


Policy Title:	<b>Acceptable Use Policy</b>		
	<b>OFFICE OF CHIEF INFORMATION OFFICER</b>	<b>Category</b>	Information Technology Services
		<b>Administrative Policy #</b>	
		<b>Revision #</b>	
		<b>Review Frequency</b>	As Needed – no less frequently than triennially
<b>Administrative Division</b>	Information Technology Services (ITS)	<b>Reviewed By</b>	Chief Information Officer; Director of Human Resources
<b>BOWC Approval</b>		<b>Last Reviewed/Update Date</b>	
<b>Implementation Date</b>			

## 1. OBJECTIVES

- 1.1. To protect the integrity and availability of DWSD’s information and technology resources from unauthorized use or modification, from accidental or intentional damage or destruction by persons authorized to use DWSD’s computer and technology resources.

## 2. PURPOSE

- 2.1. The purpose of this policy is to ensure the acceptable use and control requirements of the Public Internet, DWSD electronic communications, including but not limited to: email, instant messaging (IM), and text messaging, and DWSD computer and technology resources. Additionally, this policy is to protect the integrity and availability of DWSD networks. These rules are in place to protect the employee and DWSD. Inappropriate use exposes DWSD to risks including virus attacks, compromise of network systems and services, and legal issues.

## 3. DEFINITIONS

“Chain of Command” means the supervisory and management structure of DWSD.

“DWSD” or “Department” means the City of Detroit Water and Sewerage Department.

“Direct Supervisor” or “Direct Supervision” means the Public Servant who exercises immediate supervisory authority regarding another Public Servant’s job performance or conduct; the person responsible for monitoring a Contractor’s performance.

## 4. SCOPE

- 4.1. This policy applies to all DWSD employees, contractors, student interns, volunteers, and other persons authorized to use DWSD’s computer and technology resources. Failure to comply with this policy by a DWSD employee is a violation of DWSD’s Employee Standards of Conduct policy and may lead to revocation of system privileges and/or disciplinary action according to DWSD’s Disciplinary policies. Failure to comply with this policy by a contractor using DWSD technology resources may be considered grounds for breach of its contract and revocation of system privileges.

- 4.2. This policy applies to the use of information, electronic, and computing devices, and network resources to conduct DWSD business or interact with internal networks and business systems, whether owned or leased by DWSD, the employee, or a third party. In addition, this policy applies to all IT equipment that is owned or leased by DWSD.

## **5. RESPONSIBILITIES**

### **5.1. Information Technology Services**

- 5.1.1. The Chief Information Officer (CIO) is responsible for developing and updating the policy.
- 5.1.2. Information Technology Services has authority to disable any equipment or services that are in violation of this policy.

### **5.2. Management**

- 5.2.1. DWSD management is responsible for the actions of their staff, contractors, and volunteers and must ensure that all standards applicable to their environment are followed and alerting Human Resources when a violation has occurred.

### **5.3. Employees**

- 5.3.1. All DWSD computer and technology resource users are responsible for being familiar with and fully complying with this policy; knowing, understanding, and following all DWSD policies and ensuring that DWSD information is protected per IT policy requirements.
- 5.3.2. All DWSD computer and technology resource users are responsible for exercising due care when using DWSD electronic communication systems and the management, retention, disposal, and classification of their electronic communications consistent with adopted DWSD record retention policies.
- 5.3.3. All DWSD computer and technology resource users are expected to exercise good judgement and act in a professional manner when using DWSD technology resources.
- 5.3.4. Effective security is a team effort involving the participation and support of every DWSD employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

### **5.4. Human Resources**

- 5.4.1. Human Resources is responsible for any disciplinary action for employees that do not comply with this policy.

## **6. POLICY**

### **6.1. Public Internet**

- 6.1.1. Users are accountable for their actions when accessing the Public Internet using DWSD network and/or with DWSD computing resources.

- 6.1.2. Inappropriate use of the Public Internet, including excessive use of the internet, i.e. 'web-surfing', etc. for personal purposes is prohibited.
- 6.1.3. DWSD may, at its discretion, restrict or block access to Public Internet sites and/or services, prevent the downloading of certain file types, and manage connectivity. The ability to access a specific Public Internet website does not in itself imply that users of DWSD systems are permitted to visit that site.
- 6.1.4. DWSD does not automatically protect information sent via the Public Internet.
- 6.1.5. Use of a Public Internet service for other than its intended purpose is considered an abuse of the service and is subject to termination of the right to use the service.

