

#2.4.1

**CITY OF BOTHELL  
ADMINISTRATIVE ORDERS**

**TITLE:** Information Security

**EFFECTIVE DATE:** June 1 2017

**REPLACES ORDER:** 2.4.1 dated April 1, 2014

**APPROVED BY:**

  
Name: Jennifer Phillips  
Title: City Manager

**1.0 PURPOSE:**

To maintain City of Bothell's (hereinafter, the "City") compliance with applicable laws and standards, protect the City from liability and protect the confidentiality, integrity and availability of City information systems, data and network resources.

**2.0 DEPARTMENTS/DIVISIONS AFFECTED:**

All.

<b>Chapter</b>	<b>Description</b>	<b>Date of Adoption or Revision</b>	<b>Section</b>	<b>Description</b>
1	Purpose and Scope	02/14	1.1	Adoption, Purpose and Scope
		02/14	1.2	Definition of Terms
2	User Responsibilities	02/14	2.1	User Understanding
		02/14	2.2	Network Access
		02/14	2.3	Building Access
		02/14	2.4	Data Handling
		02/14	2.5	Workstations
		02/21/2013	2.6	Purchasing
3	Information Services Roles and Responsibilities	02/14	3.1	Information Services Roles and Responsibilities
4	Access Control	02/14	4.1	Logical Control
		02/14	4.2	Physical Control
5	Risk Management	02/14	5.1	Risk Assessment
		02/14	5.2	Data Retention
		02/14	5.3	Security Training and Awareness
		02/14	5.4	Logging and Auditing
		02/14	5.5	Information Security Testing
		02/14	5.6	Malicious Software Protection
		02/14	5.7	Patch Management
		02/14	5.8	Personnel Vetting
6	Network Security	02/14	6.1	Network Security
				Transmission of Data
7	Incident Response	11/2/11	7.1	Incident Response Plan
8	Development	02/14	8.1	Application and Web Development
9	Change and Configuration	02/14	9.1	Change Control
			9.2	Information Systems Configuration
10	Employee Technologies	02/14	10.1	Employee Technologies
11	Distribution and Review	02/14	11.1	Distribution and Review
12	Compliance	11/2/11	12.1	Compliance

## City of Bothell Information Services Information Security Administrative Order

### FORWARD

This administrative order applies to all users of City of Bothell technology services and computer network, and technology located on City Premises, inside City Facilities or for the purpose of doing city business including but not limited to, employees, contractors, service providers and vendors.

This administrative order is necessary in order to maintain City of Bothell (hereinafter, the "City") compliance with applicable laws and standards, protect the City from liability and protect the confidentiality, integrity and availability of City information systems, data and network resources, and to assure the city realizes an effective return on its technology investments .

The City Information Security Administrative Order represents the combined efforts of the City Information Services Division (IS), Human Resources Department (HR), Legal Department and user communities.

<b>Date of Last Review</b>	<b>Section</b>	<b>Description</b>	<b>Required Under</b>
05/2017	all	Information Services Department Name Update. Information Services Manager to Director language update.	n/a
5/2017	1.2	Definitions added for PCI, WCIA, PII, CJIS. Information Systems, physical token, master plan definition update	n/a
5/2017	All	Updated CJIS and PCI acronym	n/a
5/2017	2.3	Updated employee ID badge language to match policy language added to ID badges.	PCI DSS 9.2
5/2017	5.3	Updated language related to Information	PCI DSS 12.6 v.3.2

		Security awareness training noting mandatory training	
5/2017	2.4	Updated language to include CJIS data handling	
5/2017	2.5	Clarified language regarding thumb drive encryption standards	PCI DSS 3.4
5/2017	4.1	Clarifying language regarding vendor remote access	PCI DSS 12.6
5/2017	5.8	Clarifying language to add CJIS clearance to vetting process	N/a
5/2017	Apx C	Updated Sensitive Information language	n/a
5/2017	4.2	Clarified language that makes it more understandable that those managing key card systems must be CJIS cleared and vetted	PCI DSS, CJIS

1.1 Adoption, Purpose and Scope

---

1. PURPOSE: To establish the authority for the adoption of the Security Administrative order
2. ORGANIZATIONS AFFECTED: All units of city government; branches, departments and divisions.
3. REFERENCE: Not applicable
4. ORDER:

The Information Security Administrative order is adopted by the City of Bothell City Manager. The City may at any time, make changes to this administrative order.

In the event that the Information Services Department determines that changes to this Administrative Order is appropriate, the Information Services Director will so advise the City Manager and present proposed revisions for consideration and adoption.

Adoption of Information Security Standard Operating Procedures. The Information Services Director is authorized and directed to adopt, amend and maintain Information Security Standard Operating Procedures as required by the banking industry, the City's liability insurance underwriter, and federal criminal justice agencies to assure the proper and responsible operation of the Information Services Department.

Annual Review. Review and technical approval is performed annually by the Information Services Security Officer, who is designated by the IS Director to ensure compliancy with PCI and external agency security requirements.

Information Security Administrative and Standard Operating Procedures Handbook. The Information Services Department is directed to maintain an Information Security Administrative and Standard Operating Procedures Handbook.

## 1.2 Definition of Terms

---

1. PURPOSE: To establish generally-accepted words and phrases used in the Information security administrative order manual

2. ORGANIZATIONS AFFECTED: All departments/divisions.

3. REFERENCE: Not applicable

4. DEFINITIONS:

Availability: Ensuring that information systems, data and network resources are available and ready for use when they are needed.

CJIS: Criminal Justice Information Services Security Requirements as mandated by the Federal Bureau of Investigation. These security requirements apply to all networks and information systems on which criminal justice information is stored or transmitted.

Cloud Services/Storage: Data services, applications, or storage provided by a third party and not operated or residing on the City's network.

Confidentiality: The protection of data from unauthorized disclosure.

CVC2/CVV2/CID/CAV2: Three or four digit security code printed on a payment card.

