CITY OF MADRAS COUNCIL POLICIES

IN MEMORY OF PFC THOMAS TUCKER
"Our debt to the heroic men and valiant women in the service of our country can never be repaid. They have earned our undying gratitude; America will never forget their sacrifice."
Harry Truman
HONORING ALL THOSE WHO SERVE
AHEAD

A vibrant, responsive community where you can thrive and grow.

CITY OF MADRAS
City Council Policies

Adopted and Effective as of April 27, 2021

COUNCIL:

Richard Ladeby, Mayor

Bartt Brick, Council President

Rosalind Canga, Councilor

Royce Embanks, Jr., Councilor

Jennifer Holcomb, Councilor

Gary Walker, Councilor

(Vacant Seat)

DIRECTORS:

Gus Burril, City Administrator

Kristal Hughes, Finance

Jeff Hurd, Public Works

Charo Miller, HR & Administration

Nicholas Snead, Community Development

Tanner Stanfill, Police Chief

UPDATED BY:

Lysa Vattimo, City Recorder

TABLE OF CONTENTS

SECTION ONE: ROLES & RESPONSIBILITIES OF THE COUNCIL 1

1.1 MAYOR (2-YEAR TERM):........ 1
1.2 COUNCIL PRESIDENT (SERVES 2-YEAR TERM):........ 1
1.3 COUNCIL (4-YEAR TERMS): 1
1.4 MEETINGS AND ATTENDANCE 2
1.5 TRAINING 2
1.6 EXPENSE REPORTS AND TRAVEL 2
1.7 EQUIPMENT AND ELECTRONICS 3
1.8 ETHICS AND CONFLICTS OF INTEREST........ 3
1.9 CONFIDENTIALITY 3

SECTION TWO: CODE OF CONDUCT 3

2.1 GENERAL........ 4
2.2 COUNCIL MEMBER CONDUCT WITH ONE ANOTHER 4
2.3 COUNCIL MEMBER CONDUCT WITH CITY STAFF 6
2.4 COUNCIL MEMBER CONDUCT WITH THE PUBLIC 6
2.5 PRINCIPLES OF PROPER CONDUCT 8
2.6 SOCIAL MEDIA........ 8

SECTION THREE: DELEGATION TO THE CITY ADMINISTRATOR 9

SECTION FOUR: MONITORING CITY PERFORMANCE........ 9

4.1 COUNCIL’S CONNECTION TO STAFF 9
4.2 POLICY SETTING BOUNDARIES FOR CITY ADMINISTRATOR 10

SECTION V: ANNUAL STRATEGIC GOALS 10

SECTION VI: COUNCIL DISCIPLINE AND CENSURE 11

6.1 COUNCIL MEMBER CONDUCT 11
6.2 CENSURE........ 11
6.3 EXPULSION........ 12
6.4 AMENDMENT 12

APPENDIX A – CITY ADMINISTRATOR FUNCTIONS A-1

APPENDIX B – CYBER POLICY........B-1

APPENDIX C – MICROSOFT SURFACE USER POLICY........ C-1

APPENDIX D – TRAVEL POLICY D-1

SECTION ONE: ROLES & RESPONSIBILITIES OF THE COUNCIL

The job of the council is to represent the citizens and taxpayers and lead the City by determining and requiring appropriate and excellent organizational performance. The council, comprised of six councilors and a mayor, acts as the policy makers, as required by the council/administrator form of government. The council members provide the city administrator with policy-making guidelines and performance objectives. The city administrator's staff turns these guidelines and objectives into programs and services.

1.1 MAYOR (2-YEAR TERM):

The mayor presides over council meetings preserving order in the meeting, enforcing the rules of the council, and determining the order of business. The mayor does not vote unless a tiebreaker is needed. The mayor will serve as the council's primary point of contact for the city administrator.

1.2 COUNCIL PRESIDENT (SERVES 2-YEAR TERM):

The council president is elected every two years during odd-numbered years by the council and serves as mayor pro-tem in the mayor's absence.

1.3 COUNCIL (4-YEAR TERMS):

A. Represents the interests of the citizens of the City. The council will review and make decisions on staff reports, presentations, resolutions, and ordinances that affect the livability and future of the community.

B. Determines and uses proactive strategies to ensure constructive two-way dialogue on input from staff and citizens as a means to link the entire City around goal achievement.

C. Develops written policies that address:

i. How the council will conceive, carry out, and monitor its own work;

ii. How authority is delegated and its proper use monitored; the city administrator's role and his or her authority and accountability;

iii. Constraints on city administrator authority which establish the practical, ethical, and legal boundaries within which all staff activity and decision-making will take place and be monitored; and

iv. What the council intends for the City to achieve through annual strategic goals.

D. Ensures city administrator performance by monitoring the:

i. Annual strategic goals;

ii. City administrator's accountability policies;

iii. Results of an annual assessment on city administrator performance; and

iv. Ensures annual strategic goals are the focus of organizational performance.

1.4 MEETINGS AND ATTENDANCE

All council members serve as members of the Madras Redevelopment Commission (“MRC”) and are expected to attend these meetings. MRC meetings begin at 5:30 p.m. and are held on the second and fourth Tuesday each month in the Madras City Hall Council Chambers located at 125 S.W. "E" Street. Occasionally, additional meetings (e.g., work sessions, executive sessions) may be held at other times or meetings may be cancelled.

Regular council meetings immediately follow MRC meetings. Occasionally, additional meetings (e.g., work sessions, executive sessions) may be held at other times or meetings may be cancelled.

Joint meetings between the council and Jefferson County Commission generally meet at 8:15 am on the first Wednesday of every other month beginning in February, in the Jefferson County Courthouse Annex located at 66 SE “D” Street.

Council members are expected to attend all council meetings; provided, however, the community understands that conflicts may prevent a member from attending every council meeting. Council members are expected to attend no less than 75% of all council meeting each year. For these purposes, the term “year” refers to the twelve-month period beginning from the start date of the member’s term and continuing each twelve-month period thereafter. As needed or appointed, council members will also attend various committee/commission meetings, outside agency meetings, and events and functions related to City business. Council members should notify the mayor and city recorder when they will be unable to attend a council meeting.

All council meetings are recorded and audio recordings are available to the public via the City’s website.

Any council member wishing to place an item on an agenda must contact the city administrator no later than seven (7) days prior to the regular meeting at which the item is to be considered.

1.5 TRAINING

Newly elected or appointed council members may be scheduled to meet with each City department director to learn about the function of the director’s department. In addition, the City pays for council members to attend ethics training with the League of Oregon Cities and the annual three-day League of Oregon Cities Conference in September. During the conference, council members will hear speakers discuss various city programs and projects and have the opportunity to interact with other elected officials from around the state.

1.6 EXPENSE REPORTS AND TRAVEL

When traveling on City business, council members will conduct themselves professionally as representatives of the City. Expenses must be pre-approved and documented completely and accurately, in accordance with the City of Madras Travel Policy (Appendix D) to be considered for reimbursement. Council members should coordinate with the HR & Administrative Director for assistance in travel plans and expense reports.

1.7 EQUIPMENT AND ELECTRONICS

Council members will be issued a tablet and a city-issued email address to conduct city business. Council members will not use either for private purposes. For more information, please refer to the Cyber Policy (Appendix B) and Microsoft Surface User Policy (Appendix C). It is important for council members to recognize that council member communications may be subject to public record laws. Council members should use the city-issued tablet and email address for official business only.

1.8 ETHICS AND CONFLICTS OF INTEREST

Public officials' ethics and conflicts of interest are covered by various constitutional provisions, the common law, state statutes, and occasionally, charter or ordinance provisions. Annually, council members are required to file a Statement of Economic Interest with the Oregon Government Ethics Commission by April 15th of each year. This annual filing is completed electronically.

Under no circumstances will a council member accept a gift or favor that is a bribe, or reflects to a reasonable person, an effort to improperly influence the councilor contrary to that council member's responsibility to the public to act impartially and on the merits of a matter.

1.9 CONFIDENTIALITY

Councilors will keep all written materials and verbal information provided them on matters of confidentiality under law in complete confidence to ensure that the City's position is not compromised. No mention of the information read or heard should be made to anyone other than other council members, the city administrator, or city attorney.

If the council, in executive session, provides direction or consensus to staff on proposed terms and conditions for any type of negotiations (whether it be related to property acquisition or disposal, pending or likely claims or litigation, or employee negotiations), all contact with the other parties will be made by designated staff or representatives handling the negotiations or litigation. A council member will not have any contact or discussion with any other party or its representative nor communicate any executive session discussion. If a council member does not refrain from disclosing such information as required by these council rules, the council will convene and address the matter, as provided in the censure provision of these rules.

SECTION TWO: CODE OF CONDUCT

The council is composed of individuals with a wide variety of backgrounds, personalities, values, opinions, and goals. Each council member has chosen to serve in public office to preserve and protect the present and future of the City. This common goal should be acknowledged even as council members may "agree to disagree" on contentious issues. The governance of Madras relies on the cooperative efforts of all council members, who set policy, and city staff, who implement and administer the council's policies. Therefore, every effort should be made to be cooperative and show mutual respect for the contributions made by each individual for the good of the community.

Making the public feel welcome is also an important part of the democratic process. No signs of partiality, prejudice, or disrespect should be evident on the part of individual council members toward an individual participating in a public forum. Every effort should be made to be fair and impartial in listening to public testimony.

