


Policy Title:	Information Security Policy		
	INFORMATION TECHNOLOGY SERVICES (ITS)	Category	Information Security
		Administrative Policy #	
		Revision #	
		Review Frequency	As Needed – no less frequently than triennially
Administrative Division	Information Technology Services (ITS)	Reviewed By	
BOWC Approval		Last Reviewed/Update Date	
Implementation Date			

1. OBJECTIVES

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

2. PURPOSE

- 2.1. To establish guidelines and responsibilities for information security, to maintain the confidentiality, integrity, and availability of DWSD information and systems.

3. DEFINITIONS

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

“DWSD” or “Department” means the Detroit Water and Sewer Department.

“Direct Supervisor or Direct Supervision” means the DWSD employee who exercises immediate supervisory authority over another employee’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, students, volunteers, and other persons authorized to use DWSD’s computer and technology resources.

5. RESPONSIBILITIES

5.1. Chief Information Officer (CIO)

- 5.1.1. The Chief Information Officer (CIO) is responsible for publishing this policy; communicating this policy to all employees; for review, approval and publishing of divisional standards; and for updating this policy as necessary.
- 5.1.2. The CIO, or delegate, is responsible for interpreting and enforcing this policy; ensuring that information resource usage is in compliance with Departmental policies and standards.

5.2. Information Technology Services

- 5.2.1. Supporting the need for appropriate security controls within the IT environment, supporting DWSD information security awareness and education program efforts.

- 5.2.2. Providing direction and support for the continual development, implementation, and maintenance of DWSD-wide information security policies, programs, and procedures.
- 5.2.3. Providing information as necessary to DWSD about existing and emerging legal and compliance requirements and about best practices associated with information systems security as well as reviewing exceptions to this policy to ensure their appropriateness and legality.
- 5.2.4. Acting as an advocate for budget and resource requests related to ensuring the maintenance of effective information security programs.

5.3. Management

- 5.3.1. Management is responsible for monitoring work areas for compliance and addressing any incident(s) of noncompliance and alerting Human Resources when a violation has occurred.

5.4. Employees

- 5.4.1. The employee is responsible for being familiar with and fully complying with this policy, including protecting their accounts and privileges.
- 5.4.2. Accepting personal accountability for all activities associated with the use of their user accounts and related access privileges.
- 5.4.3. Ensuring that their use of DWSD computers, electronic communications, networks, and Internet access is restricted to authorized purposes and defined use limitations.
- 5.4.4. Maintaining the confidentiality of sensitive information to which they are given access privileges.
- 5.4.5. Reporting all suspected security and/or policy violations to the appropriate authority (e.g. Group Officer, Division Director or Department Manager, and/or ITS through the Service Desk).

6. POLICY

- 6.1. The Director will form and designate individuals to serve on an Information Technology Leadership Board (ITLB).
- 6.2. The ITLB will develop an Information Security Program that adheres to best practices established by the Information Systems Audit and Control Association (ISACA) and other relevant best practice guidelines.
- 6.3. It is the policy of DWSD to protect DWSD information in accordance with all applicable laws, governmental regulations and accepted best practices to minimize information security risk and ensuring information is available only to authorized individuals.
- 6.4. The information security objectives of DWSD are critical to the success of DWSD's governance and service missions. The success of the information security program depends on strong support from all users throughout DWSD. Everyone is responsible for security.

- 6.5. Failure to comply with this policy by a DWSD employee is a violation of the DWSD's employee standards of conduct and may lead to revocation of system privileges and/or disciplinary action according to the DWSD's discipline policy.
- 6.6. 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.

7. PROCEDURE

7.1. Information Security Program Oversight.

- 7.1.1. To achieve the information security goals of DWSD, the Information Technology Leadership Board (ITLB) develops and maintains the DWSD Information Security Program and requires all Divisions and Departments to comply. The Information Security Program will consist of the Information Security practices and protocols and, at minimum, annual Information Security Awareness Training for all DWSD employees.

