City of Prosser
CITY COUNCIL
WORK SESSION MEETING AGENDA
Council Chambers, 601 7th Street, Prosser WA 99350
Tuesday, July 7, 2015 at 7:00 P.M.

1. **CALL TO ORDER**

2. **PLEDGE OF ALLEGIANCE**

3. **ROLL CALL**

4. **MAYOR AND CITY COUNCIL REPORTS AND COMMENTS**

   a) **Oath of Office of Reserve Officer Chris Baugh** *(City Clerk, Rachel Shaw)*

   b) **Prosser Aquatic Center Program Update** *(Lindsay Barnes, Pool Manager)*

5. **COUNCIL DISCUSSION**

   a) **Mayor Compensation**…….***Page 2***

   b) **IT Policy**……..***Page 5***

6. **ADJOURNMENT**

CITY OF PROSSER, WASHINGTON

AGENDA BILL

Agenda Title: Mayor Compensation Discussion		**Meeting Date:** July 7, 2015 Work Session	
Department: Administration	**Director:** Paul Warden	**Contact Person:** Paul Warden	**Phone Number:** (509) 786-2332
Cost of Proposal: $4200 annually - Based on a $850/month.			**Account Number:** 511-60-10
Amount Budgeted:			**Name and Fund#** General Fund (001)

Reviewed by Finance Department:

Attachments to Agenda Packet Item:
Compensation Comparison - Source AWC Survey

Summary Statement:
At the end of 2015, the wage for the position of Mayor will revert to the monthly wage of $500, or $6000 a year. Nine years ago in 2006 the Mayor's wage was increased from $300 to the present $500/month. The information attached was gathered to help facilitate a conversation regarding how this wage compares to like sized cities in our state and as compared to some neighboring communities.

Below is a summary of the AWC attached AWC data:

Comparison	Mayor	Council
Prosser	$ 500.00	$ 250.00
Union Comps	$ 727.00	$ 275.00
AWC 2499-7500	$ 938.52	$ 244.80
AWC 7500-14999	$ 1,748.79	$ 544.48

As we are a strong mayor form of city governance, the demands on the mayor's time are substantial. While there may be individuals who would put in the time to do the Mayor's various duties for the current pay, that doesn't address the fact that they should be fairly compensated for their time spent doing City business. It is hard not to spend 20 hours weekly working with administration, attending meetings etc. As well as the operational demands of being the CEO, the public demands for the Mayor's time for events and presence at organizational meetings can be challenging. Prosser may be small in

population but it makes up for that by being a very active, dynamic and challenging environment is which to operate in. Fairly compensating an engaged and hands on Mayor based on AWC's statewide compensation figures is a reasonable approach. Any change in compensation would not take effect until January, 2016.

Consistent with or Comparison to:

EXISTING ADOPTED OR PREVIOUS PLANS, POLICIES OR ACTIONS TAKEN BY THE COUNCIL

Recommended City Council Action/Suggested Motion:

No Action: The Council can review and discuss this information and provide staff with direction or request that staff provide additional information to assist in this evaluation.

Reviewed by Department Director:	Reviewed by City Attorney:	Approved by Mayor:
Paul Vander Date: 7-2-15	N/A Date:	Paul Vander Date: 7-2-15
Today's Date: June 17, 2015	Revision Number/Date:	File Name and Path:

Wage	Mayor	Council
Monthly	$ 500.00	$ 250.00
Annual	$ 6,000.00	$ 3,000.00

AWC 7500-14999	Population	Mayor	Council	Column1
Airway Heights	7970	$ 2,000.00	$ 750.00	
Burlington	8445	$ 4,242.00	$ 800.00	
Cheney	11310	$ 1,500.00	$ 450.00	
College Place	9050	$ 850.00	$ 375.00	
DuPont	9175	$ 1,300.00	$ 375.00	
East Wenatchee	13370	$ 4,687.00	$ 550.00	
Edgewood	9525	$ 338.00	$ 250.00	
Enumclaw	11110	$ 1,000.00	$ 325.00	
Ephrata	7930	$ 500.00	$ 200.00	
Ferndale	12710	$ 2,619.00	$ 572.00	
Fife	9045	$ 632.00	$ 526.00	
Gig Harbor	7985	$ 1,500.00	$ 600.00	
Grandview	11170	$ 540.00	$ 300.00	
Hoquiam	8625	$ 840.00	$ 260.00	
Kelso	11960	$ 800.00	$ 400.00	
Lake Forest Park	12750	$ 3,000.00	$ 600.00	
Liberty Lake	8675	$ 1,250.00	$ 400.00	
Lynden	12920	$ 1,800.00	$ 600.00	$200 per meeting
Newcastle	10850	$ 800.00	$ 700.00	
Othello	7695	$ 750.00	$ 300.00	
Port Orchard	13150	$ 5,343.00	$ 1,500.00	$500 per meeting
Port Townsend	9355	$ 750.00	$ 500.00	
Poulsbo	9775	$ 5,864.00	$ 500.00	
Sedro-Woolley	10610	$ 2,095.00	$ 500.00	
Shelton	9995	$ 1,510.00	$ 1,510.00	$1300+$70 per meeting
Snohomish	9270	$ 700.00	$ 450.00	
Snoqualmie	12130	$ 2,500.00	$ 500.00	
Sumner	9545	$ 1,800.00	$ 750.00	
Toppenish	8955	$ 450.00	$ 400.00	
Washougal	14910	$ 2,000.00	$ 475.00	
West Richland	13620	$ 550.00	$ 350.00	
Woodinville	11240	$ 700.00	$ 600.00	
Yelm	7915	$ 2,500.00	$ 600.00	
AWC Average		**$ 1,748.79**	**$ 544.48**	

Union Comps	Population	Mayor	Council
Clarkston	7210	$ 600.00	$ 250.00
College Place	9050	$ 850.00	$ 375.00
Goldendale	3410	$ 1,000.00	$ 100.00
Grandview	11010	$ 540.00	$ 300.00
Othello	7565	$ 750.00	$ 300.00
Selah	7340	$ 620.00	$ 325.00
Union Comps Average		**$ 727.00**	**$ 275.00**