DMZ: Demilitarized zone. Network added between a private and a public network to provide an additional layer of security.

Employee: Any person employed by the City of Bothell, including those employed on a limited or part time basis.

Emergency Change: A change which, due to urgency or criticality, needs to occur outside of the City's formal change management process.

Employee Technologies: Technologies used by an employee to access or interact with electronic or sensitive data (i.e., remote-access technologies, wireless technologies, removable electronic media, laptops, PDAs, etc)

Encryption: Process of converting data into an unintelligible form except to holders of a specific cryptographic key.

Information Services Steering Committee (ISSC): A lateral city committee representing all city departments for the purposes of effectively leveraging technology purchases across City Departments in a manner aligned with city goals and objectives. The Committee consists of representatives from all city departments as appointed by department directors and is chaired by the Information Services Director. The ISSC meets quarterly to review progress on active Division projects and initiatives, reviews concept papers submitted by units of the city government wishing to make or receive a technology investment. At least once a year, the Committee reviews requests, develops priority ranking and recommendations which are forwarded to the City Manager by the Division for the City Manager's information.

Information System: Information systems include any devices that may be connected to or installed on the city network, a city-owned computer, city facility, or the city telephone system. Information systems include, but are not limited to: laptop computers, workstations, servers, scanners, computers, routers, switches, external hard drives, digital cameras, telephones, fax machines, printers, mobile phones or devices, smart phones, software or applications, thumb drives, wireless access points and networkable copiers.

Integrity: The accuracy, completeness and validity of information.

Limited Access Areas: Any areas within or around City buildings that are not regularly open to the public.

Logical Controls: Controls that limit logical or intellectual access to information systems and/or electronic data. For example, passwords, user accounts, firewall rules

Magnetic stripe data: Also referred to as "track data". Data encoded in the magnetic stripe or chip of a payment card.

Malicious software: Software designed to damage or disrupt information systems, data or network resources.

Network Resource: Communication links and network bandwidth.

PAN: Primary account number. The 16 digit number found on the front of credit cards.

PCI: Payment Card Industry Security Standards. Security standards, as related to credit card handling, set forth by the PCI Standards Council and mandated by financial institutions. These security requirements apply to all networks and information systems on which credit card or PII information is stored or transmitted.

Physical Controls: Controls that are physically implemented. For example, surveillance cameras, motion alarms, door locks, security guards.

Physical Token: City issued ID, visitors Badge, keycard, or other device lending to building or Information System access.

PII: Personally Identifiable Information. Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

PIN/PIN Block: Secret numeric password.

Risk: The likelihood of a given threat exercising a particular potential vulnerability, and the resulting impact of that adverse event on an organization.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or services used or provided by the City.

Sensitive Data: Sensitive data includes but is not limited to passwords, Social Security numbers, credit card information, protected health information (PHI), personally identifiable information (PII), bank account numbers, credit card numbers, tax ID numbers and criminal justice data that are stored, processed or transmitted on or by City information systems or network resources.

Technology Master Plan: An ongoing technology plan that is updated annually and maintained by Information Services. The plan provides a road map of significant technology related projects and assures that new and existing technologies are secured, maintained and implemented in alignment with city goals and in a manner to most effectively serve the needs of Bothell. The plan insures that major projects are incorporated into or anticipated in the capital facilities plan.

Strong Cryptography: A cryptographic algorithm or protocol that makes it very difficult for an unauthorized person to gain access to encrypted data.

Technology Services: Technology Services include, but are not limited to: technology-related professional services, brokering services, subscriptions, agreements, hosting, telephony or internet services and all other technology services provided by internal City staff or by any

other agency, firm, contractor or representative acting on behalf of or providing service to the City or on City premises.

Threat: Condition that may cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the City.

Two Factor Authentication: The use of two independent mechanisms for authentication (something you have and something you know). For example, a security token and a password or two layer password protection.

User: Anyone who accesses City information systems, data or network resources.

Visitor: A vendor, guest of an employee, service personnel, or anyone who needs to enter a City facility containing information systems, data or network resources for a short duration, usually not more than one day.

WCIA: Washington Cities Insurance Authority. The City's liability insurance provider.

## 2.1 User Understanding

---

1. PURPOSE: To ensure all users of information technology understand User Responsibilities within the information security administrative order.

2. ORGANIZATIONS AFFECTED: All units of city government, including branches, departments and divisions.

3. REFERENCE:

PCI DSS Requirements - Section 11, 12

WCIA Annual Audit and Review

CJIS Security Policy Section 5.2.1.2

4. ORDER:

Acknowledgement and Understanding. All employees are required to acknowledge that they have read and understand applicable sections of this Administrative Order (Appendix a,b).

Confidentiality. All employees who may have access to sensitive information as outlined in this document may be required to complete a confidentiality agreement (Appendix c).

## 2.2 Network Access

---

1. **PURPOSE:** To establish procedures for the protection of the City's information technology assets and data from potential network access intrusion.

2. **ORGANIZATIONS AFFECTED:** All units of city government, including branches, departments and divisions.

3. **REFERENCE:**

City of Bothell Personnel Policies and Procedures (10.5)

PCI DSS Requirements - Section 7 & 8

WCIA Annual Audit and Review

CJIS Security Policy Section 3.4, 4.4

4. **ORDER:**

**User Authorization.** Users must not attempt to gain access to City information systems, data or network resources for which they have not been given proper authorization.