## **6.2. Electronic Communications**

- 6.2.1. Personal accountability is mandated for user electronic communications accounts.
- 6.2.2. All DWSD electronic communications must be consistent with the DWSD's HR Confidentiality and Social Media Use policies.
- 6.2.3. Despite the best efforts of the DWSD, electronic communications systems may deliver unsolicited messages that contain offensive content. DWSD is not responsible for the content of material viewed, downloaded or received through the Internet.
- 6.2.4. The ITS Department cannot guarantee that public electronic communications systems are private with access limited to only the intended recipient(s).
- 6.2.5. "All user" email broadcasts or mass electronic communications are not permitted except by the Public Affairs Division, IT Service Desk, or with the permission of the DWSD Director.
- 6.2.6. Vendors wishing to communicate electronically with DWSD must use their own electronic communications systems.
- 6.2.7. All use of electronic communications must be consistent with DWSD policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
- 6.2.8. Electronic communications should be used primarily for DWSD business related purposes; personal communication is permitted on a limited basis, but non-DWSD related commercial uses are prohibited. All information on DWSD phones and DWSD information stored on personal phones are subject to the Freedom of Information Act.
- 6.2.9. DWSD will not be liable for the loss of personal cellphones brought into the workplace.

## **6.3. Privacy and Legal Rights**

- 6.3.1. Employees (and other authorized personnel) do not and should not have any expectation of privacy in their use of DWSD-provided technology resources or the contents of any electronic communication or file, both business and personal, sent through or stored on DWSD technology resources.
- 6.3.2. The DWSD reserves the right to remove unauthorized software found on any DWSD technology resource, with or without notice.

- 6.3.3. The DWSD reserves the right to remove from its information systems any material it views as offensive or potentially illegal.
- 6.3.4. Information created in the course of business is DWSD's property.
- 6.3.5. DWSD technology resources must be protected in a manner commensurate with their sensitivity, value, and critically or as required by law, contract, or operating agreement.

#### **6.4. Prohibited Behavior**

- 6.4.1. Loading, installing, or storing non-DWSD-provided software or applications on DWSD technology resources without express permission and/or authorization from ITS is strictly prohibited. Such software includes but is not limited to, remote control software, unapproved instant messaging software (such as AIM, Google Talk, MSN, Yahoo Messenger, etc.), peer-to-peer file sharing software (such as Bittorrent, Limewire, etc.), shareware, open source software, public-domain software, and freeware.
- 6.4.2. Using or accessing DWSD resources that are not intended for the performance of their jobs is strictly prohibited. Access to a DWSD technology resource does not imply permission to use the resource. For example, access to software installation packages on network drives does not imply that these can be installed. Software may require licenses and may not be installed without the purchase of those licenses.
- 6.4.3. Examining, altering, copying, or deleting the files or directories of other users without owner permission or the appropriate authority is strictly prohibited.
- 6.4.4. Knowingly entering false or inaccurate information into any DWSD technology system is strictly prohibited.
- 6.4.5. Misuse of system access privileges is strictly prohibited. Such misuse could include preventing legitimate authorized users access to DWSD resources, or obtaining extra resources or access privileges without proper authorization.
- 6.4.6. Unauthorized copying or distribution of system configuration files is strictly prohibited.
- 6.4.7. Any other use that is illegal, violates DWSD policy, or that could embarrass, offend, or harm the DWSD, its employees, or its customers is strictly prohibited.
- 6.4.8. Accessing, creating, reproducing, displaying, distributing, or storing any materials that are sexually explicit, obscene, defamatory, harassing, illegal, or otherwise inappropriate is strictly prohibited. In addition, any users who discover they have connected with a website that contains sexually explicit, racist, sexist, violent, or other potentially offensive material must immediately disconnect from the site.
  - 6.4.8.1. An exception is made for Law Enforcement, Security Staff, Information Technology Staff, General Counsel, and Human Resources personnel only when handling this type of material is required in the course of their official DWSD duties.
- 6.4.9. Misrepresenting, obscuring, suppressing, or replacing another user's identity on an electronic communications systems and Public Internet is prohibited. The user

name, electronic communications address, organizational affiliation, and related information included with electronic communications and Public Internet must reflect the actual originator of the messages or postings.

## **6.5. Reasonable and Necessary Accommodations**

- 6.5.1. Management may take reasonable and necessary actions to accomplish the intent of this policy.

## **7. PROCEDURE**

### **7.1. Public Internet**

#### **7.1.1. Public Internet Connections**

- 7.1.1.1. All communications between a DWSD network and any non-DWSD network must use solutions approved by ITS management and use network suppliers chosen by DWSD.
- 7.1.1.2. Departments are prohibited from procuring unapproved dedicated connections to the Public Internet without the documented approval of ITS management.
- 7.1.1.3. All communications between DWSD-provided equipment on DWSD premises and any other non-DWSD network, such as Public Internet, must use solutions approved by ITS management, which are secured with appropriate administrative and technical controls.
- 7.1.1.4. Privileged and confidential DWSD information must be only be revealed on the Internet if the information has been officially approved for public release per DWSD's Communications Guidelines.
- 7.1.1.5. Protection mechanisms such as secure Internet connections (<https://>) or other DWSD-approved encryption techniques can be used to protect sensitive information. Contact ITS if assistance is needed to determine proper protection methods for sensitive information.