Comparison	Mayor	Council
Prosser	**$ 500.00**	**$ 250.00**
Union Comps	**$ 727.00**	**$ 275.00**
AWC 2499-7500	**$ 938.52**	**$ 244.80**
AWC 7500-14999	**$ 1,748.79**	**$ 544.48**

AWC 2500 to 7499	Population	Mayor	Council	
Algona	3090	$ 1,500.00	$ 250.00	
Benton City	3255	$ 750.00	$ 75.00	
Black Diamond	4180	$ 1,000.00	$ 160.00	
Blaine	4865	$ 500.00	$ 300.00	
Brier	6345	$ 1,000.00	$ 350.00	$200 +$50/meeting
Buckley	4430	$ 500.00	$ 250.00	
Cashmere	3010	$ 400.00	$ 100.00	
Chehalis	7370	$ 150.00	$ 100.00	
Chelan	4020	$ 1,665.00	$ 550.00	
Chewelah	2615	$ 658.00	$ 100.00	
Clarkston	7225	$ 600.00	$ 250.00	
Clyde Hill	2995	$ 100.00	$ 150.00	$50/meeting
Colfax	2765	$ 600.00	$ 225.00	$75/meeting
Colville	4690	$ 1,000.00	$ 150.00	$50/meeting
Connell	5330	$ 600.00	$ 175.00	
Dayton	2545	$ 1,000.00	$ 150.00	
Deer Park	3870	$ 1,000.00	$ 200.00	
Duvall	7325	$ 1,500.00	$ 500.00	
Eatonville	2840	$ 1,402.00	$ 150.00	$50/meeting
Elma	3130	$ 500.00	$ 250.00	
Everson	2570	heathl ins	$ 150.00	
Fircrest	6555	$ 571.00	$ 571.00	$121; $150 reg meeting; $50 special meeting
Forks	3565	none	none	
Goldendale	3420	$ 1,000.00	$ 100.00	
Granger	3495	$ 650.00	$ 120.00	$40/meeting
Granite Falls	3390	$ 1,000.00	$ 100.00	
La Center	3050	$ 705.00	$ 355.00	
Mattawa	4460	$ 500.00	$ 62.50	
Medical Lake	4965	$ 700.00	$ 200.00	
Medina	3055	none	none	
Milton	7265	$ 1,500.00	$ 400.00	
Montesano	4075	$ 550.00	$ 200.00	
Moxee	3720	$ 500.00	$ 175.00	
Normandy Park	6375	none	none	
North Bend	6280	$ 2,000.00	$ 400.00	
Ocean Shores	5880	$ 4,000.00	$ 350.00	
Okanogan	2595	$ 724.00	$ 125.00	
Omak	4840	$ 1,200.00	$ 450.00	$150/meeting
Orting	7065	$ 1,000.00	$ 100.00	
Pacific	6830	$ 750.00	$ 200.00	
Quincy	7235	$ 1,200.00	$ 470.00	
Raymond	2890	$ 371.00	$ 247.00	
Ridgefield	6035	$ 500.00	$ 250.00	
Selah	7395	$ 620.00	$ 325.00	
Sequim	6910	$25 hr	$15/hour	
Stanwood	6530	$ 1,200.00	$ 325.00	
Steilacoom	6060	$ 750.00	$ 300.00	
Sultan	4665	$ 500.00	$ 150.00	
Union Gap	6140	$ 600.00	$ 600.00	
Wapato	5040	$ 833.00	none	
Warden	2710	$ 400.00	$ 160.00	
Woodland	5695	$ 3,300.00	$ 250.00	
Zillah	3140	$ 1,000.00	$ 180.00	$60/meeting
AWC Average		**$ 938.52**	**$ 244.80**	

CITY OF PROSSER, WASHINGTON

AGENDA BILL

Agenda Title: Review and Discuss the Information Technology Policy.		Meeting Date: July 7, 2015 Work Session	
Department: City Clerk	Director: Rachel Shaw	Contact Person: Rachel Shaw	Phone Number: (509) 786-8218
Cost of Proposal: $0 Amount Budgeted: $0			Account Number: Name and Fund#

Reviewed by Finance Department:

NA -

Attachments to Agenda Packet Item:

1. Information Technology Policy

Summary Statement:

During recent discussions with Council regarding amendments to the Personnel Policy, staff proposed the need to strike sections of Policy 905 "Use of City Owned Cell Phones" and Policy 906 "Computer, Electronic Mail (Email), Internet and Technology Use" and replace those sections with an Administrative Policy specific to Electronic Devices and Information Technology.

With recent changes in law regarding the Public Records Act and agency responsibility, it is important to address electronic records and devices and acceptable use of equipment. The attached Information Technology Policy is comprised of several sections that incorporate amendments to the Personnel Policy previously discussed with Council and includes updated provisions that protect both the employees and the City.

Based on Council direction, staff will send the Information Technology Policy to the Collective Bargaining Units for review.

Consistent with or Comparison to:

EXISTING ADOPTED OR PREVIOUS PLANS, POLICIES OR ACTIONS TAKEN BY THE COUNCIL

Recommended City Council Action/Suggested Motion:

Review and discuss the IT Policy. No action at this time, this is a discussion item only.

Reviewed by Department Director:	Reviewed by City Attorney:	Approved by Mayor:
Date: 7/1/2015	Date: 7/1/15	Date: 7-2-15
Today's Date: July 1, 2015	Revision Number/Date:	File Name and Path:

Information Technology Policy and Procedure
City of Prosser, Washington

SUBJECT: Information Technology		
Effective Date: _____, 2015	**Policy No.:** IT 001	**Pages:** 20
Developed By: Rachel Shaw, City Clerk	**Department Head Approval:**	**City Administrator Approval:**

DRAFT

OVERVIEW

1. PURPOSE

This policy is comprised of several sections that outline the acceptable use of computer equipment, email, internet, network, remote access and teleworking, storage, procurement, passwords, and personal devices for the City of Prosser. These rules protect the employees and the City. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

2. ORGANIZATIONS AFFECTED

This policy applies to all employees, agents and volunteers of the City.