The council commits itself and its members to ethical, businesslike and lawful conduct, including proper use of authority appropriate decorum when acting as council members.

2.1 GENERAL

A. Council members will represent the interests of the citizens of the entire City. This accountability to the whole City supersedes:

i. Any conflicting loyalty a member may have to other advocacy or interest groups.

ii. Loyalty based upon membership on other councils or staffs.

iii. Conflicts based upon the personal interest of any council member.

iv. Conflicts based upon being a relative of an employee of the City.

v. Any other conflicts of interest as outlined by the Oregon Government Ethics Commission.

B. Council members may not attempt to exercise individual authority over the organization. As such:

i. Council member interaction with the city administrator, or with staff must recognize the lack of authority vested in individuals except when explicitly authorized by the council; and

ii. Council member interaction with the public, press, or other entities must recognize the same limitation and the inability of any council member to speak for the council except to repeat explicitly stated council decisions. The mayor may respond to requests for information on issues that have not yet been decided by council. The city administrator may respond to requests for information on issues that have been decided by council.

C. Council members will maintain confidentiality appropriate to sensitive issues and information that otherwise may tend to compromise the integrity or legal standing of the council and/or City, especially those matters discussed in closed session.

D. Council members will abide by the current Code of Conduct for council members. Changes or additions to the current Code of Conduct requires a majority vote of the council.

2.2 COUNCIL MEMBER CONDUCT WITH ONE ANOTHER

A. PUBLIC MEETINGS

i. **Practice Civility and Decorum in Discussions and Debate.** Difficult questions, tough challenges to a particular point of view, and criticism of ideas and information are legitimate elements of a free democracy in action. This does not allow, however, council members to make belligerent, personal, impertinent, slanderous, threatening, abusive, or disparaging comments. No shouting or physical actions that could be construed as threatening will be tolerated. Council members should conduct themselves in a professional manner at all times, including dressing appropriately for the meeting and/or event they are attending. This includes apparel that advertises businesses, social groups, or special interest groups. Apparel with the City logo is acceptable.

ii. **Honor the Role of the Mayor in Maintaining Order.** It is the responsibility of the mayor to keep the comments of the council members on track during all meetings. Council members should honor efforts by the mayor to focus discussion on current agenda items. If there is a disagreement about the agenda or the mayor's actions, those objections should be voiced politely and with reason, following procedures outlined in parliamentary procedures.

iii. **Avoid Personal Comments that Could Offend other Council Members**. If a council member is personally offended by remarks of another council member, the offended council member should make notes of the actual words used and call for a "point of personal privilege" that challenges the other council member to justify or apologize for the language used. The mayor will maintain control of this discussion. If the mayor is challenged, the council president will step in to control the discussion.

iv. **Demonstrate Effective Problem-Solving Approaches.** Council members have a public stage to show how individuals with disparate points of view can find common ground and seek a compromise that benefits the community as a whole.

B. PRIVATE ENCOUNTERS

i. **Continue Respectful Behavior in Private.** The same level of respect and consideration of differing points of view that is deemed appropriate for public discussions should be maintained in private conversations.

ii. **Be Aware of the Insecurity (Non-Confidentiality) of Written Notes, Voicemail, and Email**. Technology allows words written or said without much forethought to be distributed wide and far. Would you feel comfortable having this note sent to others? How would you feel if this voicemail message was played on a speakerphone in a full office? What would happen if this Email message were forwarded to others? Written notes, voicemail messages and Email should be treated as potentially "public" communication!

iii. **Even Private Conversations can have Public Presence**. Elected officials are always on display – their actions, mannerisms, and language are monitored by people around them that they may not know. Lunch table conversations will be eavesdropped upon, parking lot debates will be watched, and casual comments between individuals before and after public meetings noticed.

C. QUICK TIPS

- Preserve dignity and self-respect.
- Listen for the message even if you don't agree with it.
- Respect others as they are.
- Express your independent perspective.
- Participate intelligently.
- Be willing to delegate and let others make decisions.
- Lead from the front of the parade.
- Control all you should; not all you can.
- Use few words after much thought; rather than many words after little thought.
- Seek to create change and overcome the influence of conventional wisdom.
- Recognize when you need outside experts.

- Recognize the efforts of others.
- Continuously pursue excellence.

2.3 COUNCIL MEMBER CONDUCT WITH CITY STAFF

A. **Treat all Staff as Professionals.** Clear, honest communication that respects the abilities, experience, and dignity of each individual is expected. Poor behavior towards staff is not acceptable.

B. **Direct Administrative and Operational Questions to City Management.** Questions of city staff and/or requests for additional information that may take staff time in excess of fifteen minutes should be directed <u>only</u> to the city administrator or designee. The city administrator should be copied on any request. Materials supplied to a council member regarding pertinent, urgent or important issues that would be of interest to other council members will be made available to all members of the council so that all have equal access to information.

C. **When Possible, Keep Communication with City Staff Short, to the Point and at the Best Possible Time.** Every effort should be made to limit disruption to the work of city staff. Council members should avoid making requests to staff who are in meetings, on the phone, or engrossed in performing their job functions.

D. **Never Publicly Criticize an Individual Employee.** Council members should never express concerns about the performance of a city employee in public or to the employee directly. Comments about staff performance should only be made to the city administrator through private correspondence or conversation.

E. **Do Not Get Involved in Administrative Functions.** Council members must not attempt to influence city staff on the hiring process, awarding of contracts, selecting of consultants, or other such administrative functions except when council input is requested by the city administrator.

F. **Check with City Staff on Correspondence Before Taking Action.** Before sending correspondence, council members should check with the city administrator to see if an official city response has already been sent or is in progress.

G. **Do not Attend Meetings with City Staff Unless Requested by Staff.** Even if the council member does not say anything, the council member’s presence implies support, or may show partiality, intimidate staff, and hamper staff’s ability to do their job objectively.

2.4 COUNCIL MEMBER CONDUCT WITH THE PUBLIC

A. PUBLIC MEETINGS

i. **Be Welcoming to Speakers and Treat Them with Care and Gentleness.** Because personal concerns are often the issue of those who come to present to the council, council members should remember that how they treat the speaker will either help them relax or push their emotions to a higher level of intensity.

ii. **Be an Active Listener**. It is disconcerting to speakers to have council members not look at them when they are speaking. It is fine to look down at documents or to make notes, however reading for a long period of time or gazing around the room gives the appearance of disinterest. Be aware of facial expressions, especially those that could be interpreted as “smirking,” disbelief, anger, or boredom.

iii. **Ask for Clarification, Avoid Debate and Argument With the Public**. Only the mayor (and not individual council members) may interrupt a speaker during a presentation. However, a council member may ask the mayor for a “point of order” if the speaker goes off topic or exhibits behavior or language the council member finds disturbing.

iv. **If speakers become flustered or defensive by Council questions**, it is the responsibility of the mayor to calm and focus the speaker and to maintain the order and decorum of the meeting. Questions by council members to members of the public should seek to clarify or expand information. It is never appropriate to belligerently challenge or belittle the speaker. Council members’ personal opinions or inclinations about upcoming votes should not be revealed until after the public hearing.

v. **Make No Personal Attacks of any Kind, Under any Circumstances**. Council members should be aware that their body language and tone of voice, as well as the words they use, can appear to be intimidating or aggressive. This includes verbal and written words.

B. UNOFFICIAL MEETINGS

i. **Make no Promises on Behalf of the Council or Staff.** It is inappropriate to promise council action overtly or implicitly, or to promise city staff will do something specific (i.e., fix a pothole, replace flowers, fix a leak, etc.)

ii. **Speak with One Voice**. Council members will frequently be asked to explain a council action or to give their opinion about an issue as they meet and talk with constituents in the community. It is appropriate to give a brief overview of the facts or city policies as they relate to council action. Objectively present the council’s collective decision or direction, even when you may not agree. If you feel the need to express your own opinion, state it in terms such as: “I would have preferred “x” however the council wanted “y” so that’s what we will be doing.” Explaining council decisions, without giving your personal criticism of the council’s actions, will serve to strengthen the community’s image of the council.

iii. **Make No Personal Comments About Other Council Members**. It is acceptable to publicly disagree about an issue, however it is unacceptable to make derogatory comments about other council members, their opinions, and their actions. Honesty and respect for the dignity of each individual should be reflected in every word and action taken by council members. It is a serious and continuous responsibility.

iv. **Intentional or Repeated Improper Conduct of a Council Member**. Council members who intentionally and repeatedly do not follow proper conduct may be reprimanded or formally censured by the council. Serious infractions of the Code of Conduct could lead to other sanctions as deemed appropriate by the council.

Council members should point out to the offending council member infractions of the Code of Conduct. If the offenses continue, then the matter should be referred to the mayor in private. If the mayor is the individual whose actions are being challenged, then the matter should be referred to the council president.

It is the responsibility of the mayor to initiate action if a council member's behavior may warrant sanction. If no action is taken by the mayor, the alleged violation(s) can be brought up with the full council in executive session or a public meeting.

If violation of the Code of Conduct is outside of the observed behaviors by the mayor or council members, the alleged violation should be referred to the mayor. The mayor may ask the city administrator and/or the city attorney to investigate the allegation and report the findings to the mayor. It is the mayor's responsibility to take the next appropriate action.

These actions can include but are not limited to: discussing and counseling the individual on the violations; recommending sanction to the full council to consider in an executive session or public meeting; or forming a council ad hoc subcommittee to review the allegation; the investigation and its findings, as well as to recommend sanction options for council consideration.

