1 IT Security Standards

1.1 Preface

1.1.1 INTRODUCTION

A. The IT Security Standards (ITSS) document is written to communicate Silver Lake Water & Sewer District's (SLWSD) requirements for information technology (IT) security at District facilities.

B. The ITSS is written for an audience of Employees, Vendors, Consultants and Service Providers who use SLWSD's IT systems, provide services affecting SLWSD's IT systems or handle the District's data.

C. This document (especially sections 2 and 3) is considered confidential and disclosure of some of the information described herein would be injurious to the District.

D. This is a "living document" that will evolve regularly as needs and circumstances change.

E. It is the responsibility of recipients of this document to protect the content from distribution to unauthorized persons and to comply with the policies and practices it describes.

F. The federal computer fraud and abuse statute, 18 USC § 1030[1], outlaws conduct that victimizes computer systems. It is a cyber-security law. It protects federal computers, bank computers, and computers connected to the Internet. It shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud.

G. Employees who are aware of violations of this policy must report them to a supervisor.

1.1.2 GOALS FOR CONTROLS

There are three primary goals or objectives for establishing IT Security Controls:

1. Preventative – policies, procedures, best practices
2. Detective – audits, intrusion detection systems, physical inventories
3. Corrective – malware removal, restoring backups

[1] http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t17t20+613+5++%28%29%20%20AN

1.1.3 CLASSES OF CONTROLS

There are three primary classes of action or device associated with IT Security Controls:

1. Management/Administrative – focused on management of risk, security, policies/procedures, plans, assessments
2. Operational/Physical – awareness training, change management, contingency planning, and physical security practices
3. Technical – Identification, authentication, access controls,

1.2 Resolutions and Standards

A. The ITSS was adopted under Resolution No. 682 by the SLWSD Board of Commissioners on April 12, 2012. It therefore represents the fully-authorized policy of the District regarding IT Security.

B. Other previously adopted resolutions addressing IT Security topics include Resolutions No. 634 Approving and Adopting an Identity Theft Prevention Program and No. 648 Providing for a Policy to Regulate Use of the District's Information Technology Systems and Services.

C. Due to the ever-evolving information technology industry, it is acknowledged that it is not realistic to foresee and fully address all possible conditions, circumstances and applications that may affect IT Security. Therefore, the ITSS is also expected to change over time to adapt to new opportunities and new threats presented by this industry.

D. ISO/IEC 27002 is an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled ***Information technology - Security techniques - Code of practice for information security management***. Where circumstances occur that are not adequately addressed by this document, SLWSD will refer to ISO/IEC 27002 as it now reads or is hereafter updated or changed for guidance until the ITSS has been updated to address the concern.

1.3 Document Structure

The ITSS is organized in the following sections:

1. IT Security Standards
2. IT Systems and Operations
3. Key IT Parameters

A. **IT SECURITY STANDARDS** (this section) describes this document, its intent and its relationship to industry standards, practices and the various audiences affected by the document. It also describes policies and best practices to be followed by Employees, Vendors, Consultants and Service Providers who use

SLWSD's IT systems, provide services affecting SLWSD's IT systems or handle the District's data.

B. The **IT SYSTEMS AND OPERATIONS** section defines and discusses the functions, operations, practices and procedures involved in designing, configuring, operating and maintaining secure information technology systems at SLWSD. This portion of the document is only provided to those with a genuine need for this information pursuant to the interests of the District, but is otherwise exempt from public inspection and copying pursuant to the provisions of RCW 42.56.420 and 5 USC 552b(c)(3) and Section 1433(a)(3) of the Safe Drinking Water Act (Title XIV of the Public Health Services Act).

C. The **KEY IT PARAMETERS** section discusses the most sensitive configuration parameters of the information technology parameters in use at SLWSD. This portion of the document is only provided to the following individuals:

- General Manager
- System Administrator
- Designee of General Manager by written communication

This section is otherwise exempt from public inspection and copying pursuant to the provisions of RCW 42.56.420 and 5 USC 552b(c)(3) and Section 1433(a)(3) of the Safe Drinking Water Act (Title XIV of the Public Health Services Act).

1.4 Definitions

1.4.1 DEFINITION OF IT SECURITY

A. IT security is defined as the prevention of loss of Availability, Confidentiality and Integrity of data, systems or services. Pursuant to these objectives, SLWSD has done the following:

- Established robust facilities designed to withstand disaster and malice
- Deployed redundant systems and services
- Implemented policies and practices to meet performance expectations

1.4.2 DEFINITION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

A. Full name
B. Address
C. Account Number (either SLWSD or bank)
D. Social Security Number
E. Driver's License Number
F. Birthdate
G. Other items not used at SLWSD include: Genetic Information, Biometric Information and Birthplace.