3. REFERENCES

RCW 42.56 Public Records Act; RCW 40.14 Preservation and Destruction of Public Records; WAC 44-14 Public Records Act-Model Rules; WAC 434-662 Preservation of Electronic Public Records; and City of Prosser Personnel Policy.

4. DEFINITIONS

4.1 Computer Systems. The combination of computer hardware and software that allows for the user to input, store, print or distribute City information for internal or external purposes. A typical computer system consists of a central processing unit, monitor screen, keyboard, mouse, printer, modem, operating system and application software.

4.2 Computer Hardware. Any electronic device that is used to input, store, print or distribute City information for internal or external purposes. This includes, but is not limited to, personal computers, local area network file Servers and workstations, mainframe computers and terminals, printers, modems, scanners and backup units.

4.3 Computer Software. Any program or operating system that allows the user of computer hardware to input, store, print or distribute City information for internal or external purposes. This includes, but is not limited to, personal computer operating systems, network operating systems, word processors, spreadsheets, databases, accounting, electronic mail, management utilities and user interfaces.

4.4 Computer Networks. Computer systems linked together by department or location, for the purpose of sharing data or applications that are stored centrally. This includes local area network workstations, wide area network workstations, emulated personal computers and other systems that may be connected, such as bulletin boards, Internet, and on-line information services.

4.5 Computer Services. Any advice, support, recommendation or contact with a computer system, regardless of form or physical characteristic, which has been purchased or otherwise obtained by the City. Computer services are performed by Information Technology personnel or by an approved consultant. Computer services include, but are not limited to, recommending, purchasing configuring, installing and supporting computer systems. Support includes, but is not limited to, troubleshooting hardware and software problems, upgrading hardware or software, and assisting in using application software.

4.6 Electronic Records. Records stored or archived to a form that only a computer can process and the electronic transfer of information between staff, typically in the form of electronic notes and memoranda.

4.7 IP Address. Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.

4.8 Password. A unique authentication phrase used along with User ID when logging into the corporate network.

4.9 Personal Device. PDA (Personal Digital Assistant, i.e. smart phone) that combines computing, telephone, Internet and networking features.

4.10 PST. (Personal Storage) Data storage file that contains personal email information used by Microsoft Outlook and Exchange; includes email folders, contacts, addresses, and other data.

4.11 Server. A computer and storage device dedicated to storing files. Only authorized users on the network can access and store files on the Sever.

4.12 SPAM. SPAM (Unsolicited Internet Email) sites are links to websites from unsolicited Internet mail messages.

4.13 Text Messaging. An electronic communication sent and received by cellular phone.

4.14 User ID. User name or other identifier used when an associate logs into the corporate network.

4.15 VPN. Virtual Private Network (VPN), a network that uses public wires to connect securely between two locations. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. VPN is used by outside computers to connect to the City of Prosser network.

5. STATEMENTS OF POLICY AND PROCEDURES

5.1 General Provisions.

5.1.1 The City of Prosser provides employees with computer hardware, software and networks (WAN, LAN, Intranet and Internet). These resources are for business purposes. Information Technology resources may occasionally be used for incidental personal needs during breaks or lunch as long as such use does not result in or subject the City of Prosser to additional costs or liability, interfere with business productivity or performance, pose any additional risk to security, reliability or privacy, cause or tend to cause damage to the City of Prosser reputation or credibility, or conflict with the intent and requirements of any City policy or work rule, or State or Federal Law.

5.2 Acceptable Use.

5.2.1 All electronic data stored on computers or other electronic devices owned, used or leased by the City is the property of the City. As such the City retains the right, but not the duty, to monitor, read, review and copy any electronic data created, modified, stored, or used on any electronic device owned or used by the city or to perform City business, including but not limited to computers, telephones, PDAs and other communication devices, iPads, laptops, electronic tablets, notebooks, Kindles, Nooks, and similar devices, photocopiers, fax machines, etc. This monitoring includes, but is not limited to, reviewing files or correspondence created by any software medium, periodic scans of an employee's computer and review of department and system log files. Employees who use such devices at work or for work-related purposes waive any right to or expectation of privacy with respect to any such devices. Employees are required to provide the City with access to and copies of electronically-kept information that is the property of the City; and/or that was developed, accessed or used by employees to perform work for the City; and/or that was developed, accessed or used during work hours even if such information was developed, accessed or used on a device that is not owned by the City.

5.2.2 The City of Prosser's Information Technology department recommends that any information that users consider sensitive or vulnerable be encrypted and/or password protected.

5.2.3 For security and maintenance purposes, only authorized IT employees, management, or City contractors may monitor equipment, systems and network traffic at any time.

5.2.4 The City of Prosser reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

5.2.5 Employees shall not install copies of Computer Software, data, or personal information/data on any City equipment. If an employee requires the software, a copy must be purchased by the City.

5.2.6 To install software, the City of Prosser employees must contact the City IT Department and request installation via an IT Help Desk Request Form (Help Desk Request Form). Arrangements for installation will be made and employees will be notified when installation is completed.

5.2.7 City owned computer software is not to be taken home and installed on an employee's home computer, laptop, tablet, etc. for personal or City use, regardless of the computer software's licensing agreement.

5.2.8 Unless otherwise dictated by public disclosure laws and except to the extent disclosure of such information is protected under applicable labor laws relating to discussion of wages or working conditions among employees, all information regarding the computer networks, or data created by employees, is considered confidential. Removing data from City offices without the express consent of the City is considered a breach of confidentiality, except as otherwise provided in this section. Furthermore, all City related work should always be performed on City-owned or City-issued Computer Hardware unless employees are remotely connecting to the City's network. Violations of this City policy may lead to revocation of computer use or disciplinary action, up to and including termination.