#### **7.1.2. Public Internet Services**

- 7.1.2.1. The use of any Public Internet (AKA "Cloud") service must be reviewed and approved by ITS management. The risk associated with the service must be identified and appropriate controls to minimize the risk must be defined and implemented. An ITS staff member must be included in the development of any business case and process.
- 7.1.2.2. Confidential personal information and information that can be used to gain access to goods, services, or computer resources must not be sent over the Public Internet in readable form. Proper encryption must be used.
  - 7.1.2.2.1. DWSD email is not encrypted, therefore confidential information must not be sent via email.

#### **7.1.3. Acceptable Use**

- 7.1.3.1. News feeds, email lists, RSS feeds, and other mechanisms for receiving information over the Internet must be restricted to material that is clearly

related to both DWSD business and the duties of the receiving user. Users are reminded that the use of DWSD technology resources must never create the appearance or the reality of inappropriate use.

## **7.2. Electronic Communications**

### **7.2.1. Electronic Communications Content**

- 7.2.1.1. Offensive material must not be forwarded or redistributed to either internal or external parties, unless this forwarding or redistribution is in connection with your official DWSD-assigned work duties or is being sent to the Human Resources Department or DWSD Office of General Counsel in order to assist with the investigation of a complaint.
- 7.2.1.2. Electronic communications content should not be altered and then forwarded without the permission of the originating sender. If content is altered to remove sensitive information, it must be clearly indicated in the new message. Altering the content to change the intention of the originator is strictly prohibited.

### **7.2.2. Electronic Communications Management**

- 7.2.2.1. Electronic communications inboxes are not intended to be repositories for official DWSD records or other important business-related correspondence. Email must not be treated as a record management system. Users must regularly move these correspondences to word processing documents, databases, or other electronic file storage areas located on the DWSD Network that are intended for storing official documents in accordance with DWSD Records Management policy.

### **7.2.3. Electronic Communications Forwarding**

- 7.2.3.1. Automatically forwarding electronic communications from a DWSD electronic communications account to a public electronic communications system is prohibited without written permission from the ITS department since the contents of the electronic communications, including attachments, can be forwarded, intercepted, printed, and stored by unauthorized parties.

### **7.2.4. Delegate Authority**

- 7.2.4.1. Electronic communications must not be read or sent from another user's account, except under proper delegate arrangements.

### **7.2.5. Phishing (Fraudulent) Messages**

- 7.2.5.1. Users must immediately delete "phishing" (fraudulent) electronic communications messages that ask for sensitive information. If assistance is needed to determine an electronic communication's legitimacy, contact the Service Desk.
- 7.2.5.2. User must not click links or download any attachments within phishing (fraudulent) electronic communications messages.

#### **7.2.6. Third Parties**

- 7.2.6.1. Contractors operating in direct support of DWSD business operations may use DWSD electronic communications systems. In these cases, requests for use of DWSD electronic communications systems and deviations from prescribed functionality must be reviewed and approved by the ITS department management with recommendation from their contract administrator.

#### **7.2.7. Acceptable Use**

- 7.2.7.1. Personal non-DWSD electronic communications accounts must not be used for the generation of DWSD records.
- 7.2.7.2. Personal devices must not be used to conduct DWSD business or to transmit DWSD information.
- 7.2.7.3. The personal use of DWSD electronic communications systems and non-DWSD public electronic communications systems (such as Gmail, Yahoo, Live, Hotmail, etc.) is permitted as long as it is approved by the ITS and complies with all provisions of this policy.
- 7.2.7.4. Without prior written authorization from the Director and/or General Counsel, DWSD electronic communication systems must not be used for charitable fund raising campaigns.
- 7.2.7.5. Electronic communications shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails or social media communication with this content from any DWSD employee should report the matter to their supervisor immediately.
- 7.2.7.6. DWSD electronic communications and technology resources or similar assets may not be used for political advocacy efforts, religious efforts, private business activities, distributing chain mail, propagating hoaxes, or other purpose that could cause embarrassment to the DWSD or otherwise adversely affect its interests or violate federal or state laws.
- 7.2.7.7. With the exception of DWSD-sanctioned electronic communications systems (IT system maintenance notices, list servers, etc.) that are intended to be anonymous electronic communications is strictly prohibited. Additionally, the use of anonymous proxies or other anonymous facilities are not permitted.

#### **7.3. Encryption**

- 7.3.1. Whenever encryption is implemented, DWSD-approved encryption methods must be used. The use of all other encryption methods is not permitted.
- 7.3.2. In circumstances where application of an established control cannot be followed, compensating controls, authorized and approved by ITS management, must be applied to mitigate the risk. Sound business judgment must govern this process.