- A. Access to City information systems and media must be provided only to those having a need for specific access in order to accomplish a legitimate task and must be based on the principles of need to know and least possible privilege.
- B. A unique user name must be used by all persons accessing City information systems and media containing sensitive data. Along with the unique user name, appropriate authentication methods must be used.
- C. Two-factor authentication must be used by users for remote access to City information systems and media containing sensitive data. City employees who telecommute must take all precautions necessary to secure any and all sensitive City data in their homes and prevent unauthorized access to any City information system or data.
- D. All login accounts are created by Information Services on an individual basis. Group, shared or generic login accounts are not permitted on City information systems.
- E. The following requirements must be met for passwords on such systems:
  - 1. User passwords must be changed at least every 90 days
  - 2. Passwords must be at least 8 characters long and include both numeric and alphabetic characters

3. Password reuse must be restricted to no more than once every 8 uses.
  4. User accounts must be locked after six failed login attempts. The lockout must be for at least 30 minutes or until authorized City personnel unlock the account.
  5. City employees must not use passwords that are also used for non-City accounts.
  6. Users must not share any City account passwords.
- F. All external data or telephony connections (including but not limited to internet or phone) must be approved by Information Services and be installed and managed in a manner that meets all criteria of this Administrative Order. All external data or telephony connections are subject to all management, monitoring, logging and external security testing and assessment requirements as outlined in sections 3, 4, and 5 of this document.

---

## 2.3 Building Access

---

1. PURPOSE: To establish procedures for the protection of the City's information technology assets and sensitive data.

2. ORGANIZATIONS AFFECTED: All units of city government, including branches, departments and divisions.

3. REFERENCE:

City of Bothell Personnel Policies and Procedures (10.5-F.1)

PCI DSS Requirements - Section 9

WCIA Annual Audit and Review

CJIS Security Policy Section 4.4

4. ORDER:

Employee Access to Limited Access Areas. Access to 'limited access areas' must be denied until specifically authorized by appropriate City personnel. Such access must be provided only to those having a need for specific access in order to accomplish a legitimate task and must be based on the principles of need to know and least possible privilege.

Visitor Access to Limited Access Areas. Visitors to 'limited access areas' must be formally authorized by an appropriate City employee to access such areas. Visitors must be provided a physical token (i.e., a photo ID badge) that has an expiration date and identifies a visitor as a non-employee. Visitors must return their physical token upon leaving a 'limited access area' or at the expiration date. Visitors to any City building must be escorted while in limited access areas. Visitors must sign a visitor's log prior to being granted physical access to 'limited access areas'. The log must document the visitor's name, the company represented, the authorizing City employee, and the date and time of entrance and departure.

Employee Identification. Employees must be provided a physical token (ie:, a photo ID badge) that identifies them as an employee. ID badges are to be visibly displayed on a neck lanyard or chest pocket clip as to clearly identify staff as a city employee. Identification cards and building access cards are required to be carried separately. Employees forgetting or misplacing an ID badge are required to notify Human Resources and obtain a temporary identification badge.

## 2.4 Data Handling

---

1. PURPOSE: To minimize the potential risk to sensitive employee or customer data through established best practice data handling.

2. ORGANIZATIONS AFFECTED: All units of city government, including branches, departments and divisions.

3. REFERENCE:

City of Bothell Personnel Policies and Procedures (10.5)

PCI DSS Requirements - Section 3, 7, 8, 9

WCIA Annual Audit and Review

Information Services Standard Operating Procedures (7.1)

4. ORDER:

Data Sharing. Sharing of electronic data with outside agencies, contractors, vendors, or any other entity is required to be examined by Information Services to ensure data can be shared without violation of mandated security requirements imposed by banking industry, law enforcement, HIPPA, or other agencies.

Credit Card Handling Procedures. City Employees who interact with payment card data must review and adhere to the City Credit Card Handling data handling requirements and processes.

Sensitive and PII Data Handling Procedures. City Employees who interact with sensitive data or PII data must review and adhere to City data handling requirements and processes.

Copying of Sensitive Data. When sensitive data on City information systems is remotely accessed, the data must not be copied, moved, or stored onto local hard drives or removable electronic media.

Payment Card Processing. After a payment card transaction is authorized, the following types of data must never be stored in electronic or written form at a City facility:

- A. Magnetic stripe data
- B. CVC2/CVV2/CID/CAV2
- C. PIN/PIN Block

---

## 2.5 Workstations

---

1. PURPOSE: To establish practices to protect the integrity of city information technology and sensitive data.

2. ORGANIZATIONS AFFECTED: All units of city government, including branches, departments and divisions.

3. REFERENCE:

City of Bothell Personnel Policies and Procedures (10.5-F)

PCI DSS Requirements - Section 3, 5, 6, 8

WCIA Annual Audit and Review

CJIS Security Policy Section 3.4

4. ORDER:

Downloading and Installing Software. City employees are responsible for obtaining the approval of their supervisor and the Information Services Department before downloading or installing software on any city-owned computer.

Technology Services and Web Based Applications. The use of any hosted or web based applications or services must be first approved by and coordinated through the Information Services Department. Technology Services and Web Based Applications, whether requiring a budget expenditure or at no cost to the City, are subject to these conditions. Refer to section 2.6-Purchasing for additional information.

Removing or Reconfiguring Software. City employees are not permitted to remove or reconfigure any software installed by Information Services. This includes, but is not limited to, virus software, workstation power configuration, and workstation security settings.

Workstation Security. City employees must take reasonable security measures to help prevent unauthorized access to their assigned city workstation or any workstation they are utilizing. Users are required to lock the workstation when leaving their work area for any extended period of time and all workstations must be powered down at the end of an employee's shift.

Non-City Equipment. Unless authorized by Information Services; employees, vendors and other user must not connect any non-city owned equipment into the City's network. This includes but is not limited to employee personal computer equipment, mobile devices, and vendor or presenter equipment.

External Devices. Workstation add-on or external devices, not authorized by Information Services and meeting encryption standards, are not permitted. Add-on devices include but are not limited to media burners, hard drives, thumb drives, and other removable storage device.

Ethics. All users of City information systems, data or network resources must use them in an ethical, legal and responsible manner. Unless otherwise authorized, all use of City information systems, data or network resources must be consistent with this Administrative Order.

Notification of Unauthorized Access. All users of City Information Systems, data, and network resources must notify Information Services of the loss of and/or unauthorized access to any City data.