2.5 PRINCIPLES OF PROPER CONDUCT

- Keep promises.
- Be dependable.
- Build a solid reputation.
- Participate and be available.
- Demonstrate patience.
- Show empathy.
- Hold onto ethical principles under stress.
- Listen attentively.
- Study thoroughly.
- Keep integrity intact.
- Overcome discouragement.
- Go above and beyond, time and time again.
- Model a professional manner.
- Respect one another as individuals.
- Respect the validity of different opinions.
- Respect the democratic process.
- Respect the community we serve.

2.6 SOCIAL MEDIA

Social media platforms create and foster online social communities that connect users from various locations and interest areas. These platforms offer many different ways for users to interact with one another, such as instant messaging, blogging and commenting, microblogging, events, status updates, online communities, discussion forums, message boards, podcasts, website link sharing, wikis, video conferencing, and sharing photos and videos. The City acknowledges that this type of technology changes rapidly and, therefore, this list is intended to be illustrative rather than comprehensive, and this definition should in no way be construed to limit applicability.

Council members will not establish, operate, maintain or use any social media accounts in their official capacity as a council member. Council members who engage in personal use of social media outside of their official capacity may not use the logo of the City. Council members may not speak as a representative of the City in the course of their personal use of social media.

It is important to reflect on how social media posts may be interpreted by viewers and whether the post will "Help or Hurt" the reputation of city staff, other council members or whether it will stir up controversy that will require city staff to have to respond in an official capacity. If in doubt, a council member should reach out to the city administrator for guidance.

SECTION THREE: DELEGATION TO THE CITY ADMINISTRATOR

The council will instruct the city administrator through written policies that prescribe the City goals to be achieved and describe organizational situations and actions to be avoided. The council will support any reasonable and consistent interpretation of those policies by the city administrator.

Accordingly:

1. Council will develop policies instructing the city administrator to achieve defined goal results. These policies will be developed systematically from the broadest, most general level to more defined levels, and will be called Strategic Goals.
2. Council will develop policies to let the city administrator know what practices and circumstances to avoid and to establish the practical, ethical and legal boundaries within which all staff activity and decision-making will take place and be monitored. These policies will be developed systematically from the broadest, most general level to more defined levels, and they will be called City Administrator Accountability Policies (Appendix A).
3. As long as the city administrator uses any reasonable and consistent interpretation of the Council's Strategic Goals and City Administrator Accountability Policies the city administrator is authorized to establish administrative procedures, make all decisions, establish all practices and develop all activities the city administrator deems appropriate to achieve the council's vision, goals, and policy expectations.
4. The council may change its Strategic Goals and/or City Administrator Accountability Policies at any time after input from staff and by majority vote of council members, thereby shifting the boundary between council and city administrator domains. By doing so, the council changes the latitude of choice given to the city administrator. However, as long as any council-specified delegation of authority is in place, the council will respect and support any reasonable and consistent interpretation of its policies, even though city administrator choices may not be the choices the council or its members may have made.

SECTION FOUR: MONITORING CITY PERFORMANCE

While the council is encouraged to communicate with staff, the council's connection to the City's daily operations, its achievements, and conduct will be through the city administrator.

4.1 COUNCIL'S CONNECTION TO STAFF

The city administrator is the council's only link to operational achievement and conduct, so that all authority and accountability of employees, as far as the council is concerned, is considered the authority and accountability of the city administrator. Accordingly:

A. The council will not give instructions to persons who report directly or indirectly to the city administrator.

B. The council will not evaluate the performance of any employee other than the city administrator.

C. The council will review city administrator performance on a semi-annual (November) and annual (May) basis. Systematic and rigorous monitoring of, and–feedback on city administrator job performance will be against the expected progress of the Annual Strategic Goals and compliance with the boundaries specified in city administrator Accountabilities Policies. The council will acquire monitoring data by one or more of three methods:

    i. By internal report, in which the city administrator discloses compliance information to the council.

    ii. By external report, in which an external, disinterested third party selected by the council assesses compliance with City policy.

    iii. By direct council member inspection, in which the council member assesses compliance with the appropriate policy criteria.

4.2 POLICY SETTING BOUNDARIES FOR CITY ADMINISTRATOR

All policies that set boundaries for the city administrator will be monitored at a frequency and by a method recommended and approved by the council. The council can monitor any policy at any time by any method, but will ordinarily depend on a routine schedule:

Task	**Method**	Frequency
Benefits Review (cost and level/quality of service)	HR and CIS	Annually
Wage Analysis	Internal By HR and External by Third Party	Every Three Years
Insurance Rate Comparison Bids	External By Agent of Record and CIS	Annually
Financial Reports	Internal By Finance Director	Monthly
Financial Audit	External Auditor	Annually
Customer Satisfaction Surveys	Internal And External Methods	Following service delivery
Grant Progress Reports	Internal By Finance Director and Departments	Quarterly or as needed

SECTION V: ANNUAL STRATEGIC GOALS

The council has established broad goals that will serve the City for many years as part of the City's overall strategic direction. It will be the responsibility of the city administrator to produce Annual Strategic Goals for Council review and approval. The Annual Strategic Goals will demonstrate through Objectives and Action Plans what the City intends to accomplish in the coming year in support of City goals. Accordingly:

1. Each year in February, the city administrator will present the City's "draft" Annual Goals to the council.

2. Each year in April the council will adopt the City's Annual Strategic Goals as-is or with recommended changes or additions. If there are additions, both council and staff must agree that the overall plan is doable in a one-year period of time or modify the plan until such agreement is reached.
3. The Annual Strategic Goals will be presented showing:
   - A. **Objectives** that will be accomplished in the coming year to support city goals.
   - B. The City **Goal** that the Objective supports.
   - C. The **Responsible Person or Department** for Objective achievement.
   - D. The **Target Date for Objective Completion.**
4. The Objectives in the Annual Strategic Goals should state specifically what will be accomplished in one year.
5. Moving Objective achievement to a new year will occur only if the council agrees by majority vote, after reviewing supporting argument for the move, that unforeseen circumstances warrant delaying Objective achievement.
6. If the council determines it is in the best interest of the City to add an Objective to the Annual Strategic Goals any time other than at the April Council meeting, the council, working with the city administrator, will determine which of the existing Objectives will be moved to next year's Annual Strategic Goals to allow adequate time and other resources for the new Objective.
7. Success or failure in the achievement of the Objectives in the Annual Strategic Goals will be considered the success or failure of the City Administrator's performance and will be considered as one part of the city administrator's annual review.
8. The city administrator will be responsible for all Objective achievement either by his/her own effort or through the efforts of the management team.

SECTION VI: COUNCIL DISCIPLINE AND CENSURE

6.1 COUNCIL MEMBER CONDUCT

At all times, while in session or otherwise, each councilor will conduct himself or herself in a manner appropriate to the dignity of the office and in a manner the councilor reasonably believes is in the City's best interests.

6.2 CENSURE

The council has the inherent right to make and enforce its own rules, code of conduct, and to ensure compliance with laws generally applicable to public bodies. Should any councilor act in a manner constituting a substantial violation of the council's rules, code of conduct, and/or other general laws, the council, acting as a whole, may discipline the councilor to the extent provided by law, including public reprimand. To exercise such inherent right, the council has the right to investigate the councilor's actions. Neither the council nor any councilor will have the right to make public any information obtained through the investigation. Any councilor accused of a substantial violation of the council's rules, code of conduct, and/or any other laws applicable to public bodies will have the right to present a defense to the allegations, including the right to present rebuttal evidence, and to have representation by legal counsel. Upon the council's finding that a substantial violation has occurred, and that such violation affects the councilor's ability to represent the interests of the City as a whole, the council may, upon a majority vote of the council (other than the offending member) impose a censure on the offending member.

6.3 EXPULSION

Subject to applicable laws, any of the following will be sufficient for the mayor to direct a councilor to leave the premises for the duration of a meeting: (a) use of unreasonably loud or disruptive language, conduct, and/or noise; (b) engaging in violent or distracting actions; (c) refusal to obey the rules of conduct provided within this Handbook; and/or (d) refusal to obey an order of the mayor or an order issued by a councilor which has been approved by a majority of the council. Before being required to leave, the affected councilor will be given a warning by the mayor to cease. If a counselor is expelled, his or her expulsion from the meeting will result in that councilor's unexcused absence. If the mayor fails to act under this Section 6.3, any member of the council may obtain the floor and move to require enforcement of this rule. Upon affirmative vote of the majority of the council, the person so expelled will be removed.

6.4 AMENDMENT

These policies replace and supersede the Councilor policies dated effective July 23, 2019 (the "Existing Policy") in its entirety (the Existing Policy is of no further force and effect). This Handbook (and the rules and policies contained herein) supersedes all resolutions, policies, and/or practices concerning or related to matters contained in this Handbook if and to the extent in conflict with the policies contained in this Handbook.