5.3 Security and Proprietary Information.

5.3.1 Employees shall keep passwords secure. Employees shall not share email accounts. Authorized users are responsible for the security of their passwords and accounts. For more details, see Section 9: Password Policy.

5.3.2 All PCs, laptops, and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the computer is unattended.

5.3.3 Because information contained on portable computers is especially vulnerable, special care should be exercised and all City related work should always be performed on City-owned or City-issued devices. Further security requirements associated with use of personal devices may be found in Section 10: Personal Device Policy.

5.3.4 The following are laptop security tips, which must be observed when using a city-owned or a city-issued laptop/tablet:

5.3.4.1 Do not keep your Password in the laptop bag.

5.3.4.2 Do not leave your laptop/tablet unattended.

5.3.4.3 When you finish your task or work, either lock or log off your laptop/tablet.

5.3.4.4 Encrypt sensitive data – Do not store any confidential information on the local hard drive or any attached portable drives unless the data is encrypted. Please contact the City's Information Technology staff to set up encryption for your project files.

5.3.4.5 If your laptop/tablet is lost or stolen immediately report the theft to local authorities (such as the police) and to the City's Information Technology department.

5.3.4.6 All computers connected to the City of Prosser infrastructure, whether owned by the employee or the City of Prosser, must be continually executing approved virus-scanning software with up-to-date virus definitions.

5.3.4.7 Employees must use extreme caution when opening e-mail attachments received from unknown senders. E-mails may contain viruses or other malicious code.

5.4 Unacceptable Use.

5.4.1 Installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City of Prosser.

5.4.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, web sites, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City of Prosser or the end user does not have an active license.

5.4.3 Downloading or installing software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Appropriate management should be consulted prior to export of any material that is in question.

5.4.4 Introduction of malicious programs into Server Computer Hardware (e.g., viruses, worms, Trojan horses, etc.).

5.4.5 Revealing your account Password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

5.4.6 Using the City of Prosser's Computer Hardware or Computer Software to actively engage in procuring or transmitting material that is in violation of unlawful harassment or hostile workplace laws.

5.4.7 Making fraudulent offers of products, items, or services originating from any City of Prosser account.

5.4.8 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data where the employee is not an intended recipient or logging into a Sever or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties.

5.4.9 Unless otherwise dictated by public disclosure laws and except to the extent disclosure of such information is protected under applicable labor laws relating to discussion of wages or working conditions among employees, removing data from City offices without the express consent of the City, including unauthorized access and copying of confidential data to portable devices.

5.4.10 Executing any form of network monitoring which will intercept data not intended for the employee's computer, unless this activity is a part of the employee's normal job/duties.

5.4.11 Interfering with or denying service to any user (for example, denial of service attack).

5.4.12 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

5.4.13 Providing any personal information about the City of Prosser employees to anyone, except as required by law. Further, this rule does not prohibit employees from discussing and disclosing information regarding their own conditions of

employment, as well as the conditions of employment of employees other than themselves, amongst each other or to third parties.

5.4.14 Any form of harassment via email or telephone, whether through language, frequency, or size of messages.

5.4.15 Unauthorized use, or forging, of email information.

5.4.16 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

5.4.17 Use of the City email system for private business purposes.

5.4.18 Use of the City email system or telephone to violate the Open Public Meetings Act.

5.4.19 Use of the city's electronic equipment, directly or indirectly, for the purpose of assisting a campaign for election of any person to any office or for the promotion of or opposition to any ballot proposition, except as authorized by state law.

5.4.20 Use of the City's email or electronic equipment in violation of any other City Information Technology Policy.

5.5 Email and Communications.

5.5.1 **General Use.** The City of Prosser encourages its employees to utilize the email system, whenever practical, in lieu of using paper. Email is to be used for professional business communications. Use of language and subject matter should reflect business purposes. All use of Email must comply with the City's practices regarding fair employment and unlawful harassment policies. For more details, please see the City of Prosser Personnel Manual.

5.5.2 **Personal Use.** For non-business related email communication, employees are encouraged to use third party hosts (Hotmail, Google, Comcast, etc.). Occasional personal emails are allowed to be sent or received on the City's email system as long as such use does not result in or subject the City of Prosser to additional cost or liability, interfere with business, productivity or performance, pose additional risk to security, reliability or privacy, cause or tend to cause damage to the City of Prosser reputation or credibility, or conflict with the intent or requirements of any City policy or work rule. These emails should be kept to a minimum. Employees are highly encouraged not to include personal information within the same email or email string as city business communications as such personal information may be subject to public disclosure. Personal email sent or received on the City's email system may become subject to public disclosure and production for various reasons; thus, the City's email system is not an appropriate forum for any discussion of confidential or personal issues.

5.5.3 **Prohibited Use.** The City strives to maintain a work environment free of harassment and sensitive to the diversity of its employees, customers, and vendors. Therefore, the City prohibits employees' use of computers and electronic communication devices, regardless of whether they are owned by the City or by the employee or by a third party, in ways that are disruptive, offensive to others, or harmful to morale except to the extent such use is protected under applicable labor laws relating to discussion of wages or working conditions among employees. For example, but not by way of limitation, the display or transmission of sexually explicit images, messages, and cartoons is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, religion, politics, physical disabilities, or anything that may be construed as

harassment or showing disrespect for others based on their membership in or association with someone who is in a protected class as described in the City's policies regarding equal opportunity employment, harassment, and discrimination. All use of email must comply with the City's practices regarding fair employment and unlawful harassment policies. The City of Prosser email system further shall not be used for any of the following purposes:

5.5.3.1 Creation or distribution of chain letters or joke emails

5.5.3.2 Gambling

5.5.3.3 Violation of the Open Public Meetings Act

5.5.3.4 Use, directly or indirectly, for the purpose of assisting a campaign for election of any person to any office or for the promotion of or opposition to any ballot proposition, except as authorized by state law

5.5.3.5 Copyright infringement

5.5.3.6 Any other unlawful activity

5.5.4 Public Disclosure. All emails sent or received on the City's email system (in addition to other computerized records and attachments) meeting the definition of public record as defined in the Public Records Act, are subject to public disclosure and production unless specifically exempt under the Act. All email files stored on computers, other electronic devices, or email Severs owned or used by the City are regarded as the property of the City. Employees shall not store any personal information or date on any City Computer Hardware or Computer Software. All email files are subject to *review and disclosure by supervisory* or other personnel at any time without prior notification to employees. All email files are subject to review and disclosure to members of the public with or without prior notification to employees. Further, any emails sent or received in employees' personal email accounts relating to city business and meeting the definition of a public record as defined in the Public Records Act are subject to public disclosure and production.