Electronic Media. Electronic media must be purged, degaussed, shredded or otherwise destroyed so that sensitive data cannot be reconstructed.

---

## 2.6 Purchasing

---

1. PURPOSE: To establish centralized procurement practices to protect the integrity of the City information technology and sensitive data and to assure effective return on its IT investments .

2. ORGANIZATIONS AFFECTED: All units of city government, including branches, departments and divisions.

3. REFERENCE:

City of Bothell Personnel Policies and Procedures (10.5-F)

PCI DSS Requirements - Section 3, 7, 9

Information Technology Purchasing Administrative Order 2.4.2

WCIA Annual Audit and Review

4. ORDER:

Technology Purchases.

Acquisitions of all information systems, technology services, cloud services/storage, software and hardware must be first approved by the Office of the City Manager, or designee, regardless of funding source as governed by Administrative Order 2.4.2 (Information Technology Purchasing).

Additional Information Required for Understanding.

Refer to Administrative Order 2.4.2 for clarification and additional information related to purchasing.

---

### 3.1 Information Services Department Roles and Responsibilities

---

1. PURPOSE: To provide information to management and employees about the roles and responsibilities of the Information Service Division.

2. ORGANIZATIONS AFFECTED: Information Services.

3. REFERENCE:

PCI DSS Requirements  
CJIS Security Policy  
WCIA Annual Audit and Review

4. ORDER:

Security of Information Technology. While responsibility for information security on a day-to-day basis is every City employee's duty, specific guidance, direction, and authority for information security is centralized in the City's Information Services (IS) Division. Accordingly, this Division will:

- A. Establish, document and distribute information security policies, standards and procedures.
- B. Monitor and analyze security alerts and information and distribute to appropriate City employees.
- C. Establish, document, and distribute security incident response and escalation procedures
- D. Administer user accounts, including additions, deletions, and modifications
- E. Monitor and control all access to sensitive data

#### 4.1 Logical Control

---

1. PURPOSE: Establish procedures to limit logical access to the City's sensitive data based on authorization and need.

2. ORGANIZATIONS AFFECTED: All departments/divisions.

3. REFERENCE:

PCI DSS Requirements - Section 7 & 8

CJIS Security Policy Section 3.4, 4.4

WCIA Annual Audit and Review

4. ORDER:

Intellectual Access. Logical or intellectual access to City information systems and media potentially containing sensitive data must be denied until specifically authorized by appropriate City personnel.

Defined Access. Appropriate City information system owners and/or data custodians or their designated delegates must define and approve access to City information systems and media containing sensitive data.

Formal Documentation. The City must have a formal, documented user management process which enables the controlled addition, change, and termination of logical access rights on City information systems, data and network resources. The process must be capable of granting different levels of access to City information systems, data and network resources.

Limited Vendor Access. Vendor login accounts are permitted only to those individuals vetted through the City of Bothell and have acknowledged the City's information security policies. Login accounts and access ports on City information systems must be disabled until the specific time they are needed by the vendor. After appropriate use by the vendor, they must again be disabled. Vendors not completing the City's Information Security Training and acknowledgment process must be monitored at all times while accessing Bothell information systems.

Access Locking. Activation of information system locking software or log off must occur when a user session on a City information system is inactive for more than 15 minutes.

User Identity. User identity must be appropriately verified before any password, which enables access to a City information system or network resource, is reset.

User Accounts. User accounts that are inactive for more than 90 days on City information systems that store, process or transmit sensitive data must be disabled or removed.

Logical Access Review. At least every 6 months, appropriate City information system owners and/or data custodians or their designated delegates must review and verify logical access rights to City information systems and media containing sensitive data. Such rights must be revised as necessary.

Revocation. City employees and contractors experiencing a change in status (e.g. termination, position change) must have their logical access rights promptly reviewed, and if necessary, modified or revoked.

## 4.2 Physical Control

---

1. PURPOSE: Establish procedures to limit physical access to the City's sensitive data based on authorization and need.

2. ORGANIZATIONS AFFECTED: All departments/divisions.

3. REFERENCE:

PCI DSS Requirements - Section 9

CJIS Security Policy - Section 4.4

WCIA Annual Audit and Review

4. ORDER:

Annual Assessment. At least annually, the City must identify all of its physical areas that must be protected from unauthorized physical access. The assessment must take into consideration areas where sensitive data is stored, processed, or transmitted as well as the location of any supporting assets or critical infrastructure.

Securing Sensitive Data. City information systems and electronic and non-electronic media containing sensitive data must be located in physically secure areas ("limited access area"). Typically, such areas have a defined security perimeter such as a card controlled entry door or a staffed reception desk. City information systems located in unrestricted, public access areas must be physically secured to prevent theft. Access privileges to limited access areas must be reviewed at least annually. Those with access to secured areas where data is stored or those who have the ability to control access to those areas must be properly vetted by Information Services and the Police Department.

Video Monitoring. Cameras or other access control mechanisms must monitor the entry and exit points of City physical areas containing information systems that store, process or transmit sensitive data or electronic and non-electronic media containing sensitive data. Camera data must be stored for at least three (3) months unless otherwise restricted by law.

Public Access Areas. The City must control and restrict physical access to publicly accessible network jacks; it must also restrict physical access to wireless access points (WAPs), gateways and handheld devices located at City facilities.

Backup Media. Backup media, both paper and electronic, that contains sensitive City data must be stored in a secure location. The location's security must be reviewed at least annually. An inventory of all such media must be conducted at least annually.

Confidential Media. City electronic and non-electronic media containing sensitive data must be labeled as "confidential." Distribution of such media outside the City must be tracked and logged. Such media must only be distributed outside the City via a delivery method that can be tracked.

Relocation of Sensitive Data. Appropriate City management must approve the movement of any City media containing sensitive data from a limited access area.

User Documentation. The City must have a formal, documented process in place that clearly identifies and distinguishes between employees, contractors, and visitors.

