Resolution #2021-10-19

Adoption of Information Security Policy

WHEREAS, West Multnomah Soil & Water District ("District") desires to respond to an increasingly sophisticated cyber threat environment, and

WHEREAS, the District has reviewed its practices related to information security and updated them as necessary;

WHEREAS, the District is committed to following best practices for its Board of Directors as recommended by the Special Districts Association of Oregon (SDAO) through SDAO's Special District Insurance Services (SDIS) Best Practices Program;

WHEREAS, adopting an Information Security Policy is a requirement of the SDIS Best Practices Program;

NOW, THEREFORE, BE IT RESOLVED that the District adopts the Information Security Policy in **Exhibit A**, which is attached to this Resolution and incorporated herein by reference.

APPROVED AND ADOPTED BY THE BOARD OF DIRECTORS THIS 19th DAY OF OCTOBER, 2021.

_____

Terri Preeg Riggsby, Board Chair

_____

Date

ATTEST:

_____

Shawn Looney, Board Secretary

_____

Date

EXHIBIT A

West Multnomah Soil & Water Conservation District Information Security Policy

Introduction

This Information Security Policy ensures appropriate measures are in place to protect customer, client, landowner, and employee personal and sensitive information that is held or used by WMSWCD. All such information will be protected and the risk of internal and external threats minimized.

Administrative Access

Access to WMSWCD's systems and applications above and beyond general user access shall be limited to WMSWCD's contracted information services provider (CogentIT) and WMSWCD management as necessary.

Data Backup & Recovery*

WMSWCD will conduct regular backups of all critical business data. Incremental backups are performed daily and a full back up weekly which is rotated offsite. An annual archive backup is created at the end of each year and stored offsite. Confirmation that backups were performed successfully and testing of cloud backups and restoration capability will be performed as needed to ensure that the restoration process works.

Endpoint Protection*

All WMSWCD servers and workstations will utilize endpoint protection tools (i.e., antivirus, URL filtering to restrict traffic to trusted websites, restricted network access, etc.) to protect systems against malware and viruses.

Firewall with Security Services*

WMSWCD will protect the network from the Internet through the use of a properly configured firewall utilizing appropriate industry best-practices.

Email Security

WMSWCD will protect their email system by utilizing antivirus, antispam and anti-phishing technologies.* WMSWCD will never use email to send or receive sensitive information. Sensitive information includes social security numbers, driver's license numbers, bank account numbers, credit or debit card numbers, and protected health information.

Multi-factor Authentication*

Multi-factor authentication will be utilized on all systems or services that are external to the organization, including services and systems accessed by personal computers and devices used for remote work. This includes email, VPN, and any software that contains confidential or senstive information.

Wireless*

WMSWCD's wireless network will be setup utilizing two separate service set identifiers (SSIDs or internet wireless names and access passwords): one corporate SSID for employees and another guest SSID for personal/ guest devices. The password for the corporate SSID will not be shared with guests or used on personal devices.

Password Management*

WMSWCD will utilize the following password configuration to login to accounts that can access server resources (active directory and VPN access):

- Invalid login attempts before lockout: 5
- Lockout period: 30 Minutes
- Minimum password length: 12
- Maximum password age: 180 days
- Password history: 7
- Password complexity: On

In addition, WMSWCD will educate users on creating/ utilizing secure passwords for systems/ services that can't be controlled by WMSWCD.

Email Phishing Exercises*
WMSWCD will perform simulated phishing exercises to test and educate users.

Security Awareness Training*
WMSWCD personnel are required to participate in security training in the following instances:

1. All new hires are required as part of their onboarding process to read an annually updated "Most Important Security Issues" document before being granted system access.
2. A formal refresher training will be conducted on an annual basis by CogentIT. All employees are required to participate in and complete this training.

Acceptable Use Policy
WMSWCD will require all users to read and sign an Acceptable Use Policy before accessing organizational resources. This policy governs the use of the WMSWCD resources and covers a wide range of issues surrounding the rights, responsibilities, and privileges – as well as sanctions – connected with computer use. See *Appendix A* for a copy of current Acceptable Use Policy, which will be incorporated into the Employee Handbook by reference beginning in 2022.

Asset Management
Access to server room and IT equipment storage area will be secured by a locked door. An inventory of all WMSWCD's hardware and software will be maintained and will document the following:

- Employee in possession of the hardware or software
- Location of hardware or software
- Date of purchase
- Serial number
- Type of device and description

Patch Management*
All software and operating system updates and patches will be configured, when possible, to automatically install. Periodic review will be conducted to ensure all updates and patches are applied to all devices.

Standard Configuration*
WMSWCD will utilize a standard configuration (network settings and controls) for all WMSWCD's endpoints, servers, network devices, and printers. Any changes to the standard configurations will be reviewed and approved by WMSWCD management.

Vulnerability Scanning*
WMSWCD will ensure all critical external and internal resources have annual vulnerability scans conducted on them to ensure they are properly configured and updated.

Incident Response
WMSWCD will, as part of its Business Continuity Plan, utilize an incident response plan in the event of a cyber-related incident. This plan will include at a minimum:

- Essential contact information for CogentIT, Special District Insurance Services, FBI, and local law enforcement.
- User's roles and responsibilities.
- Schedule of regular testing of the incident response plan.*

Auditing and Logging*

WMSWCD will ensure proper logging is enabled on all critical resources. At a minimum the following events will be recorded:

- Invalid Login Attempts
- Creation of New User Accounts
- Escalation of User Privileges

Employee Compliance

Non-compliance with this policy may pose a risk to WMSWCD; accordingly, compliance with this program is mandatory. Failure to comply may result in disciplinary action up to and including termination of employment or business relationships. Management reserves the right to monitor, consistent with applicable laws, all activities within their business environment. WMSWCD will appropriately report violations of State and/or Federal laws and will cooperate with regulatory bodies and law enforcement agencies investigating such incidents.