5.5.5 Public Records Request. Any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by the City of Prosser regardless of physical form or characteristics is subject to a public records request.

5.5.6 Retention. The retention requirements for email and other Electronic Records are the same as the retention requirements for similar paper records listed on the records retention schedules approved by the State Local Records Committee. Questions regarding retention schedules should be forwarded to the City Clerk's Office. Management of Electronic Records is the responsibility of each user. Each user should periodically review his/her Electronic Records for deletion or archiving.

5.6 Internet.

5.6.1 General Use. The City of Prosser encourages its employees to utilize the Internet and various Internet resources to improve overall productivity, knowledge management, communication and customer service. Furthermore, acceptable use of the Internet and Internet resources includes, but are not limited to:

5.6.1.1 Communication between employees and non-employees for business purposes

5.6.1.2 IT technical support downloading software upgrades and patches

5.6.1.3 Research and review of possible vendor websites and product information

5.6.1.4 Referencing regulatory or technical information

5.6.1.5 Conducting research regarding city-related businesses

5.6.2 Personal Use. The Internet resources may be used for incidental personal use as long as such use does not result in or subject the City of Prosser to additional cost or liability, interference with business, productivity or performance, pose additional risk to security, reliability or privacy, cause or tend to cause damage to the City of Prosser reputation or credibility, or conflict with the intent or requirements of any City policy or work rule. Personal usage should generally conform to limits typically associated with personal phone calls. Thus, the City's Internet users are required to use common sense and exercise their good judgment while using Internet resources. This rule shall not be construed as prohibiting employees from discussing and disclosing information regarding their own conditions of employment, as well as the conditions of employment of employees other than themselves, amongst each other or to third parties via the internet or social media.

5.6.3 Inappropriate Use of Resources. The Internet shall not be used for transmission of information that promotes or transacts the following:

5.6.3.1 Commercial use - Any form of use for private business purposes is prohibited.

5.6.3.2 Copyright violations - Any use of the Internet that violates copyright laws is prohibited.

5.6.3.3 Harassment - Discrimination or harassment on the basis of age, race, color, gender, creed, marital status, national origin, disability or sexual orientation, or other status protected by law. The use of the Internet to harass employees, vendors, customers, and others is prohibited.

5.6.3.4 Political - The use of the Internet, directly or indirectly, for the purpose of assisting a campaign for election of any person to any office or for the promotion of or opposition to any ballot proposition, except as authorized by state law, is prohibited.

5.6.3.5 Aliases - The use of aliases while using the Internet is prohibited. Anonymous messages are not to be sent. Also, the misrepresentation of an employee's job title, job description, or position in the City is prohibited. City of Prosser employees may not post to any social media site or the Internet in the name of the City or in any manner that could be reasonably attributed to the City without prior authorization.

5.6.3.6 Misinformation/Confidential Information - The release of untrue, distorted, or confidential information regarding City business is prohibited. This rule shall not be construed as prohibiting employees from discussing and disclosing information regarding their own conditions of employment, as well as the conditions of employment of employees other than themselves, amongst each other or to third parties via the internet or social media.

5.6.3.7 Downloading of Non-Business Related Information - The downloading or any other method for retrieving non-City related information is prohibited except as defined in this policy.

5.6.3.8 Playing any games and/or any form of gambling.

5.6.3.9 Any activity that is prohibited by federal or state law, City code, ordinance, resolution, policies and guidelines.

5.6.4 Internet Use Filtering System and Exceptions. The Information Technology department may block access to Internet websites, social media and protocols that

are deemed inappropriate for the City of Prosser's corporate environment. The City has the sole discretion to determine what protocols and categories of websites will be blocked. Employees may request that a specific protocol, website or website service be un-blocked by submitting a request to the Information Technology Help Desk (Help Desk Request Form). An Information Technology employee, in consultation with City Management, will review the request and whether it is necessary for business purposes.

5.6.5 Public Disclosure. All access to the Internet and contents of hard drives and back-up systems which are created or received qualify as public records and therefore may be subject to disclosure under Ch. 42.56 RCW.

5.6.6 Social Media. The City of Prosser is permitted, to the fullest extent allowed by law, to request or require employees to share content from their personal social networking accounts to investigate unauthorized transfer of confidential information or employee misconduct. In addition, posts to social media accounts relating to City business may be subject to public disclosure and production under the Public Records Act.

5.7 Computer Network.

5.7.1 General Use. Network resources are made available by the City of Prosser to its employees to support their day to day business projects. Users must manage their electronic documents in accordance with record retention policies and procedures as defined and identified by the City Clerk's Office. Documents past their retention schedules, duplicate files, draft versions that do not represent significant basic steps in the preparation of a record document or miscellaneous files should be deleted from the network to save space and eliminate the need to backup unnecessary files.

5.7.2 Prohibited Use. Exploiting or attempting to exploit any vulnerability in application or network security is prohibited. Sharing of internal information with others that facilitates the exploitation of vulnerability in any application or network security is also prohibited. It is prohibited to knowingly propagate any kind of spyware, denial of service attack, or virus onto the City network or computers. If you encounter or observe vulnerability in any application or network security, report it to the City's Information Technology department immediately.

5.7.2.1 Disabling, altering, over-riding, or turning off any mechanism put in place for the protection of the network and workstation environments is strictly forbidden.