7.2. Access Controls (These controls protect data from unauthorized disclosure, modification or loss.)

7.2.1. Data Access

- 7.2.1.1. Data access should be controlled to sufficiently restrict access to authorized users.
- 7.2.1.2. Access to information must be on a need to know basis, restricted to authorized users with a business need to access the information.

7.2.2. User Access

- 7.2.2.1. Access to the network, systems, and applications should be controlled with individual and unique user IDs, and require authentication.
 - 7.2.2.1.1. Users are responsible for all actions taken with their personal user accounts (user IDs).
- 7.2.2.2. Users must not share user accounts or passwords, and passwords must not be written down or stored/transmitted in electronic files or communications, unless originating from authorized ITS personnel and delivered through an encrypted email.
- 7.2.2.3. Passwords must be in accordance with the DWSD Password Policy.
- 7.2.2.4. Granting of access requires approval of supervisor/manager and will follow the rule of least privilege, granting only as much access as needed to complete ones job duties.
- 7.2.2.5. Refer to User Account Management Policy for procedures related to granting, modifying, and terminating access to the network and business applications.

7.3. Network Controls

- 7.3.1. To protect the security and integrity of DWSD networks, users are not permitted to connect non-DWSD owned technology resources to private, internal DWSD networks without permission from ITS. Such equipment includes but is not limited

to personal PCs, laptops, printers, mobile devices (phones, tablets, handhelds, etc.), and networking equipment (wireless access points, routers, switches, etc.). Note: The term “connect” is intended to include both wired and wireless connections.

- 7.3.2. All access to or from DWSD networks must be via ITS management-approved telecommunication solutions. The use of modems and the private installation of data or voice lines, either fixed or wireless, is prohibited without explicit authorization from ITS.
- 7.3.3. All inbound connections to DWSD’s internal networks, including process control and security networks require a DWSD ITS approved virtual private network (VPN) software package.
- 7.3.4. The presence of any active secondary network connection on a computer that is attached to DWSD’s network is not permitted.

7.4. Security Incidents

- 7.4.1. Users must immediately report security incidents, such as their computer becoming infected with a virus, to the Service Desk.
- 7.4.2. If any user of DWSD’s technology resources believes for any reason that their credentials (User ID and password, token, etc.) have been compromised or misused, they must immediately shut down the involved computer, disconnect from all networks, and report the event to the Chief Information Officer.
- 7.4.3. ITS is the only division authorized to broadcast information about computer security alerts and determine the appropriate action in response to such notices. Users must not propagate or forward any virus notification messages except to ITS for examination.

7.5. Virus and Malware Prevention

- 7.5.1. Virus detection software, provided by ITS, must be installed, functional and updated on PCs, laptops, and similar devices.
- 7.5.2. Users must not click on links or download any attachments contained within electronic communications from unknown sources. If assistance is needed to determine an electronic communication’s legitimacy, contact the Service Desk.
- 7.5.3. Refer to the DWSD Virus and Malware Prevention and Detection Policy for more information.

7.6. Safeguarding of Information

- 7.6.1. DWSD information, both hard copy and electronic files, must be managed and protected.
- 7.6.2. Customer and employee information must not be shared with unauthorized individuals.
- 7.6.3. Information must be protected with due care and due diligence regardless of the computing platform. It must be protected in a similar manner to the information that is stored on DWSD servers, and only accessible to authorized individuals.

- 7.6.4. Encryption requirements must be followed for information stored on end-user technology resources, digital storage media (such as memory cards, USB based storage devices etc.), or online providers.
- 7.6.5. Other than public use, kiosk, and related computers, all DWSD workstations will be set to automatically lock after a predefined period of inactivity requiring that the user enter their password to unlock the system.
- 7.6.6. Privileged and confidential DWSD information may only be revealed on the Internet if the information has been officially approved for public release per the DWSD General Counsel.
- 7.6.7. Technology Disposal – Technology resources (computers, copiers, mobile devices, etc.) or digital storage media removed from service or removed from the DWSD technology environment (end of lease, sale, recycling, disposal, etc.) must be securely disposed of through ITS only. Refer to the IT Asset Management Policy for additional information.