APPENDIX A – CITY ADMINISTRATOR FUNCTIONS

CITY ADMINISTRATOR ACCOUNTABILITY POLICY

The city administrator will not cause or allow any practice, activity, decision, or organizational circumstance that is either unlawful, imprudent, or in violation of commonly accepted business and professional ethics including but not limited to the following:

1. The city administrator will not allow the assets to be unprotected, inadequately maintained, or unnecessarily risked. Accordingly the city administrator may not:
    a. Allow unauthorized personnel access to City funds.
    b. Subject facilities or equipment to improper wear and tear or insufficient routine maintenance.
    c. Unnecessarily expose the City, council, or staff to claims of liability.
    d. Make any purchase without following the City's current purchasing policy, state statute and City policy.
    e. Fail to protect intellectual property, information, and files from loss or significant damage, or access by unauthorized persons.
    f. Receive, distribute and/or account for funds under controls that are insufficient to meet standard accounting practices and/or to protect the City.
    g. Invest or hold operating capital in insecure instruments, including uninsured checking accounts or in non-interest-bearing accounts except where necessary to facilitate ease in operational transactions or where it does not benefit the City.
    h. Endanger the City's image or credibility, particularly in ways that would hinder its accomplishment of its mission.
    i. Fail to timely provide council, staff, contract vendors and the public information necessary to carry on the City's business.
2. With respect to the treatment of employees, the city administrator may not cause or allow conditions that are unfair or undignified. Accordingly, the city administrator will not:
    a. Operate without following written personnel policies. This would include things that clarify personnel rules for employees, provide for effective handling of complaints and protect against wrongful or illegal conditions.
    b. Discriminate against any employee at any time for any reason.
    c. Fail to acquaint staff with this policy.
3. Financial planning in any fiscal year will not deviate from actual expenditures approved in the Annual Strategic Implementation Plan, except for approved budget adjustments, or risk fiscal jeopardy for the City. Accordingly, the city administrator will not allow budgeting that:
    a. Contains too little information to enable credible projection of revenues and expenses, separation of capital and operational items, cash flows and disclosure of planning assumptions.
    b. Acquires, encumbers or disposes of real property without the Council's approval.
4. Regarding employment, compensation and benefits to employees, consultants, and contract workers, the city administrator will not cause or allow jeopardy to fiscal integrity or City image. Accordingly the city administrator may not:

a. Change his/her own compensation and/or approved benefits.
b. Promise or imply benefits that are outside approved benefit policies.
c. Promise or imply permanent or guaranteed employment.
d. Establish compensation that deviates materially from the geographic or professional market for the skills employed and/or that is outside of the approved budget.

5. The city administrator will not permit the council to be uninformed or unsupported in its work. Accordingly, the city administrator will not:

   a. Neglect to submit monitoring data, status reports, financial information or other pertinent information required by the council in a timely, accurate, and understandable manner.

   b. Let the council be unaware of relevant trends or significant changes of any kind that could [or have] negatively impact[ed] the City.

   c. Fail to report in a timely manner an actual or anticipated non-compliance with local, state, and federal rules and statutes.

6. Regarding City insurance, employee benefit providers and employee wages, the city administrator will not:

   a. Fail to review all benefit providers for cost, and comparative services at time intervals specified in Policy VI.

   b. Fail to do wage research and analysis at time intervals specified in Policy VI.

With respect to treatment of paid and volunteer staff, the city administrator will not knowingly cause or knowingly allow conditions, procedures, actions or decisions which are unlawful, unethical, unsafe, disrespectful, undignified, immoral, disreputable, disruptive of City operations, or in violation of council policy.

Accordingly, the city administrator may not:

1. Fail to develop procedures for reasonable background inquiries and checks prior to hiring any paid personnel or utilizing the services of any volunteers;
2. Operate without written personnel and administrative policies which:
   a. Clarify personnel rules and procedures for staff.
   b. Provide for effective handling of grievances.
   c. Include adequate job descriptions for all staff positions.
   d. Include salary and compensation plans that comply with state law.
   e. Include an effective personnel performance evaluation system.
   f. Establish procedures for reductions in workforce.
   g. Protect against sexual harassment.
   h. Protect against racial, religious, gender, age, disability and ethnic bias or discrimination or any known legal infraction against a protected groups(s).
   i. Provide for a workplace that is free from illegal drugs; misuse of legal drugs; and alcohol.
3. Prevent employees from grieving to the Council when internal grievance procedures have been exhausted and the employee alleges that Council policy has been violated;
4. Fail to protect confidential information;
5. Fail to provide for open communication and the sharing of ideas; and
6. Fail to provide staff with an opportunity to become familiar with the provisions of this policy.

APPENDIX B – CYBER POLICY

City of Madras

Cybersecurity Policy

May 1, 2020

Table of Contents

Roles and Responsibilities 3
IDENTIFY (ID) 4
Asset Management 4
PROTECT (PR) 5
Identity Management, Authentication and Access Control 6
Awareness and Training 7
Data Security 7
Data Classification 7
Data Storage 8
Data Transmission 8
Data Destruction 8
Data Storage 9
Information Protection Processes and Procedures 9
Secure Software Development 9
Contingency Planning 10
Network Infrastructure 10
Network Servers 11
Protective Technology 12
Email Filtering 12
Network Vulnerability Assessments 12
DETECT (DE) 12
Anomalies and Events 12
Security Continuous Monitoring 13
Anti-Malware Tools 13
Patch management 13
RESPOND (RS) 13
Response Planning 13
Electronic Incidents 14
Physical Incidents 14
Notification 14
RECOVER (RC) 15
Appendix A – Acceptable Use Policy 16
Appendix B – Confidentiality and Non-Disclosure Agreement 20

Objective

The focus of this policy is to help City of Madras meet its objectives. We recognize that information and the protection of information is required to serve our citizens. We seek to
to ensure that appropriate measures are implemented to protect our citizen's information. This Cybersecurity Policy is designed to establish a foundation for an organizational culture of security. This policy will be reviewed annually and approved by the Security Officer.

The purpose of this policy is to clearly communicate the City of Madras security objectives and guidelines to minimize the risk of internal and external threats while taking advantage of opportunities that promote our objectives.

This policy applies, to all City of Madras elected officials, employees, contractors, consultants, and others specifically authorized to access information and associated assets owned, operated, controlled, or managed by City of Madras. Additionally, leadership must ensure that all contracts and similar agreements with business partners and service providers incorporate appropriate elements of this policy.

Compliance

Oregon public entities must comply with the Oregon Identity Theft Protection Act, ORS 646A.600 – 628. ORS 646A.622 (d) requires the implementation of a Cybersecurity program. Non-compliance with this policy may pose risks to the organization; accordingly, compliance with this program is mandatory. Failure to comply may result in failure to obtain organizational objectives, legal action, fines and penalties. Breaches with the potential to impact more than 250 individuals must be reported to the Oregon Department of Justice.

https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/data-breaches/

Roles and Responsibilities

City of Madras has appointed the following roles and responsibilities to execute and monitor the policies described in this document.

Security Officer

- Ensure that a written Cybersecurity Policy is developed and implemented.
- Confirm identification, acquisition, and implementation of information system software and hardware.
- Identify all Personally Identifiable Information.
- Ensure implementation, enforcement, and effectiveness of IT Security policies and procedures.
- Facilitate an understanding and awareness that security requires participation and support at all organizational levels.

- Oversee daily activities and use of information systems to ensure employees, business partners, and contractors adhere to these policies and procedures.

MSSP – Managed Security Service Provider

- Execute requested changes made by the Security Officer
- Monitor and manage security components protecting city data and systems
- Prepare and present periodic security reports and notifications
- Advise on best practices for cyber security protection

Employees and Contractors

- See Appendix A - Acceptable Use Policy

Identify, Protect, Detect, Respond, and Recover

The following sections outline City of Madras requirements and minimum standards to facilitate the secure use of organizational information systems. The information presented in this policy follows the format of the control families outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST CSF): ***Identify, Protect, Detect, Respond, and Recover***.

The scope of security controls addressed in this policy focus on the activities most relevant to City of Madras as defined by the Center for Internet Security (CIS) and industry best practices. Questions related to the interpretation and implementation of the requirements outlined in this policy should be directed to the Security Officer.

IDENTIFY (ID)

Objective: To develop the organization’s understanding that’s necessary to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Asset Management

An inventory of all approved hardware and software on City of Madras network and systems will be maintained in a computer program or spreadsheet that documents the following:

- The employee in possession of the hardware or software.
- Date of purchase.
- Amount of purchase.
- Serial number.
- Type of device and description.
- A listing of software or devices that have been restricted.

Personally Identifiable Information (PII)

An inventory of all PII information by type and location will be taken. The following table may be useful to inventory PII.

Location	**PII by type**	**Essential**	**Location**	**Owner**
Website				
Contractors				
File in staff office				
File in building				
File offsite				
Desk top				
HR System				
Financial System				
Laptop				
Flash drive				
Cell phones				
Tablets				
Other				

Each manager will determine if PII is *essential*. If PII is not essential, it will either not be collected, or (if collected) will be destroyed. Do not collect sensitive information, such as a Social Security numbers, if there is no legitimate business need. If this information does serve a need, apply your entity's record retention plan that outlines what information must be kept, and dispose of it securely once it is no longer required to maintain.

All PII no longer needed shall be shredded if in paper form or destroyed by IT if in electronic form.

The Oregon Identity Theft Protection Act prohibits anyone (individual, private or public corporation, or business) who maintains Social Security numbers from:

- Printing a consumer's SSN on any mailed materials not requested by the consumer unless redacted
- Printing a consumer's SSN on a card used by the consumer that is required to access products or services
- Publicly posting or displaying a consumer's SSN, such as on a website

Exceptions include requirements by state or federal laws, including statute records (such as W2s, W4s, 1099s, etc.) that are required by law to be made available to the public, for use for internal verification or administrative processes, or for enforcing a judgment or court order.