5.7.2.2 Because of band-width limitations inherent in any network system, use of the City network to download non-business related information is prohibited. Examples include but are not limited to streaming vide and online games.

5.7.2.3 Transmission, distribution, or storage of any information or materials in violation of federal, state or municipal law is prohibited. Software that is copyrighted or licensed may not be shared or illegally distributed. Copyright violations are federal offenses that may result in civil and criminal penalties to employees and the City of Prosser.

5.7.3 Network Access and Connectivity. The Information Technology department gives approval to connect devices to the City's network. This includes but it is not

limited to workstations, tablets, smart-phones, handhelds, scanners, hubs, switches, routers, printers, and remote connections, wireless and wired devices.

5.7.4 User Local Access. The Information Technology department authorizes all access to the City's computer network system. Only City of Prosser employees and authorized third parties (customers, vendors, etc.) may access the City of Prosser local network and resources by entering a valid user name and password. Network level access is driven by department or job description. If an employee moves to another department or changes job functions, a new network access request must be submitted to the Information Technology department. The same rule applies to users who cannot access certain data, project files and resources due to limited access rights. When submitting a request to the Information Technology department, requestors need to fill out the Employee IT Access Request (ITAR) Form (attached in the Appendix). All requests will be reviewed by the Information Technology department. Management will be notified about the network/data access request prior to a final decision.

5.7.5 Security. Each authorized employee and/or third party service provider or vendor will be assigned a unique User ID and password for network access. Access to systems and applications will only be allowed via unique User IDs and Passwords. Access will be monitored and actions will be traceable to authorized users. Users shall not share their password with any other person. The use of another person's account or attempt to capture other user's passwords is prohibited. Each user is responsible for restricting unauthorized access to the network by locking their computer or logging out of their computer account when leaving their computer unattended. If you discover unauthorized use of your account, immediately contact the City's Information Technology department.

5.7.5.1 Staff with access to critical information is responsible for its protection. Staff must take reasonable steps to ensure the safety of critical information including: encrypting data; ensuring that inadvertent viewing of information does not take place, and destroying or rendering the information unreadable when done with it in accordance with applicable records retention schedules.

5.7.5.2 The City will restrict access to critical information only to staff that have a legitimate business need-to-know. Each system owner is responsible for keeping an inventory of critical information and ensuring that access to it is limited.

5.7.6 Document Retention. Users must manage their electronic documents in accordance with the record retention policies and procedures as defined and identified by the City Clerk's Office. Documents past their retention schedules, duplicate files, draft versions that do not represent significant basic steps in the preparation of a record document or miscellaneous files should be deleted from the network to save space and eliminate the need to backup unnecessary files.

5.7.7 Backup and Recovery. Daily backup and recovery procedures are based on the industry best practices as well as State and City mandated retention schedules. Employees should not save data to their local computer hard drives as these are excluded from the backup and recovery procedures.

5.7.8 Public Disclosure. All Electronic Records meeting the definition of a "public record" as defined in the Public Records Act are subject to public disclosure and production unless specifically exempt under the Act. All Electronic Records are regarded as property of the City. The City's Electronic Records are not

confidential to the extent they may be monitored, read, or reviewed by City personnel at any time without prior notification to employees and/or subject to public disclosure and production. All files are subject to review and disclosure to members of the public with or without prior notification to employees. Thus, users recognize they cannot have any expectation of privacy in any e-mail communication, or any temporary or permanently stored data, and that the City of Prosser has no intention or purpose to keep such communications private or confidential to the extent public disclosure and production is required by law or to the extent that such communications may be monitored internally.

5.7.9 Appropriate Use. Do not release any information to anyone about the City's IT infrastructure system. Public records requests received for documents containing information about the City's IT infrastructure system should be forwarded to the City Clerk's Office. Forward any inquiries about the City's IT infrastructure to the City's Information Technology department.

5.7.9.1 Do not share your password with anyone.

5.7.9.2 Do not write your password down.

5.7.9.3 Change your password at least every 6 months.

5.7.9.4 Lock your computer or password-enable your computer screen saver so when you leave your desk someone else cannot access your files. For assistance in setting this up, contact the City's Information Technology department.

5.7.9.5 Do not save City files or information on your personal computer. If uniquely-created or edited documents are maintained on a personal computer, the procedure for such documents as provided in Section 10: Personal Device Policy should be followed.

5.7.9.6 Certain websites may try to obtain information about your city computer use and habits. Carefully read any pop-up messages and other alerts before responding.

5.7.9.7 Do not store personal information that is not required for City business. Do not conduct personal business on any City computer equipment, except incidental use as otherwise allowed in Section 2: Acceptable Use Policy. Personal information stored on City computers may be subject to public disclosure and production (RCW 42.56). Failure to follow this policy will violate computer use policies.

5.8 Remote Access and Mobile Computing (Teleworking).

5.8.1 General Use. Only City of Prosser approved employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of remote access and/or VPN, a user managed service. This means that the City's Information Technology department will only support City owned or leased equipment. On non-City owned or leased equipment, the user is responsible for installing an appropriate remote access and/or VPN program, configuring remote access software and/or VPN program and selecting an Internet Service Provider (ISP).

5.8.2 General Provisions. Requestors need to fill out an IT Access Request Form (ITAR) (attached in the Appendix) and indicate a business need for the remote access.

5.8.2.1 Remote connection to the City network is denied unless specifically authorized by the appropriate department manager and the Information Technology department.

5.8.2.2 Upon approval, the Information Technology department will allow entry through the City's firewall.

5.8.2.3 VPN users must use secure VPN software with an authorized ID and password. Access will be monitored and actions will be traceable to authorized users. Users shall not share their password with any other person. The use of another person's account or attempt to capture other user's passwords is prohibited. Each user is responsible for restricting unauthorized access to the network by locking their computer or logging out of their computer account when leaving their computer unattended. If you discover unauthorized use of your account, immediately contact the City's Information Technology department.

5.8.2.4 Remote access users will be automatically disconnected from the City of Prosser's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network.

