MAC Recreation District
1195 SE Kemper Way, Madras, OR 97741
541.475.4253 • www.macrecdistrict.com

Information Security & Acceptable Use Policy

Purpose

The purpose of this policy is to clearly communicate the MACRD's security objectives and guidelines to minimize the risk of internal and external threats. The MACRD seeks to ensure that appropriate measures are implemented to protect patron and employee personal and sensitive information. This policy is designed to establish a foundation for an organizational culture of security.

Compliance

Non-compliance with this policy may pose risk to the district; 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. The MACRD will appropriately report violations of State and/or Federal laws and will cooperate with regulatory bodies and law enforcement agencies investigating such incidents.

Privileged Access

Access to the organization's systems and applications above and beyond general user access shall be limited to the executive director and information technology support personnel.

Data Backup & Recovery

The MACRD will conduct regular backups of all critical business data. Full data backups will be performed on a daily basis. Confirmation that backups were performed successfully will be conducted daily. Testing of cloud backups and restoration capability will be performed on a quarterly basis by information technology support personnel.

Multi-factor Authentication

Multi-factor authentication will be utilizted on all systems or services used by the MACRD. This includes microsoft 365 and registration software programs.

Endpoint Protection

All MACRD servers and workstations will utilize an endpoint protection tool (anti-virus/anti-malware solution) to protect systems against malware and viruses.

Firewall with Security Services

MAC Recreation District
1195 SE Kemper Way, Madras, OR 97741
541.475.4253 • www.macrecdistrict.com

The MACRD will protect the corporate network from unauthorized access through the use of a firewall with Intrusion Prevention System (IPS) capability.

Email Security

The MACRD will protect the email system by utilizing antivirus, antispam and anti-phishing technologies. The organization will also not utilize email to send or receive sensitive information.

Wireless Internet

The MACRD's wireless internet will be setup utilizing two separate SSID's, including one for internal/MACRD staff devices and another for personal/guest devices. The password for the corporate SSID will not be shared with end-users, will only be known by authorized personnel, and will be changed periodically for security purposes.

Password Management

The MACRD will utilize the following password configuration:

- System account lockout threshold: 15 Minutes
- Invalid login attempts before lockout: 3
- Minimum password length: 12
- Maximum password age: 90 days
- Password history: 7
- Password complexity: On
- Must use multi-factor authentication.

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

Email Phishing Exercises

The MACRD will perform simulated phishing exercises used to test and educate users.

Security Awareness Training

MACRD staff are required to participate in security training in the following instances:

1. All new hires are required to complete security awareness training before being granted system access.
2. A formal refresher training is conducted on an annual basis. All employees who utilize district technology are required to participate in and complete this training.

MAC Recreation District
1195 SE Kemper Way, Madras, OR 97741
541.475.4253 • www.macrecdistrict.com

Acceptable Use Policy

The MACRD will require all users to sign an acceptable use policy before accessing organizational resources. This policy governs the use of the company resources and covers details surrounding the rights, responsibilities, and privileges – as well as sanctions – connected with computer use. See *Appendix A* for a copy of the current Acceptable Use Policy.

Asset Management

An inventory of all the organization's hardware and software will be maintained that documents 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
- Type of access approved for the machine.

Patch Management

All software and operating system updates and patches will be configured to automatically install. Periodic review will be conducted to ensure all updates and patches are applied to all devices.

Securing Remote Workers

The organization requires all remote users to utilize company owned devices when working remotely. Users may access their data through their OneDrive login. Users will be allowed access using MS 365 Identity Authentication, Authorization, and Machine Authorization.

MAC Recreation District
1195 SE Kemper Way, Madras, OR 97741
541.475.4253 • www.macrecdistrict.com

Standard Configuration

The organization will utilize a standard configuration for all endpoints, servers, network devices, mobile devices, and printers. Any changes to the standard configurations will be reviewed and approved by leadership (the Security Team). A list of all approved applications, services, and tools is maintained and reviewed regularly.

Vulnerability Scanning

The MACRD will ensure all critical external and internal resources have periodic vulnerability scans conducted on them to ensure they are properly configured and updated.