PROTECT (PR)

Objective: To develop and implement appropriate safeguards to ensure the delivery of critical services.

Identity Management, Authentication and Access Control

The Security Officer is responsible for ensuring that access to the organization's systems and data is appropriately controlled. All systems housing City of Madras data (including laptops, desktops, tablets, and cell phones) are required to be protected with a password or other form of authentication. Except for the instances noted in this policy, users with access to City of Madras systems and data are not to share passwords with anyone.

City of Madras has established following password configuration requirements for all systems and applications (where applicable):

- Minimum password length: 8 characters
- Password complexity: requires alphanumeric and special characters
- Prohibited reuse for twelve (12) iterations
- Changed periodically every 90 days
- Invalid login attempts set to three
- Automatic logout due to inactivity = 30 minutes

Other potential safeguards include:

- Not allowing PII on mobile storage media
- Locking file cabinets
- Not allowing PII left on desktops
- Encrypting sensitive files on computers
- Requiring password protection
- Implementing the record retention plan and destroying records no longer required

Where possible, multi-factor authentication will be used when users authenticate to the organization's systems.

- Users are granted access only to the system data and functionality necessary for their job responsibilities.
- Privileged and administrative access is limited to authorized users who require escalated access for their job responsibilities and where possible will have two accounts: one for administrator functions and a standard account for day to day activities.
- All user access requests must be approved by the Security Officer.
- It is the responsibility of the Security Officer to ensure that all employees and contractors who separate from the organization have all system access removed within I hour of departure.

On an annual basis, a review of user access will be conducted under the direction of the Security Officer to confirm compliance with the access control policies outlined above.

Awareness and Training

City of Madras personnel are required to participate in security training in the following instances:

1. All new hires are required to complete security awareness training before receiving login credentials.
2. Formal security awareness refresher training is conducted on an annual basis. All employees are required to participate in and complete this training.

Upon completion of training, participants will review and sign the ***Acceptable Use Policy*** included in Appendix A.

Two online classes are available through the CIS Learning Center at learn.cisoregon.org: "*Cyber Threats and Best Practices to Confront Them*" and "*Cyber Security Basics*."

On an annual basis, City of Madras will conduct email phishing exercises of its users. The purpose of these tests is to help educate users on common phishing scenarios. It will assess their level of awareness and comprehension of phishing, understanding and compliance with policy around safe handling of e-mails containing links and/or attachments, and their ability to recognize a questionable or fraudulent message.

Data Security

Data Classification

You must adhere to your Records Retention Policy regarding the storage and destruction of data. Data residing on corporate systems must be continually evaluated and classified into the following categories:

- **Employees Personal Use**: Includes individual user's personal data, emails, documents, etc. This policy excludes an employee's personal information, so no further guidelines apply.
- **Marketing or Informational Material**: Includes already-released marketing material, commonly known information, data freely available to the public, etc. There are no requirements for public information.
- **Operational**: Includes data for basic organizational operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.
- **Confidential:** Any information deemed confidential. The following list provides guidelines on what type of information is typically considered confidential. Confidential data may include:

  - Employee or customer Social Security numbers or personally identifiable information (PII)
  - Personnel files
  - Medical and healthcare information
  - Protected Health Information (PHI)
  - Network diagrams and security configurations

- Communications regarding legal matters
- Passwords/passphrases
- Bank account information and routing numbers
- Payroll information
- Credit card information
- Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

Data Storage

The following guidelines apply to storage of the different types of organizational data.

- **Operational:** Operational data should be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). Some type of system- or disk-level redundancy is encouraged.
- **Confidential**: Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard or code secured.

Data Transmission

The following guidelines apply to the transmission of the different types of organizational data.

- **Confidential**: Confidential data must not be 1) transmitted outside the organization’s network without the use of strong encryption, 2) left on voicemail systems, either inside or outside the organization's network.

Data Destruction

You must follow your records retention policy before destroying data.

- **Confidential:** Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

  - Paper/documents: Cross-cut shredding is required.
  - Storage media (CD's, DVD's): Physical destruction is required.
  - Hard drives/systems/mobile storage media: At a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the organization must use the most secure commercially-available methods for data wiping. Alternatively, the organization has the option of physically destroying the storage media.

Data Storage

Stored Data includes any data located on organization-owned or organization-provided systems, devices, media, etc. Examples of encryption options for stored data include:

- Whole disk encryption
- Encryption of partitions/files
- Encryption of disk drives
- Encryption of personal storage media/USB drives
- Encryption of backups
- Encryption of data generated by applications

Data while transmitted includes any data sent across the organization network or any data sent to or from an organization-owned or organization-provided system. Types of transmitted data that shall be encrypted include:

- VPN tunnels
- Remote access sessions
- Web applications
- Email and email attachments
- Remote desktop access
- Communications with applications/databases

Information Protection Processes and Procedures

Secure Software Development

Where applicable, all software development activities performed by City of Madras or by vendors on behalf of the organization shall employ secure coding practices including those outlined below.

A minimum of three software environments for the development of software systems should be available – development, quality assurance, and a production environment. Software developers or programmers are required to develop in the development environment and promote objects into the quality assurance and production environments. The quality assurance environment is used for assurance testing by the end user and the developer. The production environment should be used solely by the end user for production data and applications. Compiling objects and source code is not allowed in the production environment. The information technology manager or an independent peer review will be required for promotion objects into the production environment.

- All production changes must be approved before being promoted to production.
- Developers should not have the ability to move their own code.
- All production changes must have a corresponding help desk change request number.
- All production changes must be developed in the development environment and tested in the quality assurance environment.
- All emergency changes must be adequately documented and approved.

Software code approved for promotion will be uploaded by the technical resource under the direction of the Security Officer to the production environment from the quality assurance environment once the change request is approved. The Security Officer may work with the developer to ensure proper placement of objects into production.

Contingency Planning

The organization's business contingency capability is based upon cloud and local backups of all critical business data. This critical data is defined as any data required to perform city business or to meet data retention policies. Full data backups will be performed on a weekly basis with nightly incremental backups of changed data rolled up at week's end. Confirmation that backups were performed successfully will be conducted at the completion of each backup process. Testing of cloud backups and restoration capability will be performed quarterly.

During a contingency event, all IT decisions and activities will be coordinated through and under the direction of the Security Officer.

The following business contingency scenarios have been identified along with the intended responses:

- In the event that one or more of City of Madras 's systems or applications are deemed corrupted or inaccessible, the Security Officer will work with the respective vendor(s) to restore data from the most recent cloud or local backup as appropriate and, if necessary, acquire replacement hardware.

- In the event that the location housing the City of Madras systems are no longer accessible, the Security Officer will work with the respective vendor(s) to acquire any necessary replacement hardware and software, implement these at one of the organization's other sites, and restore data from the most recent cloud or local backup as appropriate.

As an important reminder, CIS covers data reproduction (subject to a deductible) for only one week.

Network Infrastructure

The organization will protect the corporate electronic communications network from the Internet by utilizing a firewall. For maximum protection, the corporate network devices shall meet the following configuration standards:

- Vendor recommended, and industry standard configurations will be used.
- Changes to firewall and router configuration will be approved by the Security Officer and implemented by written request.
- Both router and firewall passwords must be secured and difficult to guess.
- The default policy for the firewall for handling inbound traffic should be to block all packets and connections unless the traffic type and connections have been specifically permitted.
- Inbound traffic containing ICMP (Internet Control Message Protocol) traffic should not be passed in from the Internet, or from any un-trusted external network.
- All web services running on routers must be disabled.

- Simple Network Management Protocol (SNMP) Community Strings must be changed from the default “public” and “private”.

Network Servers

Servers typically accept connections from several sources, both internal and external. Generally, the more sources that connect to a system, the more risk associated with that system, so it is particularly important to secure network servers. The following statements apply to the organization's use of network servers:

- Unnecessary files, services, and ports should be removed or blocked. If possible, follow a server-hardening guide, which is available from the leading operating system manufacturers.
- Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.
- If possible, a standard installation process should be developed for the organization's network servers. A standard process will provide consistency across servers no matter what employee or contractor handles the installation.
- Clocks on network servers should be synchronized with the organization's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.

Network Segmentation

Network segmentation is used to limit access to data within the City of Madras network based upon data sensitivity. City of Madras maintains two wireless networks. The *guest* wireless network is password protected, and proper authentication will grant the user internet access only. Access to the *secure* wireless network is limited to City of Madras personnel and provides the user access to the intranet.

Under the direction of the Security Officer, the third-party network administrator or MSSP manages the network user accounts, monitors firewall logs, and operating system event logs. The Security Officer authorizes vendor access to the system components as required for maintenance.

Device Configurations

Mobile devices such as laptops, notebooks, and smart phones as well as workstations, and other hardware and software will be configured using industry-accepted best practices. These configurations will incorporate security features and protections. All configurations will be documented and reviewed annually. The MSSP will assist in adhering to the configurations.

Protective Technology

Email Filtering

A good way to mitigate email related risk is to filter it before it reaches the user so that the user receives only safe, business-related messages. City of Madras will filter email at the Internet gateway and/or the mail server. This filtering will help reduce spam, viruses, or other messages that may be deemed either contrary to this policy or a potential risk to the organization's IT security.

Additionally, SPAM filtering and antivirus software have been implemented to identify and quarantine emails that are deemed suspicious.

