providing information to the individual(s) responsible for notifying the press and public.
- Coordinating the logging and documentation of the incident and response.
- Functioning as Incident Commander for the duration of the incident/event.
- Making recommendations to reduce exposure to the same or similar incidents.

2.3 Computer Security Incident Response Team (CSIRT)

A Computer Security Incident Response Team (CSIRT) is an ad hoc group of technical and functional specialists that will respond to a computer security incident. A CSIRT will be activated depending on the nature and severity of a particular incident. The team will consist of a core group of technical specialists who are assisted by functional business specialists. The team may be comprised of City staff, contracted computer security resources, or both. The CSIRT has the authority, as delegated by the City Manager, to:

1) Monitor suspicious activity.
2) Disable computer and/or network services.
3) Confiscate or disconnect equipment.
4) Create copies or images of affected, or potentially affected, systems.
5) Conduct forensic analysis.
6) Coordinate with appropriate law enforcement officials.

2.4 Technical Support Staff

DoIT staff shall provide technical support to the Incident Response Manager. Responsibilities include, but are not limited to:

- Assessing the situation and providing corrective recommendations to the Incident Response Manager
- Helping the Incident Response Manager make an initial response to incidents.
- Responding to the incident to contain and correct problems.

- Functioning as member of a Computer Security Incident Response Team (CSIRT).
- Reporting to the Incident Response Manager on actions taken and progress.
- Assisting with internal and external communications
- Advising and consulting with the Incident Response Manager on priorities for response and recovery
- Participating in review of the incident and development of recommendations to reduce future exposure

2.5 Legal Counsel

The City Attorney and the Human Resources Department shall provide advice as called upon, such as determination of appropriate legal remedies and risk management strategy.

3. Incident Preparation

A key aspect of security incident response is preparation. Therefore, in preparation for potential security incidents the City should maintain the following capabilities:

3.1 Computer Security Incident Response Team Communication and Facilities

Includes:

- Primary and backup contact information for Computer Security Incident Response Team members, and others within and outside the City such as law enforcement and other incident response teams.
- On-call information for other teams and resources within the City.
- Smart phones, or some other communication and coordination device, in case of the failure of main modes of communication.
- Access to a means to send encrypted file transmissions, such as Secure FTP (SFTP) server and software, to be used among the CSIRT, within the organization and with external parties.
- "War room" for central communication and coordination. The City should identify a room or facility that will be used as a temporary war room when needed.
- Secure storage facility for securing evidence and other sensitive materials.

3.2 Incident Analysis Hardware and Software

Includes:

- Digital forensic workstations and/or backup devices to create disk images, preserve log files, and save other relevant incident data.
- Laptops for activities such as analyzing data, sniffing packets, and writing reports.
- Spare workstations, servers, and networking equipment (either physical or virtual), that may be used for test environments, restoring backups, etc.
- Portable printer to print copies of log files and other evidence from non-networked systems.
- Packet sniffers and protocol analyzers to capture and analyze network traffic.
- Digital forensic software to analyze disk images.

- Removable media with trusted versions of programs to be used to gather evidence from systems.
- Evidence gathering accessories, including notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions

3.3 Incident Analysis Resources

Includes:

- Access control lists and firewall rules.
- Event or activity records, often referred to as "logs." This includes the following types:
  - Security Logs – Event data from firewalls, anti-malware software, remote access systems and web proxy servers.
  - Software Logs – System event and audit records from the OS of servers, workstations, and networking devices (e.g., routers and switches).
  - Application Logs – Event data regarding account information, significant operational application failures, or major application configuration changes.
  - Network Logs - Network flow information from routers and other networking devices.
- Documentation of operating systems, applications, protocols, intrusion prevention/detection systems and anti-malware products.
- Network diagrams and lists of critical assets, such as database servers
- Current baselines of expected network, system, and application activity

3.4 Incident Mitigation Software and Data

Includes:

- Access to images of clean OS and application installations for restoration and recovery purposes.
- Access to backups of databases and files that need to restored.

While it is not expected that the City maintain all of the resources identified above, access to these resources, or an alternate means of supporting the functions that these resources provide, should be pre-identified.

4. Computer Security Incident Response

4.1 Incident Identification and Initial Assessment

Possible types of computer security incidents include, but are not limited to, the following:

- Attempts to gain unauthorized access to a system or its data.
- Unwanted disruption or denial of service (DoS).

- Unauthorized access to critical computers, servers, routers, firewalls, etc.
- Changes to system hardware or software without approval.
- Virus or worm infection, spyware, malware.

Any staff member or anyone affected by a City computer security incident should report the suspected incident in the City's Help Desk system. Secondary reporting options include: in person, by email or by phone to the Incident Response Manager.