*Note that items marked with an asterisk are led and coordinated by CogentIT, with WMSWCD management assisting as necessary with communication/messaging to WMSWCD staff.

Appendix A – Acceptable Use Policy

Purpose
This policy outlines the acceptable use of computer equipment, email, and internet access at WMSWCD. These rules are in place to protect the employee and WMSWCD. Inappropriate use exposes WMSWCD to risks, including virus attacks, compromised network systems, and legal issues.

Scope
This policy applies to both permanent and temporary employees of WMSWCD and is a supplement to WMSWCD's Information Security Policy.

General Use
IDs/Passwords:
Access to WMSWCD's IT systems is controlled using User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals, and consequently, individuals are accountable for all actions on organization systems and services.
Password Requirements:

- Minimum password length: 12
- Must have a combination of letters, numbers, and special characters.
- If possible, utilize a password manager to create unique and much stronger passwords for each service or account.

Individuals must not:

- Allow anyone else to use their user ID/token and/or password on any organizational IT systems. Exceptions to this must be approved by leadership.
- Leave their password unprotected (for example writing it down).
- Leave their user accounts logged in at an unattended and unlocked computer.
- Perform any unauthorized changes to WMSWCD's IT systems or information.
- Attempt to access data that they are not authorized to use or access.
- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Connect any non- authorized device to WMSWCD's corporate network or IT systems.
- Insert unapproved media (i.e., CD, USB thumb drive, SD card that were not purchased through WMSWCD approved vendors) into corporate devices.
- Store organizational data on any non-authorized equipment.
- Give or transfer organizational data or software to any person or organization outside of WMSWCD without the authority of leadership.

Internet and Email Use
Use of the internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's performance, is not detrimental to WMSWCD in any way, is not in breach of any terms and condition of employment, and does not place the individual or WMSWCD in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.
Individuals must not:

- Disclose employee, client, or other proprietary information to which the employee has access.
- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.

- Access, download, send, or receive any data (including images) which WMSWCD considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libelous material.
- Use the internet or email for personal gains, to run their own personal business, or to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any unauthorized information on the Internet that relates to WMSWCD, or expresses any opinion about WMSWCD, unless specifically authorized to do so.
- Send unprotected sensitive or confidential information externally.
- Forward confidential organizational email to personal non-organizational email accounts (for example a personal Gmail account).
- Make official commitments through the internet or email on behalf of WMSWCD, unless authorized to do so.
- Download copyrighted material, such as music media (MP3) files, film, and video files (not an exhaustive list), without appropriate approval.
- In any way infringe any copyright, database rights, trademarks, or other intellectual property.
- Download any software from the internet without prior approval.
- Remove or disable anti-virus software.
- Use unauthorized services on the internet to store or transmit Personal Identifiable Information (defined as any data that could potentially be used to identify a particular person). This includes Dropbox, Google Drive, and personal email accounts.

Email

To avoid being a victim of malicious software or phishing attack remember:

- Never download or open attachments from unknown recipients.
- Hover over links to determine if the link is legitimate.
- If it's a specific account asking you to sign into an account don't click a link within the email; visit the site directly to login.
- Verify sender. Sometimes the best way to do this is to call the sender back to confirm they are the person who initiated the email.
- Never provide personal information. Legitimate companies will never ask you to provide personal information, including passwords, in an email.

Clean Desk and Clear Screen

In order to reduce the risk of unauthorized access or loss of information, WMSWCD enforces a clear desk and screen policy as follows:

- Maintain a "clean desk" or working area throughout the day and ensure there are no confidential documents in open view when absent from desk for an extended period. This will help to ensure that confidential information is not inadvertently disclosed.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Ensure that paper-based information is appropriately monitored and protected.
- Ensure that all confidential documents are properly locked-up at the end of each business day. Appropriate methods to secure documents include utilizing locking filing cabinets or desk drawers, etc.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Only equipment approved by WMSWCD may be used to download personal information locally to the device.

- Equipment and media taken off-site must not be left unattended in public places or left in sight in a car. Lock devices in the trunk out of sight while traveling.
- Laptops must be carried as hand luggage when traveling.
- When outside the office, computers must utilize WMSWCD's VPN before connecting to WMSWCD resources.

Mobile Devices

- Mobile devices such as smartphones and tablets may be used, but require approval.
- Mobile devices must be password protected.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations where network connectivity is unavailable or there is no other secure method of transferring data. Only authorized mobile storage devices with encryption enabled may be used when transferring sensitive or confidential data.

Telephone Equipment Conditions of Use

The use of organizational voice equipment is intended for business use. Personal use of voice equipment is allowed but should be limited. Individuals must not:

- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from operators, unless it is for business use.

Actions upon Termination of Contract

All organizational equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to WMSWCD at termination of employment or contract.
All data or intellectual property developed or gained during the period of employment remains the property of WMSWCD and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering

All data that is created and stored on organizationally owned computers and third-party vendor's systems is the property of WMSWCD and there is no official provision for individual data privacy, however wherever possible WMSWCD will avoid opening personal emails.

System logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. WMSWCD has the right (under certain conditions) to monitor activity on its systems, including internet and email use, to ensure systems security and effective operation, and to protect against misuse.
It is your responsibility to report suspected breaches of security policy without delay to the CogentIT and WMSWCD management. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with WMSWCD's disciplinary procedures.

Signature

I have received a copy of WMSWCD's Acceptable Use Policy. I have read and understand the policy.

_____

(Print your name)

_____ _____

(Signature) (Date)