Network Vulnerability Assessments

On a semi-annual basis, City of Madras will perform both internal and external network vulnerability assessments. The purpose of these assessments is to establish a comprehensive view of the organization’s network as it appears internally and externally. These evaluations will be conducted under the direction of the Security Officer to identify weaknesses with the network configuration that could allow unauthorized and/or unsuspected access to the organization’s data and systems.

As a rule, "penetration testing," which is the active exploitation of organization vulnerabilities, is discouraged. If penetration testing is performed, it must not negatively impact organization systems or data.

Protection from Malicious Web Sites and Content

Firewalls and related software will provide site blacklisting, geo-blocking, and content filtering to protect against users accessing malicious sites or code. Network traffic will be monitored with anomalies logged and reviewed periodically to identify access to malicious content. Logs will be reviewed regularly to identify new sites to be blacklisted and new categories of content to be filtered.

The City of Madras web site will incorporate application firewalls to guard against content tampering. Configurations will be documented and reviewed regularly.

DETECT (DE)

Definition: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Anomalies and Events

The following logging activities are conducted by the MSSP under the direction of the Security Officer:

- Domain Controllers - Active Directory event logs will be configured to log the following security events: account creation, escalation of privileges, and login failures.

- Application Servers - Logs from application servers (e.g., web, email, database servers) will be configured to log the following events: errors, faults, and login failures.
- Network Devices - Logs from network devices (e.g., firewalls, network switches, routers) will be configured to log the following events: errors, faults, and login failures.

Passwords should not be contained in logs.

Logs of the above events will be reviewed by the MSSP at least once per month. Event logs will be configured to maintain record of the above events for three months.

Security Continuous Monitoring

Anti-Malware Tools

All organization servers and workstations will utilize Microsoft Windows Defender with Windows Advanced Threat Protection (ATP) to protect systems from malware and viruses. Real-time scanning will be enabled on all systems and weekly malware scans will be performed. A monthly review of the ATP dashboard will be conducted by the MSSP to confirm the status of virus definition updates and scans.

City of Madras utilizes Microsoft Windows Defender with Windows ATP to protect mobile devices from malware and viruses.

Patch management

All software updates and patches will be distributed to all City of Madras system as follows:

- Workstations will be configured to install software updates every week automatically.
- Server software updates will be manually installed at least monthly.
- Any exceptions shall be documented.

Port, Protocol, and Services Monitoring

Monitoring will be employed to observe port traffic. Unneeded ports will be blocked. Services will be monitored for abnormal activities. Logs will be reviewed regularly for suspicious activity and the MSSP will make changes as approved by the Security Officer.

RESPOND (RS)

Definition: Develop and implement appropriate activities regarding a detected cybersecurity incident.

Response Planning

The organization's annual security awareness training shall include direction and guidance for the types of security incidents users could encounter, what actions to take when an incident is suspected, and who is responsible for responding to an incident. A security incident, as it relates to the City of Madras' information assets, can be defined as either an Electronic or Physical Incident.

The Security Officer is responsible for coordinating all activities during a significant incident, including notification and communication activities. They are also responsible for the chain of escalation and deciding if/when outside agencies, such as law enforcement, need to be contacted.

Electronic Incidents

This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes to a virus outbreak or a suspected Trojan or malware infection. When an electronic incident is suspected, the steps below should be taken in order.

1. Remove the compromised device from the network by unplugging or disabling network connection. Do not power down the machine.
2. Report the incident to the Security Officer or the MSSP.
3. Contact the third-party service provider (and/or computer forensic specialist) as needed.

The remaining steps should be conducted with the assistance of the third-party IT service provider and/or computer forensics specialist.

4. Disable the compromised account(s) as appropriate.
5. Backup all data and logs on the machine, or copy/image the machine to another system.
6. Determine exactly what happened and the scope of the incident.
7. Determine how the attacker gained access and disable it.
8. Rebuild the system, including a complete operating system reinstall.
9. Restore any needed data from the last known good backup and put the system back online.
10. Take actions, as possible, to ensure that the vulnerability will not reappear.
11. Conduct a post-incident evaluation. What can be learned? What could be done differently?

Physical Incidents

A physical IT security incident involves the loss or theft of a laptop, mobile device, PDA/Smartphone, portable storage device, or other digital apparatus that may contain organization information. All instances of a suspected physical security incident should be reported immediately to the Security Officer.

Notification

If an electronic or physical security incident is suspected of having resulted in the loss of third-party/customer data, notification of the public or affected entities should occur.

1. Contact CIS Claims at claims@cisoregon.org.
2. Inform your attorney

3. Complete this form if the breach involves more than 250 records. https://justice.oregon.gov/consumer/DataBreach/Home/Submit

RECOVER (RC)

Recovery processes and procedures are executed and maintained to ensure timely restoration of systems and/or assets affected by cybersecurity events.

CIS will help with the recovery process. CIS may provide forensics services, breach coaching services, legal services, media services and assist in paying for notification expenses. The CIS claims adjuster will discuss with you the coverages and services offered by CIS.

The Security Officer is responsible for managing and directing activities during an incident, including the recovery steps.

Recovery planning and processes are improved by incorporating lessons learned into future activities.

Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet service providers, owners of the affected systems, victims, and vendors.

External communications should only be handled by designated individuals at the direction of the Security Officer. Recovery activities are communicated to internal stakeholders, executives, and management teams.

Appendix A – Acceptable Use Policy

The intention of this Acceptable Use Policy is not to impose restrictions that are contrary to City of Madras established culture of openness, trustworthiness, and uprightness. Understanding and adhering the organization's IT security policies is necessary to protect our employees and organization from illegal or damaging actions by individuals, either knowingly or unknowingly. Effective security is a team effort involving the participation and support of every employee. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

Purpose

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

Scope

This policy applies to both permanent and temporary employees of the organization. This policy applies to all equipment that is owned or leased by the organization. This policy is a supplement to the *City of Madras Cybersecurity Policy*.

1.0 Policy

The following actions shall constitute unacceptable use of the corporate network. The list also provides a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate network and/or systems to:

1. Engage in an activity that is illegal under local, state, federal, or international law.
2. Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the organization.
3. Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, threatening, obscene or otherwise inappropriate messages or media.
4. Engage in activities that cause an invasion of privacy.
5. Engage in activities that cause disruption to the workplace environment or create a hostile workplace based on a legally protected class.
6. Make fraudulent offers for products or services.
7. Install, download or distribute unlicensed or "pirated" software.
8. Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.

Email

The following activities are strictly prohibited:

1. Using the email system to send or forward pornographic material.
2. Using the email system for any form of harassment whether through language, content,

frequency or size of the message.

3. Sending unsolicited bulk email messages, including the sending of “junk mail” or other advertising materials to individuals who did not specifically request such material (email spam).
4. Sending or forwarding emails of a non-business nature to the “All Employee” list.
5. Sending or forwarding emails of a non-business nature with either an excessive number of attachments or attachments of excessive size (examples would be emails with numerous photos, video clips, or large PowerPoint presentations).
6. Creating or forwarding “chain letters,” “Ponzi” schemes or other get rich quick “pyramid” schemes of any type.
7. Using the email system in a manner that would violate the City of Madras Cybersecurity Policy.
8. Opening file attachments with file extensions such as .vbs, .exe, .com, or .sys.

Social Networking/Blogging

The following applies to social networking/blogging:

1. Employees are discouraged from using employer-owned equipment, including computers, organizationally licensed software or other electronic equipment, or organization time to conduct personal blogging. Social networking activities are discouraged.
2. Employees are expected to protect the privacy of the organization and its employees and are prohibited for disclosing personal employee and nonemployee information and any other proprietary and nonpublic information to which the employees have access.
3. Management strongly urges employees to report any violations or possible violations or perceived violations to supervisors or managers. Management investigates and responds to all reports of violations of the social networking policy and other related policies.
4. Only executive management are authorized to remove any content that does not meet the rules and guidelines of the policy or that may be illegal or offensive.
5. Views of the individual employee are not ever attributed to the City of Madras .
6. Posts must comply with existing policies re harassment and discrimination.
7. Posts must comply with existing policies re confidentiality and improper disclosures.
8. Online activities must not interfere or negatively affect work tasks or City of Madras, except for “Concerted Activities.”
9. Employees must not reference City of Madras or its services in the employee’s social medial posts, except for “Concerted Activities.”
10. City of Madras logos should not be used in the employee’s social media posts, except for “Concerted Activities.”
11. Posts must not violate copyright laws.
12. Consult the Employee Personnel Handbook for further clarification.

Clean Desk

A significant amount of confidential customer information is maintained in paper-based form. All staff members are responsible for ensuring that this information is properly safeguarded and is not improperly disclosed to unapproved third parties. In order to accomplish this, all employees are responsible for:

1. Ensuring that paper-based information is appropriately monitored and protected.
2. Ensuring 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.
3. Maintaining 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. This will help to ensure that confidential customer information is not inadvertently disclosed.

Computer Usage (Password)

The following password criteria will be used to access Windows workstations:

1. Minimum password length: 8 characters
2. Password complexity: requires alphanumeric and special characters
3. Prohibited reuse for twelve (12) iterations
4. Changed periodically every 90 days
5. Invalid login attempts set to three
6. Automatic logout due to inactivity = 30 minutes

Portable Devices

The following Portable Devices are allowed for organization use only:

1. Cell phones
2. Laptops
3. Digital cameras
4. Any type of USB memory device or USB mass storage device

2.0 Monitoring

Employees should have no expectation of privacy for any information they store, send, receive, or access via the organization’s network. Content monitoring of email by management may occur without prior notice. All other monitoring, including but not limited to, internet activity, email volume or size, and other forms of electronic data exchange may occur without prior notice by management.