Removable Media. The City must make efforts to reduce the risk of sensitive or confidential data exposure through the use of appropriately secured removable media and Information services such as thumb drives, external hard drives, etc.

## 5.1 Risk Assessment

---

1. PURPOSE: To establish procedures for annually reviewing potential vulnerabilities and adjust practices to ensure effective risk management.

2. ORGANIZATIONS AFFECTED: Information Services Division

3. REFERENCE:

PCI DSS Requirements - Section 10,11,12

CJIS Security Policy - Section 3.

WCIA Annual Audit and Review

4. ORDER:

Annual Assessment. The City must regularly identify, define, and prioritize risks to the confidentiality, integrity, and availability of its information systems, network resources and data. The City must conduct an annual formal, documented risk assessment of its information systems, data and network resources. The assessment must identify and prioritize the threats and vulnerabilities to the City's information systems, data and network resources and define likelihood and impact of risks.

Risk Assessment Process. The risk assessment must be used in conjunction with the City's risk management process to identify, select, and implement appropriate and reasonable controls to protect the confidentiality, integrity, and availability of the City's information systems, network resources, and data.

Risk Assessment Controls. The City must conduct risk management on a regular basis and select and implement reasonable, appropriate, and cost-effective controls to manage, mitigate, or accept identified risks. All such controls must be commensurate with identified risks.

Risk Assessment Reporting. Annually, the Director of Information Services must submit an information security risk management report to appropriate City management. The report must identify the significant risks to City information systems, data and network resources that have been identified during the past year, the risks that have been accepted and which risks have been mitigated.

---

## 5.2 Data Retention and Disposal

---

1. PURPOSE: To establish procedures for annually reviewing potential vulnerabilities and adjust practices to ensure effective risk management.

2. ORGANIZATIONS AFFECTED: All departments/divisions.

3. REFERENCE:

City Records Retention Schedule  
The Public Records Act (RCW 40.14)  
PCI DSS Requirements - Sec 3,7, 9  
CJIS Security Policy - Section 4.6  
WCIA Annual Audit and Review

4. ORDER:

Retention of Sensitive Data. The City must keep the storage of sensitive data to the minimum necessary required for business, legal and/or regulatory purposes. When no longer required for such purposes, sensitive data on City information systems or on City electronic and non-electronic media must be appropriately disposed of per the City's Records Retention Schedule and The Public Records Act. The following disposal methods must be used:

- A. Non-electronic media must be cross-cut shredded, incinerated or pulped.
- B. Electronic media must be purged, degaussed, shredded or otherwise destroyed so that sensitive data cannot be reconstructed.

Inventory and Auditing. City information systems and electronic and non-electronic media that contain sensitive data must be inventoried and audited on a quarterly basis to ensure that the stored data does not exceed the City's data retention requirements.

Data Masking. Unless otherwise authorized, credit card primary account numbers (PANs) on City information systems must be masked; the first six (6) and the last four (4) digits of the PAN are the maximum that can be displayed.

Portable Storage. PANs stored electronically on City information systems or portable storage devices must be made unreadable. One of the following methods must be used:

- A. Strong one-way hash functions
- B. Truncation
- C. Index tokens and pads

D. Strong cryptography

Media Destruction. Sensitive data on City electronic media and information systems must be securely and thoroughly erased before such items can be re-used.

### 5.3 Security Training and Awareness

---

1. PURPOSE: To develop and maintain an effective process for training management, employees, and technical staff on information security.

2. ORGANIZATIONS AFFECTED: All departments/divisions.

3. REFERENCE:

PCI DSS Requirements - Section 11, 12

CJIS Security Policy - Section 4.5

WCIA Annual Audit and Review

4. ORDER:

Training Commitment. The City must ensure that employees and contractors are provided with sufficient training and supporting reference materials to enable them to appropriately protect City information systems, network resources, and data. The City must provide information security awareness to its employees and contractors upon hire and then at least annually.

Training Schedule and Method. The City must provide regular security information and awareness to its employees and contractors via methods such as log-in splash screens, posters, email messages, memos, videos, and periodic meetings. Such information and awareness must include, but is not limited to:

- A. Any significant revisions to City Information Security Administrative Order
- B. Significant new city information security controls or processes
- C. Significant changes to City information security controls or processes
- D. Significant new security threats to City information systems, network resources, or data
- E. Information security best practices

Employee Understanding. Employees must completed mandatory information security training and acknowledge, at least annually, that they have read and understood the City's Information Security Administrative Order.

SWP ACCESS Training. Information Services employees must review the WSP ACCESS Security Training within 6 months of hire and reaffirm once every three years. Upon completion of the training employees must sign an ACCESS WSP (Washington State Patrol) Signature log to be collected by the Information Security Officer.

## 5.4 Logging and Auditing

---

1. PURPOSE: To establish process to ensure effective network and system activity is collected and monitored in order to reduce risk to the City's sensitive data.

2. ORGANIZATIONS AFFECTED: Information Services Department

3. REFERENCE:

PCI DSS Requirements - Section 10, 11

CJIS Security Policy - Section 4.1

WCIA Annual Audit and Review

4. ORDER:

Required Logging. Appropriate logging and monitoring controls must be implemented on City information systems, data and network resources.

Automated Audit Logs. The City must implement automated audit trails on its information systems that store, process or transmit sensitive data. The audit trails must be able to reconstruct the following events:

- A. Individual accesses to sensitive data
- B. Actions taken by any individual with root or administrative privileges
- C. Access to audit trails
- D. Invalid logical access attempts
- E. Use of identification and authentication mechanisms
- F. Initialization of audit logs
- G. Creation and deletion of system-level objects

For each of the above events, the following must be recorded:

- A. User identification
- B. Type of event
- C. Date and time
- D. Success or failure indication
- E. Origination of event
- F. Identity or name of affected data, system component, or resource

Intrusion Detection. Logs and audit trails on City information systems that store, process or transmit sensitive data must be reviewed daily. Such logs and audit trails must be monitored

by file integrity or change detection software. Log reviews must include intrusion detection and authentication, authorization and accounting (AAA) servers.