The following information should be obtained from individuals reporting incidents:

1) Contact information.
2) Characteristics of incident.
3) Date and time incident was detected.
4) List of symptoms noticed.
5) Scope of impact (e.g. how widespread, number of users impacted, number of machines affected, etc.)
6) Nature of incident (e.g. denial of service, malicious code, unauthorized access, or other)

The Incident Response Manager will acknowledge receipt of the reported incident. All incident reports will be logged, analyzed and prioritized in order to generate an appropriate response plan. The Incident Response Manager will maintain a standard Computer Incident Report form to log incidents and a system for tracking incident information, status, etc. throughout the entire computer security event.

4.2 Incident Prioritization

The Incident Response Manager should prioritize security incidents using the following table as a general guideline. The incident priority classification will also assist with determining the Responsible Executive for the incident as defined in Section 2 of this plan.

Table 4-1 Security Incident Prioritization

Incident Factors	**Priority Characteristics**			
	Low	**Medium**	**High**	**Urgent**
Criticality – Application	Non Tier 1 or 2	Tier 2 Application	Tier 1 Application	Tier 1 Application
Criticality – Infrastructure	No	Limited scope	City Network-wide Impact	City Network-wide Impact
Impact – User/system	Affects a few people or a few systems	Department-wide impact	Several Departments	All Departments
Impact – Public	None	Potential impact	Likely impact	Definite impact

Countermeasures	Solutions are readily available	Weak countermeasures	No countermeasures	No countermeasures
Resolution procedures	Available and well defined	Resolution procedure not well defined, bypass available	No resolution procedures or bypass available	No resolution procedures or bypass available

The City Manager and the directors of affected departments should be notified immediately when a significant incident (defined as any event with Medium Priority or greater) is detected. A briefing should be provided to management by the Incident Response Manager with an assessment of the situation to help determine the necessary course of action.

As more information becomes available throughout the response process, the Incident Response Manager will provide additional briefings to help management determine if it is necessary to take additional steps, such as bringing in more resources, sharing information or involving law enforcement. The Incident Response Manager should also be prepared to determine potential business impacts to the City and work with the City Manager and department directors to provide appropriate measures to ensure continuity of operations.

4.3 Incident Staff Resources

The following table may be used as a guideline for determining staffing resources required for incident response. Each category reflects the level of and type of resources required to respond to and recover from an incident.

Table 4-2 Incident Staff Resources

Category	Definition
Regular	Time to recovery is predictable with existing resources.
Supplemented	Time to recovery is predictable with additional resources.
Extended	Time to recovery is unpredictable; additional resources and outside help are needed.
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).

The City should identify and pre-authorize additional external resources that may be required for the entire incident response process.

4.4 Incident Response Process

The incident response process includes three general phases. Following are the phases of the response process and the possible tasks that may be performed within each phase. The City should use the following tasks as a guideline only: each incident is unique, and different strategies may be used depending on the type of incident and the extent of the recovery process. All incident response process tasks should be logged and tracked by the CSIRT.

Phase One - Containment and Eradication

Tasks may include:

- Discussion with stakeholders.
- Initial intrusion, firewall and attack vector analysis.
- Collection and protection of information associated with an incident investigation
- Incident containment and determination of further recovery or bypass actions to be taken.
- Elimination of intruder's means of access and any related vulnerabilities.

Phase Two - Identification, Analysis & Notification

Tasks may include:

- Discussions and reviews with stakeholders.
- Log collection and review.
- Attack vector analysis.
- Determination of compromised systems.
- Imaging of compromised systems.
- Written or Electronic notice to affected parties.
- Forensic analysis.
- Determination of data loss, especially personally identifiable information (PII) or protected health information (PHI) (See Section 4.5)

Phase Three - Restoration, Rebuilding and Recovery

Tasks may include:

- Determine network architecture and software improvement recommendations for increased security.
- Execute restoration plan and return systems to normal operations.
- Deploy new security systems.
- Formulate and/or revise security policies.

4.5 Information Compromise and Data Loss

The City understands its fundamental role to protect and safeguard the information resources of the organization, and the residents and customers that it serves. As a result, one of the key objectives of the incident investigation will be the determination of possible information compromise and/or data loss. The table below provides examples of possible impact categories that describe the extent of information compromise that may have occurred during the incident. Note that it is possible for more than one category of information compromise as a result of a security incident.

Table 4-2 Information Compromise Categories

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised.
Privacy Breach	Personally identifiable information (PII) or protected health information (PHI) of residents, customers, employees, beneficiaries, etc. was accessed or exfiltrated.
Proprietary Breach	Sensitive data, or unclassified proprietary information, such as protected critical infrastructure information was accessed or exfiltrated.
Integrity Loss	Sensitive or proprietary information was changed or deleted exfiltrated and posted publicly).

4.6 Incident Closure

The Incident Response Manager should conduct a post-incident review of the investigation and document policy or procedural issues that enhanced or hindered incident detection, monitoring, investigation and subsequent development and implementation of corrective or problem bypass measures. The Incident Response Manager should prepare and publish a report, as required. The post-incident report should contain the following elements:

1) Executive Summary
2) Facts of the Incident
3) Business Impact
4) Root Cause
5) City Response
6) Residual Risks and Issues
7) Corrective Action Plan