Incident Response

The MACRD will utilize an incident response plan in the event of cyber related incident. This plan will include at the minimum:

- Essential contact for an incident response service provider, FBI, local law enforcement, cyber insurance company, legal counsel.
- Users' roles and responsibilities.
- Schedule of regular testing of the incident response plan.

Auditing and Logging

The MACRD 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

MAC Recreation District
1195 SE Kemper Way, Madras, OR 97741
541.475.4253 • www.macrecdistrict.com

Appendix A – Acceptable Use Policy

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment, email, and internet access at the MACRD. These rules are in place to protect the employee and the district. Inappropriate use exposes the district to risks including virus attacks, compromises of network systems and services, and legal issues.

Scope

This policy applies to both permanent and temporary employees of the MACRD. This policy applies to all equipment that is owned or leased by the district. This policy is a supplement to the MACRD Information Security Policy.

General Use

IDs/Passwords:
Access to the organization's IT systems is controlled by the use of 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 district systems and services.

Password Requirements:

- Minimum password length: 12
- Must have a combination of uppercase and lowercase letters, numbers, and special characters.
- Must be changed every 90 days.
- You must utilize a password manager (LastPass is free) to create strong, unique passwords for each service or account.
- Cannot use the same password for multiple systems.
- Must use multi-factor authentication.

Individuals must NOT:

- Allow anyone else to use their user ID/token and/or password on any district IT systems.
    - Exceptions to this must be approved by the Security Officer.
- 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 the district's IT systems or information.
- Attempt to access data that they are not authorized to use or access.

MAC Recreation District
1195 SE Kemper Way, Madras, OR 97741
541.475.4253 • www.macrecdistrict.com

- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Connect any non-company authorized device to the organizations corporate network or IT systems.
- Insert unapproved media (CD, USB thumb drive, SD card) into corporate devices.
- Store organizational data on any non-authorized equipment, or personnel equipment.
- Give or transfer organizational data or software to any person or organization outside of the organization without the written approval of the Security Officer.

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 business performance, is not detrimental to the district in any way, not in breach of any term and condition of employment and does not place the individual or organization 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, and other proprietary information 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 the organization considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libelous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email 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 information on the Internet that relates to the district, alter any information about it, or express any opinion about the organization, unless they are specifically authorized to do this.
- Send unprotected sensitive or confidential information externally.
- Forward organizational mail to personal non-organizational email accounts (for example a personal Gmail account).

MAC Recreation District
1195 SE Kemper Way, Madras, OR 97741
541.475.4253 • www.macrecdistrict.com

- Make official commitments through the internet or email on behalf of the district 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 written approval from the Security Officer.
- Remove or disable anti-virus software.
- Use unauthorized services on the internet to store or transmit patron Personal Identification Information (PII). This includes (Dropbox, Google Drive, personal email accounts, etc.)

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. Example, your bank tells to click a link to change your password.
- Verify sender. Sometimes the best way to do this is call the sender back to make sure they are the ones who initiated the email.
- Never provide personal information. Legitimate companies will never ask for 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, the organization 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 if absent from their desk for an extended period of time. This will help to ensure that confidential patron 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.

MAC Recreation District
1195 SE Kemper Way, Madras, OR 97741
541.475.4253 • www.macrecdistrict.com

- 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 the district 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 and not left in sight in a car. Lock devices in the trunk out of sight while traveling.
- Laptops must be carried as carry-on luggage when traveling.

Mobile Devices

- Mobile devices such as smartphones and tablets may be used but require approval.
- It is not permitted to save patron information locally to a mobile device.
- District issued mobile devices must be password protected and encrypted.

Mobile Storage Devices

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

Telephone Equipment Conditions of Use

The use of MACRD 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 domestic or international operators unless it is for business use.

Actions upon Termination of Contract

All MACRD equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to the district at termination of contract.

MAC Recreation District
1195 SE Kemper Way, Madras, OR 97741
541.475.4253 • www.macrecdistrict.com

All data or intellectual property developed or gained during the period of employment remains the property of the MACRD 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 MACRD and there is no official provision for individual data privacy, however wherever possible the district 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. The district has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order 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 executive director. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with the district's disciplinary procedures.

Signature

I have received a copy of the MACRD's Acceptable Use Policy as revised and approved by the Board of Directors. I have read and understand the policy.

Employee Signature _____ Date _____

Printed Employee Name _____