Monitoring may occur without prior notice of a suspected violation, either in part or in whole, of the Acceptable Use Policy or the *City of Madras Cybersecurity Policy* is detected or reported.

3.0 Reporting

Employees must report to the Security Officer when they learn of a suspected breach of information or have lost a laptop, telephone, or USB memory with City of Madras information.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Signature

I have received a copy of the organization's Acceptable Use Policy as revised and approved by the management. I have read and understood the policy.

____
(Print your name)

___________________________________ ____________________
(Signature) (Date)

Appendix B – Confidentiality and Non-Disclosure Agreement

This Confidentiality and Nondisclosure Agreement (the "Agreement") is entered into by and between **City of Madras** ("Disclosing Party") and _______________________ ("Receiving Party") for the purpose of preventing the unauthorized disclosure of Confidential Information as defined below. The parties agree to enter into a confidential relationship with respect to the disclosure of certain proprietary and confidential information ("Confidential Information").

1. Definition of Confidential Information. For purposes of this Agreement, "Confidential Information" shall include all information or material that has or could have commercial value or other utility in the business in which Disclosing Party is engaged. Examples of Confidential Information include the following:

    - Employee or customer Social Security numbers or personal information
    - Customer data
    - Entity financial data
    - Product and/or service plans, details, and schematics,
    - Network diagrams and security configurations
    - Communications about entity legal matters
    - Passwords
    - Bank account information and routing numbers
    - Payroll information
    - Credit card information
    - Any confidential data held for a third party

2. Exclusions from Confidential Information. Receiving Party's obligations under this Agreement do not extend to information that is: (a) publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party; (b) discovered or created by the Receiving Party before disclosure by Disclosing Party; (c) learned by the Receiving Party through legitimate means other than from the Disclosing Party or Disclosing Party's representatives; or (d) is disclosed by Receiving Party with Disclosing Party's prior written approval.

3. Obligations of Receiving Party. Receiving Party shall hold and maintain the Confidential Information in strictest confidence for the sole and exclusive benefit of the Disclosing Party. Receiving Party shall carefully restrict access to Confidential Information to employees, contractors, and third parties as is reasonably required and shall require those persons to sign nondisclosure restrictions that are at least as protective as those in this Agreement. Receiving Party shall not, without the prior written approval of Disclosing Party, use for Receiving Party's own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of Disclosing Party, any Confidential Information. Receiving Party shall return to Disclosing Party any and all records, notes, and other written, printed, or tangible materials in its possession pertaining to Confidential Information immediately if Disclosing Party requests it in writing.

4. Time Periods. The nondisclosure provisions of this Agreement shall survive the termination of this Agreement and Receiving Party's duty to hold Confidential Information in confidence shall remain in effect until the Confidential Information no longer qualifies as a trade secret or until

Disclosing Party sends Receiving Party written notice releasing Receiving Party from this Agreement, whichever occurs first.

5. Relationships. Nothing contained in this Agreement shall be deemed to constitute either party a partner, joint venturer or employee of the other party for any purpose.

6. Severability. If a court finds any provision of this Agreement invalid or unenforceable, the remainder of this Agreement shall be interpreted so as best to affect the intent of the parties.

7. Integration. This Agreement expresses the complete understanding of the parties with respect to the subject matter and supersedes all prior proposals, agreements, representations, and understandings. This Agreement may not be amended except in a writing signed by both parties.

8. Waiver. The failure to exercise any right provided in this Agreement shall not be a waiver of prior or subsequent rights.

This Agreement and each party's obligations shall be binding on the representatives, assigns, and successors of such party. Each party has signed this Agreement through its authorized representative.

Disclosing Party

By: ________________________________

Printed Name: _______________________

Title: ______________________________

Dated: _____________________________

Receiving Party

By: ________________________________

Printed Name: _______________________

Title: ______________________________

Dated: _____________________________

APPENDIX C – MICROSOFT SURFACE USER POLICY

THE CITY OF
MADRAS
EST. 1910

CITY OF MADRAS
MICROSOFT SURFACE (“SURFACE”) USER POLICY

SECTION 1: GENERAL STATEMENT

The City of Madras (the “City”), by authorizing the acquisition of Surfaces for Council members, recognizes that the provision and use of an Surface will assist Council members in the efficient performance of public duties, provide cost savings to the City, and improve service to the public. By reading and acknowledging this Surface User Policy (this “Policy”), each Council member acknowledges and agrees to abide by the terms of this Policy.

Each Council member has a separate City email account that is used to send official City documents, including, without limitation, agendas, staff reports, and the like. Internet access to this email account will be available through the Surface.

The Surface, internet, and email access will be used primarily for City-related business purposes (i.e., to review agenda materials, research relevant topics, obtain useful information for City-related business, and conduct business communications as appropriate). All of the City’s computer systems, including the Surface, are considered to be public property. Subject to certain limited exceptions, all City-related documents, files, and email messages are considered public records, are subject to Oregon’s Public Records Law, and are considered the property of the City.

Surface users must use the Surface honestly and appropriately on the Internet and when using email, and further agree to respect the copyrights, software license provisions, property rights, privacy, and prerogatives of others, just as in any other business dealings. All existing City email policies (and all other applicable policies, including, without limitation, the City’s Internet policy) will apply to the use of these Surfaces.

Surface email activities will be traceable to the City and will impact the reputation of the City. For this reason, users will refrain from making any false or defamatory statements in any Internet forum or from committing any other acts which could expose the City to liability. Users will not download files from sources which may be untrustworthy nor will users open and read files attached to email transmissions unless they originate from a trustworthy source. Downloaded files and attachments may contain viruses or hostile applications that could damage the City’s systems. Users will be responsible for any breaches of security caused by files obtained for non-City business related purposes.

SECTION 2: DETAILED POLICY PROVISIONS

A. The City has the right but not the duty to inspect any and all files stored on Surfaces in order to ensure compliance with this Policy. Users do not have any personal privacy right in any matter created, received, stored in, or sent from any City Surface and the City Administrator may institute appropriate practices and procedures to ensure compliance with this Policy. The City may track Surface usage. The City reserves the right (from time-to-time or at any time), to intercept, divert, discard, access, or review a Council member’s Surface and its usage. Further, the City reserves the right to disclose the use of any Surface if the City reasonably believes such disclosure is necessary or appropriate, including for the purpose of complying with or assisting law enforcement officials or legal authorities who may, by subpoena, search warrant, or otherwise, seek review of such usage, or for the purpose of litigation or other legal proceedings.

B. The City's Surfaces are intended primarily to be used for legitimate City business reasons with the goal of improving service to the public.

C. The City's IT provider will assist only in the installation of certain basic applications ("apps"), and software that are deemed to be reasonably necessary and appropriate to perform City-related duties. Any software, applications, email messages, or files downloaded by users onto a City Surface become the property of the City, and may only be used in ways that are consistent with licenses or copyrights.

D. Surfaces provided to Council members are Wi-Fi compatible. However, if any user desires to subscribe to a data plan with a cell phone provider, the plan must be purchased by the user.

E. If a user loses or damages the Surface, it must be reported to the City Administrator, or his or her designee, immediately. The user may be responsible for payment of the deductible for repair or replacement of the Surface if such loss or damage was due to negligence or misuse. After a second occurrence of loss or damage, the user is solely responsible for reimbursing the City for the fair market value of the repair or replacement.

F. As discussed above, subject to limited exceptions, email and internet communications related to City business are considered public records subject to disclosure under Oregon's Public Records Law. For this reason, all City-related emails will be generated or received through the City's email system when being accessed on a City issued Surface. This requirement is designed to ensure that all City-related emails will be captured by the City's email retention system.

G. Users will not send any messages of an obscene, libelous, vulgar, and/or defamatory nature. Users will not use any email program or service during any City meeting, and users will not use the Surface in any way as to violate Oregon's Public Meeting Laws.

H. Except as provided under Section 2 K. of this Policy, users will not use City issued Surfaces for non-City related business, including, without limitation, operating a business for personal gain, sending chain letters, soliciting money for religious or political causes, or similar purposes.

I. Users will not use City electronic communications facilities to deliberately propagate any virus or other hostile computer program or file, to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

J. In using the City issued Surfaces, users will identify themselves honestly, accurately, and completely at all times.

K. Incidental and occasional personal use of Surfaces is acceptable, provided such use complies with the following:

- Does not interfere with an employee's or Council member's regular duties or the business of the City.
- Does not result in an incremental expense to the City.
- Is not used for any form of advertising, solicitations, or promotions, commercial or

political purposes.

- Is not used to communicate abusive, profane, or offensive language.
- Is not used for criminal activities.
- Is not used for online gambling websites.
- Is not used for viewing or distributing pornographic or sexually related material.
- Is not used for viewing or distributing material related to the intolerance of a gender, race, ethnicity or religion.
- Is not used for sending or viewing inappropriate material, as outlined in this Policy, through the use of technology (e.g., email, Facebook, Twitter,
  texting, etc.)
- Is not allowed to be used by anyone other than the Council member to which the Surface was assigned.
- The Surface is not used to transmit (a) communications intended to harass or threaten another individual, or (b) sexually suggestive, sexist, racist, ethnic, or otherwise demeaning comments to any individual.