5.8.2.5 All computers/mobile devices connected to the City of Prosser internal networks via VPN, Remote Desktop or any other technology must use the most up-to-date anti-virus software.

5.8.2.6 By using remote access technology with personal equipment, users must understand that their machines are a de facto extension of the City of Prosser's network, and as such are subject to the same rules and regulations that apply to the City of Prosser owned equipment.

5.9 Portable Storage Devices.

5.9.1 Policy. Unless otherwise dictated by public disclosure laws and except to the extent disclosure of such information is protected under applicable labor laws relating to discussion of wages or working conditions among employees, all information regarding the computers systems, or data created by employees, is considered confidential. Removing data from City offices on storage devices, including but not limited to flash drives, CDs, DVDs, and other portable devices, without the express consent of the City is considered a breach of confidentiality, except as otherwise provided in this section. Furthermore, all City related work should always be performed on City-owned or City-issued device unless employees are remote connecting to the City's network.

5.9.2 General Use: The following are examples of types of uses where a portable device may be needed:

5.9.2.1 Presentations – External presentation material

5.9.2.2 Service Providers – Sharing data and information with external service providers

5.9.2.3 Public Requests – Sharing data and information with public requestors

5.9.2.4 IT – IT support and backup operations

5.9.2.5 EOC – Emergency Operation Center support and operations

5.9.3 Prohibited Use. Portable devices are easily lost or stolen, presenting a high risk for unauthorized access and an introduction of malicious software. Therefore, sensitive data and programs may not be stored and transported on a portable device. Unique documents generally should not permanently reside on storage devices, but should be transferred to the City's network for retention.

5.9.4 Security. All portable devices will be automatically scanned by City of Prosser antivirus software.

5.9.4.1 Before any portable devices are connected to the City of Prosser infrastructure (example: Vendor presentation running from a flash drive or vendor submitting project as-builts), the City staff must log in as a "PC Browser" to the specific City owned or leased workstation. The PC Browser user profile has limited access rights, ensuring that the City network is not exposed to potential malicious software.

5.10 Procurement.

5.10.1 Policy. All Computer Software and Computer Hardware and third party IT services acquisitions/outsourcing must be reviewed by the IT staff prior to purchase. All IT related installations will be performed by the IT staff and in coordination with Department who purchased software.

5.10.2 Procedure: The IT staff has the experience and resources to assist departments in making wise technology choices. IT can recommend suppliers. IT can evaluate alternatives. IT can ask questions that may not be in the department's area of expertise. Departments are expected to involve IT in the early stages of evaluation and in the final stage of selection.

5.10.2.1 Departments must follow the City's Purchasing Policy (Policy ADM 004) for purchases of materials, supplies, and equipment.

5.10.2.2 Upon procurement, arrangements for installation can be made by contacting the City's IT Department via the IT Help Desk Request Form. Departments and employees will be notified when installation is completed.

5.11 Passwords.

5.11.1 Policy. Passwords need to meet the following requirements:

Administrator/Domain Level Accounts & Passwords	**Other Accounts & Passwords**
• At least 12 characters in length	• At least 8 characters in length
• Changed at least every 6 months	• Changed at least every 6 months
• Contain at least three of the four following character classes: o Lower case characters o Upper case characters o Numbers o "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)	• Contain at least three of the four following character classes: o Lower case characters o Upper case characters o Numbers o "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)
Passwords may not be: 1. Reused 2. Shared with other employees 3. Written down and stored near your computer	
Note: Try to create passwords that can be easily remembered.	

5.11.2 Procedure. Some systems and applications come with accounts and passwords that are set at the factory. These default accounts and passwords are widely

available online; if this account is left running with a password which was set by the vendor, then the system is at a higher degree of risk for compromise.

5.12 Personal Owned Device.

5.12.1 Policy. The City of Prosser is not responsible for troubleshooting personally-owned devices or instructing staff on how to use them. Except as approved, the City of Prosser is not responsible for reimbursing any costs associated with use of any personally-owned device, including but not limited to phone or data plans. Furthermore, by connecting personal devices, users acknowledge that their devices are a de facto extension of the City of Prosser's network, and as such may be subject to reasonable searches designed to located documents for public disclosure and production (RCW 42.56) and the City's IT Policies.

5.12.2 General Provisions. Employees who use their own personal smartphone and tablet devices to access and sync with the City's email services must meet the following criteria to ensure that the City's data is protected: City employees who want to access and sync City email, calendar and contacts with their personal devices must complete the IT Personal Device Access (PDA) Form (attached in the Appendix). Upon approval of the appropriate City authority, requestors will receive access.

5.12.3 If your device is lost or stolen, you are required to promptly contact the City's Information Technology Department by calling (509) 786-8218. IT will be able to change your credentials and prevent unauthorized access to the City's email resources.

5.12.4 The following personal technologies/devices can be used to sync with the City's email services:

5.12.4.1 Smartphone

5.12.4.2 Tablet

5.12.4.3 Computer

5.12.4.4 Devices should be configured with a local password (PIN) to control access to the user device and to protect City data residing on the device. Those passwords should not be shared with other users.

5.12.4.5 No critical data Social Security Numbers, Credit Card Numbers, and etc.) should be stored on mobile devices.

5.12.4.6 Use reasonable precaution before downloading applications and review permissions before granting access to your device. Many market apps require access to mobile device key functions such as email, texting, pictures, videos, etc.

5.12.5 Creating Unique Documents on Personal Devices. While documents or data sent or received on the city's email system are archived and accessible for purposes of responding to a request for public records, unique documents created on personal devices, such as laptops, smartphones, or tablets, would not be captured for retention. Consequently, employees with a City email address should forward any uniquely-created or edited documents on their personal devices to themselves via email and delete the original document on the device. If a City of Prosser employee or volunteer is not provided with a City email address, such volunteer or official is requested to forward any uniquely-created or edited documents relating to City business to the City Clerk for retention and delete the original document on the device. However, uniquely-created or edited

documents may not be deleted from the personal device if the document is responsive to a pending public records request.