#### **7.4. Privacy and Legal Rights**

- 7.4.1. DWSD reserves the right to conduct random audits of its technology resources to identify non-compliance with policies and to monitor or access files, Public Internet

usage history, and the contents of electronic communications including but not limited to: email, instant messaging (IM), and text messaging sent through or stored on DWSD technology resources. Files stored on DWSD-provided technology resources, web browser history (cache files, web browser bookmarks, logs of web sites visited, etc.) computer system configurations, and other information stored on or passing through DWSD systems.

- 7.4.2. Actions that expose DWSD information to capture, modification, and disclosure are grounds for disciplinary actions.
- 7.4.3. Technical support personnel are prohibited from reviewing the content of an individual user's electronic communications out of personal curiosity or at the request of individuals who have not gone through proper approval channels. Written approval from the General Counsel, Chief of Security and Integrity, Division Director, and/or the Human Resources Director is required prior to any monitoring or review of electronic communications.
- 7.4.4. Intellectual Property Rights, such as copyrights, patents, and trademarks must be respected. Users using DWSD electronic communications systems can repost or reproduce material only after obtaining permission from the source or quote material from other sources only if these other sources are properly identified.

#### **7.5. Ownership and Business Use**

- 7.5.1. All technology resources purchased by or licensed to the DWSD are the property of the DWSD.
- 7.5.2. DWSD technology resources and similar DWSD assets are provided for use by DWSD employees (or other personnel) for legitimate DWSD business purposes.
- 7.5.3. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of DWSD. These systems are to be used for business purposes in serving the interests of the company, and of DWSD clients and customers in the course of normal operations.

#### **7.6. Management of DWSD Information**

- 7.6.1. When a user is transferred or their employment is terminated, all information must be returned, transferred, or reassigned to another individual, User ID or area/group, to prevent the loss of DWSD information and ensure ongoing ownership and control. See User Account Management policy for further information.

#### **7.7. Intellectual Property Controls**

- 7.7.1. Reproducing, displaying, distributing, or storing any materials that violate the trademark, copyright, licensing, or other intellectual property rights of any party, including the DWSD, is strictly prohibited.
- 7.7.2. Theft or misuse of technology resources, including unauthorized software copying or distribution, is prohibited and must be reported to the CIO immediately.



## **7.8. Configuration Control**

- 7.8.1. Users must not change, modify, or delete any configuration files or settings that will prevent, stop or interfere with the delivery of official DWSD approved patches, updates, security controls, or system enhancements.
- 7.8.2. Updates and patches must be certified and tested for compatibility with the standard DWSD computer operating system image prior to installation and must be obtained from official DWSD sources. Users are not permitted to download or obtain these from non-DWSD resources.
- 7.8.3. All hardware upgrades to DWSD supplied technology resources must be performed by the ITS Service Desk or authorized DWSD personnel.
- 7.8.4. A DWSD configured computer operating system image must be installed on DWSD supplied technology resources. Where the DWSD configured computer operating system image is not used, a clear business reason must be documented for using an alternate computer operating system image.
- 7.8.5. All proposed modifications to the DWSD configured computer operating system image must be reviewed and approved by ITS management prior to distribution or deployment. This includes but is not limited to, the installation of network services and protocols not included in the DWSD configured computer operating system image.
- 7.8.6. Whenever possible, the DWSD configured computer operating system image with the latest security and encryption capability must be used to ensure the strongest security available.

## **7.9. Physical Security Controls**

- 7.9.1. While off DWSD premises or where there is high risk of theft, technology resources, such as PC's, laptops, mobile devices, digital media, etc., must be securely stored when left unattended.
- 7.9.2. User must notify the CIO and/or Director immediately if equipment is stolen, damaged, or missing. If an item is stolen, the user must complete a police report and provide the report to the CIO.
- 7.9.3. Equipment must not be relocated without Service Unit manager approval and ITS Service Desk notification.
- 7.9.4. Except for assigned portable technology resources, equipment must not leave DWSD premises without ITS authorization.
- 7.9.5. All computing devices must be secured with a password protected screensaver with the automatic activation feature set to 10 minutes or less. The screen must be locked or logged off the device when computing device is unattended.

## **7.10. Network Controls**

- 7.10.1. End-user computer systems must not be configured to function as servers without the express consent of ITS. Prohibited behavior includes, but is not limited to, running server services or applications such as file, web, and database servers.

7.10.2. Systems that automatically exchange data between devices, such as a Smartphone, tablet, or PDA and a personal computer, must not be enabled unless the systems have been evaluated and approved by ITS management.

7.10.3. Personal devices should only be connected to networks designed for public use.