Log Data Protection. Information generated by logging and monitoring controls implemented on City information systems, data and network resources must be protected from unauthorized access. Access to such information must be limited to only those individuals with a need-to-know. Such information must be promptly backed up to a centralized log server and/or media that is difficult to alter. Logs for City wireless networks must be copied onto a log server on the City's internal network. Unless otherwise restricted by law, audit and log file information must be retained for at least one year.

Time Synchronization. City information systems must have their system clocks and times synchronized with a master time source (e.g. network time protocol [NTP]). Internal City time servers must not all receive time signals from external sources. Specific Internet time servers must be designated from which time updates will be accepted.

5.5 Information Security Testing

---

1. PURPOSE: To establish procedures to ensure the City network is regularly tested in order to protect the integrity of its information technology.

2. ORGANIZATIONS AFFECTED: Information Services Department.

3. REFERENCE:

PCI DSS Requirements - Section 11  
WCIA Annual Audit and Review

4. ORDER:

Penetration Testing. The City must annually perform internal and external penetration tests of its information systems that process, transmit or store sensitive data. The penetration tests must include both network and application layer tests.

Wireless Analysis. At least quarterly, a wireless analyzer must be used at City facilities to identify all wireless devices in use or a wireless IDS/IPS must be deployed which is capable of identifying all wireless devices in use at City facilities.

External Vulnerability Testing. The City must run quarterly external vulnerability scans against all of its information systems that are Internet reachable. The City must run quarterly internal vulnerability scans against all of its information systems that process, transmit or store sensitive data.

Traffic Monitoring. Per its risk assessment, the City must implement and maintain network IDS, host based IDS and/or IPSs to monitor all traffic to City information systems that process, transmit or store sensitive data.

File Integrity Monitoring. The City must deploy file integrity monitoring software on its information systems that process, transmit or store sensitive data. The software must perform critical file comparisons at least weekly.

---

## 5.6 Malicious Software Protection

---

1. PURPOSE: To establish procedures to ensure the City's computers are protected from malicious software.

2. ORGANIZATIONS AFFECTED: Information Services Department.

3. REFERENCE:

PCI DSS Requirements - Section 5, 6

CJIS Security Policy - Section 4.4

WCIA Annual Audit and Review

4. ORDER:

Antivirus Software Deployment. The City must deploy anti-virus software on its information systems commonly affected by malicious software. Such software must be capable of detecting, removing and protecting against malicious software including spyware and adware.

Antivirus Logging. Anti-virus software must be kept actively running and capable of generating audit logs. Anti-virus software must be regularly updated.

### 5.7 Patch Management

---

1. PURPOSE: To establish procedures to ensure the City's workstations are regularly patched in order to protect the City's data from operating system security vulnerabilities.

2. ORGANIZATIONS AFFECTED: Information Services Department.

3. REFERENCE:

PCI DSS Requirements - Section 3, 6  
WCIA Annual Audit and Review

4. ORDER:

Patches. The City must have a formal, documented process for regularly identifying and prioritizing relevant and necessary security and functional patches for its information systems and applications that process, transmit or store sensitive data. The City must use a risk based approach for prioritizing security patch installations. All critical new security patches must be applied within one (1) month of release.

5.8 Personnel Vetting

---

1. PURPOSE: To establish procedures to ensure the City's workstations are regularly patched in order to protect the City's data from operating system security vulnerabilities.

2. ORGANIZATIONS AFFECTED: All departments/divisions.

3. REFERENCE:

PCI DSS Requirements - Section 12

CJIS Security Policy - Section 3.4

WCIA Annual Audit and Review

4. ORDER:

New Employees. As determined necessary by the City's risk assessment, new City employees must be adequately vetted before being hired. Such vetting can include, but is not limited to, background checks, credit checks and/or personal references, and Police Background Investigation requirements, CJIS clearance. Such vetting is especially important for positions that involve access to sensitive data.

Confidentiality. New employees who may access sensitive data must sign a confidentiality (non-disclosure) agreement. This agreement must be regularly renewed. (Appendix c)

6.1 Network Security

---

1. PURPOSE: To establish procedures to ensure the City's network is designed and maintained in a manner to adequately protect the City's sensitive data.

2. ORGANIZATIONS AFFECTED: Information Services Department.

3. REFERENCE:

PCI DSS Requirements - Section 1, 4, 6, 10

CJIS Security Policy Section 3.4, 4.4

WCIA Annual Audit and Review

4. ORDER:

Firewall and Router Standards. The City must develop and implement formal, documented standards for its firewalls and routers. Such standards must include:

- A. A formal process for approving and testing all network connections and changes to City firewall and router configurations.
- B. A current diagram(s) of the City's computer network . The diagram must show all connections to City information systems that process, transmit or store sensitive data. This diagram should be reviewed and updated at least annually.
- C. Requirements for a firewall at each logical point where the City's network connects to the Internet and between any demilitarized zone (DMZ) and the City's internal network(s).
- D. A description of groups, roles, and responsibilities for logical management of City firewalls and routers.
- E. Documentation and business justification of all services, protocols, and ports allowed by City firewalls and routers, including documentation of security features implemented for insecure protocols (e.g. Telnet, FTP).
- F. A requirement to review City firewall and router rule sets at least every six (6) months.

Firewall Access. The City's firewalls must perform stateful inspection and must restrict connections between untrusted networks (i.e. the Internet) and City information systems

that process, transmit or store sensitive data. The firewalls must prohibit direct access from the Internet to such information systems.

Synchronization. Configuration files on City routers must be secured and regularly synchronized.

Wireless Networks. Firewall(s) must be installed between any wireless networks and City information systems that process, transmit or store sensitive data. Such firewalls must deny or control traffic from the wireless networks to the information systems.