5.12.6 Text Messaging. Using text messaging for City of Prosser business-related communications is discouraged, whether on personal or city-owned or issued devices. The City of Prosser provides an email system to conduct City business. Should text messaging be used for City of Prosser business-related communications in violation of this policy, in addition to any other disciplinary action, the City may request or require, as authorized by law, the texting employee to sign an authorization for a third party to disclose the transcripts of such text messages for purposes of response to a request for public records. Text messaging in emergency situations may be permitted, depending upon the extent of the emergency.

5.13 City-owned or City-issued devices.

5.13.1 Policy. City owned or City issued devices will be configured to automatically install and update core functions per manufacture/service provider recommendations. Furthermore, users acknowledge that their devices are a de facto extension of the City of Prosser's network, and as such may be subject to reasonable searches designed to located documents for public disclosure and production (RCW 42.56) and the City's IT Policies.

5.13.2 General Provisions. The following are further details pertaining City owned or City issued devices:

5.13.2.1 *General Use* – Resources are made available by the City of Prosser to its employees to support their day-to-day business projects. Users must manage their electronic documents in accordance with record retention policies and procedures as defined and identified by the City Clerk's Office.

5.13.2.2 *Personal Use* – Resources may be used for incidental personal use as long as such use does not result in or subject the City of Prosser to additional cost or liability, inference with business, productivity or performance, pose additional risk to security, reliability or privacy, cause or tend to cause damage to the City of Prosser reputation or credibility, or conflict with the intent or requirements of any City policy or work rule. Personal usage should generally conform to limits typically associated with personal phone calls. Thus, the City's Internet users are required to use common sense and exercise their good judgment while using Internet resources.

5.13.2.3 *Public Disclosure* - All Electronic Records meeting the definition of a "public record" as defined in the Public Records Act are subject to public disclosure and production unless specifically exempt under the Act. All Electronic Records are regarded as property of the City. The City's Electronic Records are not confidential to the extent they may be monitored, read, or reviewed by City personnel at any time without prior notification to employees and/or subject to public disclosure and production. All files are subject to review and disclosure to members of the public with prior notification to employees. Thus, users recognize they cannot have any expectation of privacy in any electronic communication, or any temporary or permanently stored data, and that the City of Prosser has no intention or purpose to keep such communications private or confidential to the extent

public disclosure and production is required by law or to the extent that such communications may be monitored internally.

5.13.2.4 *Termination of employment or end of term of service* - Upon termination of employment or end of term of service, devices are to be returned to the City in accordance with adopted policies.

Appendix

A. IT Access Request (ITAR) Form
B. IT Personal Devise Access (PDA) Form

IT Access Request (ITAR) Form	2015
Information Technology Form	

Instructions: *This form is to be filled out by the Employee's Supervisor/Department Director and submitted to* the City Clerk's Office via email at, rshaw@ci.prosser.wa.us *for processing. Be sure to fill out all applicable fields before submitting this form. Once the account is created, the information will be sent to the Supervisor/Department Director.*

Employee/Service Provider Information	
Position	☐ Employee ☐ Service Provider
Status	☐ New Hire ☐ Transfer ☐Termination ☐Update
Effective Date	Click here to enter a date.
Name (First, Last)	Click here to enter text.
Position or Title	Click here to enter text.
Department	Choose an item.
Phone Number	Click here to enter text.
Email	Click here to enter text.

Requestor Information	
Requestor Name (First, Last)	Click here to enter text.
Department	Click here to enter text.
Phone Number	Click here to enter text.
E-Mail	Click here to enter text.

Access to Information Technology Standard Resources		
	Resource	**Comments**
☐	Workstation	Workstation with standard productivity software.
☐	Laptop/Tablet	Laptop/tablet with standard productivity software.
☐	Desk Phone	City provided office phone. Ext: Click here to enter text.
☐	Cell Phone	City provided cell phone. Number: Click here to enter text.
☐	Email Account	(first letter of first name and last name@ci.Prosser.wa.us)
☐	Internet Access	Provides access to the internet via approved only web browser.
☐	Network Access	Provides access to department's folders drive, shared resources and peripherals. **Additional Access:** Click here to enter text.

Access to Applications, Programs & Databases					
	Resource	Read Only	Write	Modify	Grant Access Same as (e.g. list employee name)
☐	Office Exchange	☐	☐	☐	Click here to enter text.
☐	BIAS	☐	☐	☐	Click here to enter text.
☐	GIS	☐	☐	☐	Click here to enter text.

Comments: Any additions or special requests should be entered into the Comments field.
Click here to enter text.

Termination/Departure: In the event of termination/departure please answer the following questions:
Who should receive emails sent to the departed employee? Click here to enter text.
Who should have access to the departed employee's emails? Click here to enter text.
Who should have access to the departed employee's project/personal (U drive) files? Click here to enter text.

Authorization

Department Director	Date
IT Staff	Date

Personal Device Access (PDA) Form	2015
Information Technology Form	

Instructions: *This form is to be filled out by the Requestor and submitted to* City Clerk's Office via email at, rshaw@ci.prosser.wa.us *for processing. Be sure to fill out all applicable fields before submitting.*

Requestor Information	
Position	☐ Employee ☐ Volunteer
Name (First, Last)	Click here to enter text.
Department	Click here to enter text.
Phone Number	Click here to enter text.
E-Mail	Click here to enter text.

Personal Device Information		
	Smartphone	**Tablet**
Manufacture	Click here to enter text.	Click here to enter text.
Model	Click here to enter text.	Click here to enter text.
Operating System (OS)	Click here to enter text.	Click here to enter text.
Phone Number	Click here to enter text.	

Is your device configured with password (PIN)?
Click here to enter text.

Is your device "Remote Data Wipe" feature activated?
Click here to enter text.

Is antivirus install and configured on your device? If yes, please specify application name and version?
Click here to enter text.

Authorization

Department Director _____ Date _____

IT Staff _____ Date _____