1.4.3 DATA CONFIDENTIALITY CLASSIFICATIONS

All data shall be classified in one of the following four categories of confidentiality:

A. **Public**: This data is either publicly available or it would not pose any risk if it were publicly available. If disclosed, it would not have any negative impact on the District, its employees, customers, or business partners.

B. **Sensitive**: This data shall not be made publicly available as its disclosure could have some sort of negative impact on the District, its employees, customers, or business partners.

- Sensitive data shall be stored in designated locations that only allow access to authorized personnel.
- Sensitive data shall use the SSL/TLS encryption protocol during transmission.

C. **Private**: This data is intended for internal use only and could include such information as employee records and customer data. PII would also be considered private data. If disclosed, private data is likely to have a negative impact on the District, its employees, customers, or business partners.

- Private data shall be stored in designated locations that only allow access to authorized personnel.
- Private data shall use the American Encryption Standard (AES) while stored.
- Private data shall use the SSL/TLS encryption protocol during transmission.

D. **Confidential**: This data is to be guarded with the utmost diligence. Disclosure of this information is likely to have a significant negative impact on the mission of the District as well as potentially the safety of its employees, customers, or business partners. The Key IT Parameters are included in this classification.

- Confidential data shall be stored in designated locations that only allow access to authorized personnel.
- Confidential data shall use the American Encryption Standard (AES) while stored.
- Confidential data shall use the SSL/TLS encryption protocol during transmission.

District management, assisted by supervisors with stewardship for each set of data, shall designate the confidentiality of each data set.

Access to each set of data shall be determined by the General Manager using a Role-Based Access Control Model. Access shall be controlled through the use of permissions and passwords. Reproduction and transfer of classified data shall be made only at the discretion of an employee's supervisor. Upon reproduction or transfer of classified data, the data shall retain its original classification and be appropriately labeled with that designation.

1.5 Acceptable Use Policy

1.5.1 ACCESS PRIVILEGES

A. Supervisors shall determine which data sets an employee will be authorized to access and their degree of access, and shall communicate this to the system administrator. The system administrator shall assign permissions to the user in the directory to implement the supervisor's instructions.

1.5.2 IMPERSONATION

A. Do not attempt to use another person's credentials, including network username, keycard, etc.

B. Do not attempt to use computer that is logged-in under another person's credentials.

C. Do not attempt to access or review information or data to which you have not been authorized. This includes printed materials.

1.5.3 PERSONAL COMMUNICATION DEVICES

A. Never connect a personally-owned communication device (computer, tablet, smartphone, etc.) to the District office network or SCADA network. As a courtesy, the District has made available a separate wireless network for use with non-District communication devices. Please contact the system administrator for credentials to access this resource.

1.5.4 PRIVACY

A. The District does not take any measures to protect the privacy of anyone who uses District IT resources, except where legally required. SLWSD personnel shall not expect any level of personal privacy while using District IT resources, except where legally required.

1.5.5 LOGGING

A. SLWSD does not log every action on its networks, however its network systems are capable of logging any network activity of interest. This includes any file changes, email messages, logins, and attempts to access systems or data.

1.5.6 WORKING WITH SENSITIVE INFORMATION

A. In the course of conducting District business, some employees will know and use account numbers and other sensitive information. Sometimes it will be necessary to interact with Internet-based resources and websites for these functions.

- These actions should only be done using computers that are physically wired to the District network at the District headquarters.
- Never use a wireless device to access sensitive information.
- Never use a mobile device to access sensitive information.
- Never use a personal device to conduct District business.

1.5.7 REMOTE ACCESS

A. Remote access to District network resources shall only be made by personnel who have been authorized to do so by management. Remote access shall only be made using District-approved devices. All remote access shall be made via an encrypted virtual private network connection.

B. Remote access to District resources are subject to the same expectations and restrictions as any other use of District resources.

1.6 Best Practices

1.6.1 PASSWORD POLICY

A. Passwords shall be changed at least once every 90 days. Do not reuse previous passwords.

B. Passwords shall be a minimum of 8 characters long (longer is better) and be comprised of a combination of:

- lowercase letters
- UPPERCASE letters
- numbers
- symbols, such as !@#$%^&*()_+-=`~'":;<,>.?/|\

C. Be aware of the following when creating a new password:

- Do not use any word found in the dictionary as part of the password, including foreign languages, texting abbreviations, slang and foul language. These words are all commonly checked by password cracking software.
- Do not use any piece of information about yourself that is known by other people, including birthdate, address, names of pets or family members, sports teams or any other information that could be discovered through social interaction (either in person or online).
- Do not use a string of consecutive keys on the keyboard, such as "qwerty" or "asdfjkl;"
- Do not use part of your name within the password.