DMZ. Outbound traffic from City payment card applications must be sent to IP addresses within a City DMZ; such traffic must not be sent directly to the Internet.

Location of Sensitive Data Storage. All City databases that store sensitive data must be placed in the City's internal network(s) and be segregated from any City DMZ.

Personal Firewall Software. Personal firewall software must be installed on any mobile and/or City employee-owned computers with direct connectivity to the Internet that are used to access the City's internal network.

IP Masquerading. IP masquerading (e.g., port address translation [PAT] or network address translation [NAT]) must be used for information systems on the City's internal network(s). Use of Proxy Servers or any technology to bypass network security is prohibited.

## 6.2 Transmission of Data

---

1. **PURPOSE:** To establish procedures to ensure the City's network is designed and maintained in a manner to adequately protect the City's sensitive data during transmission.

2. **ORGANIZATIONS AFFECTED:** Information Services Department.

3. **REFERENCE:**

PCI DSS Requirements - Section 4  
CJIS Security Policy Section - 3.4, 4.4  
WCIA Annual Audit and Review

4. **ORDER:**

**Encryption.** If sensitive data must be sent over an open, public network (i.e., the Internet), strong cryptography such as SSL, TLS, or IPSEC must be used to encrypt the data.

**Wireless.** If a City wireless network is used to transmit sensitive data, strong encryption (i.e. WPA2, IPSEC or SSL) must be used.

**Cryptography.** Strong cryptography must be used whenever sensitive data is sent via end-user messaging technologies (e.g., email, instant messaging, chat).

### 7.1 Incident Response Plan

---

1. PURPOSE: To establish procedures to ensure the City's workstations are regularly patched in order to protect the City's data from operating system security vulnerabilities.

2. ORGANIZATIONS AFFECTED: Information Services Department.

3. REFERENCE:

PCI DSS Requirements - Section 12

CJIS Security Policy - Section 3.4

WCIA Annual Audit and Review

4. ORDER:

Formal Incident Response Plan. The City must have a formal, documented security incident response plan. The plan must include:

- A. Roles, responsibilities, and communication strategies in the event of a security incident including notification of appropriate parties
- B. Specific incident response procedures
- C. Business recovery and continuity procedures
- D. Data back-up processes
- E. Legal requirements for reporting security incidents
- F. Coverage and responses for all critical City information systems
- G. Reference or inclusion of payment card brand incident response procedures
- H. Procedures for responding to alerts from intrusion detection (IDS), intrusion prevention (IPS) and/or file integrity monitoring systems

Annual Testing. The security incident response plan must be tested annually and must designate specific personnel to be available on a 24/7/365 basis in order to respond promptly to information security alerts. The plan must be reviewed regularly and modified as necessary.

Annual Training. City employees who are responsible for responding to security incidents must receive regular and appropriate training in security incident response processes.

---

## 8.1 Software Application Development

---

1. PURPOSE: To establish procedures to ensure web or local application development is performed in a secure manner.

2. ORGANIZATIONS AFFECTED: Information Services Department.

3. REFERENCE:

PCI DSS Requirements - Sec 5, 6  
WCIA Annual Audit and Review

4. ORDER:

Life Cycle. When the City develops software applications that store, process or transmit sensitive data ("City developed applications"), such applications must be developed per a formal, documented software development life cycle and be based on information security best practices.

Testing. Security patches and system and software configuration changes on City developed applications must be tested before being deployed.

Environment. The City must have separate development, test and production environments for City developed applications that process, transmit or store sensitive data. There must be clear separation of duties between the three environments. Real sensitive data must not be used or must be sanitized for testing or development of City developed applications.

Test Data. Test data and accounts must be removed before City developed applications are placed into the City's production environment. Custom code used in City developed applications must be reviewed for vulnerabilities before the code is used in the City's production environment.

Web Applications. Web applications developed by the City that process, transmit or store sensitive data ("City developed Web applications") must be based on secure coding best practices such as the Open Web Application Security Project (OWASP) guidelines. City developed Web applications must be protected against the following vulnerabilities:

- A. Malicious file execution
- B. Insecure direct object references
- C. Cross-site request forgery (CSRF)
- D. Information leakage
- E. Improper error handling
- F. Insecure cryptographic storage

- G. Insecure communications
- H. Inadequate authentication and session management
- I. Cross-site scripting (XSS) attacks
- J. Failure to restrict URL access
- K. Injection flaws

Web Firewall. A Web-application firewall must be placed in front of all Internet accessible City Web applications that process, transmit or store sensitive data.

---

## 9.1 Change Control

---

1. PURPOSE: To establish procedures that changes made to Information Systems are documented and authorized.

2. ORGANIZATIONS AFFECTED: Information Services Department.

3. REFERENCE:

PCI DSS Requirements - Section 10  
WCIA Annual Audit and Review

4. ORDER:

Documentation of Changes. The City must develop and implement a formal, documented change control process for information system, technology and software configuration changes. The process must include:

- A. Identification and documentation of significant changes
- B. Assessment of the potential impact, including security implications, of significant changes
- C. Ability to terminate and recover from unsuccessful changes
- D. Testing procedures to ensure the change is functioning as intended
- E. Communication of completed change details to appropriate persons
- F. The updating of appropriate information system or software documentation upon the completion of a significant change

Emergency Changes. Only properly authorized persons may make an emergency change to City information systems, data or network resources. Such emergency changes must be appropriately documented and promptly submitted, after the change, to the City's normal change management process.