D. Here is a suggestion for creating passwords that are difficult for code breaking software to discover:

- Think of a long phrase such as a poem, song or quote.
  - For example: "Oh, say can you see by the dawn's early light"
- Use the first letter of each word in the phrase
  - For example: oscusbtdel

- Capitalize one or more of the letters
  - For example: Oscusbtdel
- Substitute a number or symbol for a word or letter
  - For example: O5cu5btdel
- Insert symbols
  - For example: O,5cu5btd’el

The resulting password **O,5cu5btd’el** is very difficult to break.

E. Each person shall be responsible to protect their password.
- Passwords shall not be shared with any other person for any reason.
- Do not write down your password.
- Do not use your password on any device that is not District property.

F. If a system administrator assigns a new password to a user, the user will be required to change the password at the next login.

G. Password audits may be conducted periodically to ensure compliance with this policy.

1.6.2 AVOIDING VIRUS/MALWARE INFECTION

A. Email
- Don't open unsolicited email messages.
- Never open attachments in emails that you were not expecting. Even emails from people you know could be dangerous because they might have been infected and the virus could be propagating by emailing itself to everyone in their email contact list.
- Never click on a link within an email. Instead, retype the target link in the address bar of the web browser.
- If you are ever in doubt about the legitimacy of an email or its attachment, please ask for assistance from the System Administrator.

B. Downloading
- Do not download any non-work related files, documents, songs, pictures, etc. from the Internet.
- Do not attempt to install applications without assistance from the System Administrator.

C. USB/Thumb-drive/CDROM
- Be aware that USB/thumb-drives and CDROMs are a potential avenue for viruses and malware to enter the network. If the drives were used on or CDROMs created on a computer that is infected, they could be carriers of the infection. Always scan media from outside the District using the antivirus software.

1.6.3 FILE MANAGEMENT

A. Duplication – storing multiple versions of documents in different locations causes many problems.

- It is wasteful with storage space
- It is difficult to know which version of the document is the current version
- It becomes difficult to know where to find the current document

B. Don't store documents on your workstation's local drives (for example C or D drive, MyDocuments, or USB/Thumb/Flash Drives). In the past, the District has permitted users to store documents in the "local_data" / MyDocuments folder where they have been backed-up. However, a process is underway to migrate from this practice and it will soon no longer be permitted.

C. Documents and data should be viewed as "belonging to a function or role" rather than "belonging to a person." Therefore, the documents and data should be stored on the network in a location that protects it from unintended manipulation and from unauthorized access, while making it available for reference by those who need the information without changing it.

D. Storing files in the correct locations ensures that they are only accessible by authorized individuals.

1.6.4 PROTECTION OF SENSITIVE INFORMATION

1.6.4.1 FILE LOSS

A. Designated network locations are backed up. If a file is corrupted or inadvertently deleted, it can usually be restored if the problem is discovered in a timely manner.

B. Normally, everything on the N Drive is backed up nightly as are the HMS and GIS applications.

1.6.4.2 DIVULGING PERSONALLY IDENTIFIABLE INFORMATION (PII)

1.6.4.2.1 TO UNAUTHORIZED 3RD PARTIES

A. Never email PII
B. Positive identification before discussing PII
C. Potentially legal implications

1.6.4.2.2 IDENTITY FRAUD

A. The federal fraud statute 18 USC § 1028 discusses the legal implications of identity fraud and related activity in connection with identification documents, authentication features, and information.

B. In addition to the federal statute, the District has adopted Resolution No. 634 Approving and Adopting an Identity Theft Prevention Program that also addresses this issue.

1.6.4.3 PERMANENT DISPOSAL OF STORAGE MEDIA

A. When a computer is re-purposed the storage media (hard drive and non-volatile RAM) on the computer shall be sanitized before reuse. Sanitization shall be performed using a utility capable of completely wiping all disk space clean, including free space.

B. When a computer is removed from service, the storage media (hard drive and non-volatile RAM) on the computer shall be physically destroyed.

C. When removable storage media (CDROMs, USB drives, external hard drives, etc.) containing District information is no longer used, the storage media shall be physically destroyed.