---

## 9.2 Information System Configuration

---

1. PURPOSE: To establish procedures that changes made to Information Systems are documented, authorized and secure.

2. ORGANIZATIONS AFFECTED: Information Services Department.

3. REFERENCE:

PCI DSS Requirements - Section 6  
WCIA Annual Audit and Review

4. ORDER:

Configuration and documentation. The City must develop and implement formal, documented configuration standards for its information systems. Such standards must be consistent with system hardening best practices as defined by organizations such as SANS, NIST and CIS. At a minimum, the standards must require the following:

- A. One primary function for servers that process, transmit or store sensitive data
- B. Disabling of unnecessary and/or insecure services and protocols
- C. Appropriate configuration of system security settings
- D. Removal of unnecessary functionality (e.g., scripts, Web servers, subsystems)

Remote Logins. All remote logins that enable administrator access to City information systems storing, transmitting or processing sensitive data must be encrypted.

Identifying Vulnerabilities. The City must have a formal, documented process to identify newly discovered security vulnerabilities and update City configuration standards to address new vulnerabilities.

**10.1 Employee Technology**

---

**1. PURPOSE:**

**2. ORGANIZATIONS AFFECTED:** Information Services Department.

**3. REFERENCE:**

PCI DSS Requirements - Section 3, 6  
WCIA Annual Audit and Review

**4. ORDER:**

**Controls.** Employee technologies (i.e., remote-access technologies, wireless technologies, removable electronic media, laptops, tablets) that have the potential to access City data must only be used by employees and contractors if the following controls are in place:

- A. Appropriate Information Services approval for the use of the technologies
- B. Appropriate authentication is used
- C. A regularly updated inventory of devices and list of the persons with access to the devices
- D. Devices are labeled with owner name, contact information, and a description of the device's purpose
- E. Devices are appropriately used and placed in appropriate network locations
- F. The City maintains a regularly updated list of approved devices
- G. Devices are appropriately encrypted

**Remote Access.** Remote access sessions to City information systems containing sensitive data must be disconnected after twenty (20) minutes of inactivity. Remote access technologies used by vendors to access City information systems containing sensitive data must be turned off when not in use by the vendors.

11.1 Distribution and Review

---

1. PURPOSE:

2. ORGANIZATIONS AFFECTED: Information Services Department.

3. REFERENCE:

PCI DSS Requirements - Section 12  
WCIA Annual Audit and Review

4. ORDER:

Distribution. This Administrative Order must be published and distributed to all appropriate City employees, contractors, vendors, service providers and business partners.

Review. This Administrative Order must be reviewed at least annually and revised as necessary.

---

## 12.1 Compliance

---

### 1. PURPOSE:

2. ORGANIZATIONS AFFECTED: Information Services Department.

### 3. REFERENCE:

PCI DSS Requirements - Section 12  
WCIA Annual Audit and Review

### 4. ORDER:

Compliance. City employees and contractors must comply with all applicable parts of this Administrative Order. Compliance is necessary to ensure the confidentiality, integrity and availability of City information systems, data and network resources.

Non Compliance. City employees and contractors who do not comply with all applicable City security policies may be subject to disciplinary actions, up to and including termination of employment.

Contractual Agreements. Third party persons (i.e. vendors, service providers) who do not comply with this Administrative Order may be subject to appropriate actions as defined in contractual agreements.

## Information Security Administrative Order Approval

This document explains the City of Bothell's information security requirements for all employees. The City has developed and is committed to this policy in order to appropriately protect the confidentiality, integrity and availability of the City's data, information systems and network resources. This policy will be reviewed and revised, as necessary, on a regular basis.

---

Dated

---

Signature

---

Printed Name

## Information Security Administrative Order List of Appendices

<u>APPENDICES</u>	<u>TITLE</u>	<u>APPROVED BY</u>
A	Bothell Employee Acknowledgement	City Manager
B	Bothell Information Services Employee Acknowledgement	City Manager
C	Confidentiality Agreement	City Manager

Appendix A

**Bothell Employee Acknowledgment**

I have received a copy of the City's Information Security Administrative Order 'User Responsibilities'. I have read and understand the user responsibilities outlined in the Administrative Order and agree to observe the terms and conditions.

---

Dated

---

Signature

---

Printed Name

Appendix B

**Bothell Information Services Employee Acknowledgment**

I am in the Information Services Department and have received a copy of the City's Information Security Administrative Order. I have read and understand the full Administrative Order and agree to observe the terms and conditions.

\_\_\_\_\_  
Dated

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Printed Name

Appendix C  
**STATEMENT OF CONFIDENTIALITY AND NON-DISCLOSURE**

As an employee of the City of Bothell, I understand that I may have access to both electronic and nonelectronic information, data, and records (hereafter referred to as "data"). I understand that some of this data described below is confidential and/or sensitive, and I am responsible for maintaining and protecting this data against accidental or unauthorized access. I also understand that my access to this data as described below is limited to - and solely for the purpose of - the performance of my job duties.

By signing below, I affirm that I have been advised of, understand, and agree to the following terms and conditions of my access to the data contained in the information systems of the City of Bothell.

- I have been informed and understand that some data held by the City of Bothell is confidential and/or sensitive and may not be disclosed to unauthorized persons or in an unauthorized manner:
  - Sensitive data includes but is not limited to passwords, Social Security numbers, credit card information, protected health information (PHI), personally identifiable information (PII), bank account numbers, credit card numbers, tax ID numbers and criminal justice data that are stored, processed or transmitted on or by City information systems or network resources.
- I agree not to divulge, transfer, sell, or otherwise make known to unauthorized persons any confidential data. Further, I understand that if I receive a request for confidential data, or for information that I think may constitute confidential data, I will forward that request to either my departments designated public records person or the City Clerk's office for response. I understand and agree that my obligation to avoid such disclosure will continue even after I leave the employment of the City of Bothell.
- I also understand that I am not to access or use this data for my own personal information but only to the extent necessary and for the purpose of performing my assigned duties as an employee of the City of Bothell under this Agreement. I understand that a breach of this confidentiality will be grounds for disciplinary action, which may include immediate termination of my access to the information, termination of my employment, criminal penalties, and civil liability.

\_\_\_\_\_  
Signature of Employee

\_\_\_\_\_  
Printed Name of Employee

\_\_\_\_\_  
Date