L. Use of Surfaces must be in compliance with applicable federal, state, and local laws, regulations, and ordinances.

SECTION 3: RETURN

Council members will return their Surface to the City Recorder when their term and service for the City of Madras has ended. Subject to applicable law, the Surface will be wiped clean of any and all information upon return of the Surface to the City Recorder at the end of the elected or appointed commission member's term and service. Any public records stored on the Surface that need to be retained will be transferred to an appropriate City computer or storage medium, coordinated through the City's IT provider.

SECTION 4: CONCLUSION

The City has provided Surface, Internet, and email access to all Council members for the purpose of performing work efficiently and effectively in the context of available communication technologies. While compliance with this Policy is mandatory, it should not impede legitimate use of these facilities. The purpose of this Policy is to ensure that all use is consistent with the law and with the ethical and business practices which the City follows.

SURFACE USER ACKNOWLEDGMENT AND AGREEMENT

I, the undersigned, have been provided a copy of the City of Madras Surface User Policy. I have read this policy in its entirety and understand and agree that I must abide by this policy. I acknowledge and agree that my failure to comply with this policy may result in, among other things, my loss of the use of the Surface.

________________________________ ______________________
Signature Date

____
Name (print)

APPENDIX D – TRAVEL POLICY

THE CITY OF MADRAS

EST. 1910

125 SW “E” Street, Madras, OR 97741 Telephone (541)475-2344 - Fax (541)475-1038

Travel Policy

TO: All City departments and staff

PURPOSE: To define the City’s policies, procedures and practice for authorizing official business regarding travel and direct expense reimbursement. The purpose of this policy is to provide a clear understanding of appropriate spending of public dollars for City-related business/travel, as well as the process for ensuring that those operating on behalf of the City are held accountable for such expenses and business conduct. Expenditures regarding travel are open to public review and any misuse or overspending during travel on City business will not be tolerated and could lead to disciplinary action.

I. GENERAL

1. This policy applies to all employees and elected officials (herein referred to as “travelers”) traveling on official City business for the benefit of the City. Temporary or part-time employees are not eligible for travel benefits, except in special circumstances approved by the department head, or when travel is included as a specific job duty described in their job description.

2. Each supervisor or department head is responsible for determining and authorizing the need for, and the method of reasonable travel expenses to be incurred by their traveler.

3. The traveler is responsible for making all travel arrangements (e.g. airfare, hotel, car rental, etc.)

4. The traveler is responsible for keeping accurate and complete cost records including all detailed/itemized receipts and supporting documentation for expenses made on behalf of the City. If a traveler does not have a detailed/itemized receipt, they will need to fill out a Lost Receipt Form to document the expense.

5. Upon returning from travel, proof of attendance is to be provided to the traveler’s immediate supervisor. Proof of attendance may be in the form of an attendance certificate, training book with notes or a copy of the sign-in sheet. The traveler’s supervisor is responsible to notify the traveler and finance if he/she is aware of any reimbursement that is sought by a traveler who has not attended the scheduled event or complied with City policy regarding allowable travel

expenses. If a traveler does not actually make the trip, he/she must report it the following workday.

6. When a traveler is spending public dollars they should consider what a prudent and reasonable person would do spending their own money while traveling. GSA Per Diem meal limits are a good example of individual or daily meal balances for how public dollars should be spent.

7. All travel expenses and reimbursements are subject to audit.

8. Consultants and other contractors shall be exempt from these rules unless it is negotiated or required as part of their contract.

9. In the event grant or contract funds are being used to cover travel costs, defined per diem or travel policies of the individual grant or contract needs to be followed in order to be eligible for reimbursement. The terms of any grant and/or contract defined travel policy will supersede the City's travel policy.

II. TRAVEL RATES

The U.S. General Services Administration (GSA) establishes annual lodging and meal rates. These rates are established based on state and region. This can be found at http://www.gsa.gov/perdiem.

Meal Rates & Reimbursement

1. The City reimburses on direct costs. It is advisable that spending is within reasonable means of the established GSA daily meal rates. GSA establishes these rates for breakfast, lunch and dinner.

2. Travelers will be entitled to pro-rated meal reimbursements (based on the individual meals vs. the daily rate) for single day trips, depending on when they are traveling for business. For example, if traveling mid-day, the traveler would not seek reimbursement for all three meals that day.

3. Under no circumstances are alcoholic beverages subject to the daily meal reimbursements. Alcohol shall always be paid separately from any detailed/itemized receipt that will be turned in to Finance, and at the expense of the employee.

4. Reimbursable gratuities include 15% per meal, and 20% for larger groups automatically imposed with a gratuity.

5. In order to receive a direct reimbursement, detailed/itemized receipts are required to be submitted with an expense reimbursement form, or if paid with the City issued purchasing card it shall accompany the monthly spend report. In the event a detailed/itemized receipt is not available, a detail of what meal was ordered needs to be in writing and signed off by supervisor.

Lodging Rates & Reimbursement

1) Anytime lodging accommodations are booked, it is the traveler's responsibility to request the government per diem rate (unless the event lodging discount is less than the per diem rate). This will require the traveler to show a picture government identification card at check in order for the per diem rate to be applied.

    a) <u>Upgraded Accommodations:</u> Payment shall be authorized for standard lodging (unless upgraded accommodations are necessary due to a medical condition and pre-arranged with HR). Those desiring to upgrade accommodations may obtain them by personally paying the difference at the time the reservations are made.

    b) <u>Booking Arrangements:</u> Hotels shall be booked directly with the servicing hotel (booking via a third party hosting site such as Expedia or Travelocity is not allowed).

In order to receive a direct reimbursement for lodging, detailed/itemized receipts are required to be submitted with an expense reimbursement form, or if paid with the City issued purchasing card it shall accompany the monthly spend report.

III. REIMBURSEMENT REQUESTS

Forms of payment

Travelers have the ability to incur traveling costs either with their City-issued purchase cards (with the exception of mileage which is always processed on a reimbursement basis) or paid on their own with the intent of seeking an expense reimbursement.

Submitting reimbursement requests

Authorized business expenses incurred by an employee or elected official in connection within the scope of their duties on behalf of the City must meet the requirements for deductibility as business expenses under Federal tax law.

Request for reimbursement for authorized business expenses shall be submitted by the traveler on the last working day of the calendar month or sooner if possible, up to 60 days after the incurrence of the expense(s), but in no case can be greater than 60 days from fiscal year end. Request for reimbursement must be submitted using a completed Expense Report. The completed form and supporting documentation must be signed by both the traveler and the supervisor for processing, and accompany all detail/itemized receipts and/or include maps to prove mileage.

Mileage Reimbursement

Mileage expenses will be reimbursed at the current IRS standard mileage rate for approved mileage with an authorized City-related business purpose (www.irs.gov/Tax-Professionals/Standard-Mileage-Rates).

Calculating mileage based on point of origin and destination

1. If a traveler is traveling out of the City of Madras area, mileage needs to be calculated from the point of origin (home) to the event destination if the mileage incurred is less than if the traveler had traveled from Madras (work location) to the event destination. This method only applies if the traveler did not physically report to work that day. (For example, if you live in Culver and report to a training in Bend, and drive straight from Culver to Bend, you would calculate miles from Culver to Bend, and back again.)

2. Calculate mileage to and from Madras (work location) if you report to work that day, or drive through Madras (which serves as point of origin) to the travel destination. (For example, if you live in Warm Springs and typically come in to work or have to drive through Madras (point of origin) to get to the training, then you would calculate mileage only from Madras to Bend, and back again.)

   Please see the HR Officer or Finance Director if there are questions on which mileage calculation is most appropriate for specific event destinations.

In order for mileage to be reimbursed, the traveler will need to provide documentation that supports the mileage claim (i.e. driving directions/map that shows the traveler's beginning and ending destinations that calculates the total number of miles). Travelers have the ability to request mileage reimbursements in advance of their travel; however, if a traveler receives pre-trip mileage reimbursement, and the traveler does not end up traveling, the reimbursement must be returned to the City within five business days.

IV. TRAVEL EXPENSE ALLOWANCES

Transportation Options

Transportation shall be selected from travel options most cost effective to the City. The following considerations are identified by the City as being most economical:

1. Personally - Owned Vehicles: Employees operating a personal vehicle while on City business are required to have a valid driver's license. When a traveler uses their own vehicle for City-related travel, the traveler understands that the traveler's auto insurance serves as the primary insurance in the event of a loss and the City's insurance would be secondary.

   Travelers using personal vehicles for City-related travel are required to have an auto insurance policy in place with coverage limits as required by the State of Oregon to hold a valid driver's license (http://www.oregon.gov/odot/dmv/pages/driverid/insurance.aspx).

2. City-Owned Vehicles: Travelers may utilize a City vehicle when deemed appropriate by the traveler's supervisor. If this form of transportation is utilized, the City vehicle is not

to be used for transporting anywhere that is not directly related to City business (i.e. other social events, shopping, meeting up with family, etc.) City-owned vehicles are not to be transporting traveler's family and friends; City staff and those representing the City are authorized to be commuting in City-owned vehicles only.

3. Commercial Conveyances: This may be deemed most economical to the City when a privately-owned vehicle is deemed inappropriate. This includes use of shuttles, taxis and other public transportation methods. Rental cars are a last option, unless the collective cost of all other modes of public transportation equate to a higher cost than a rental car.

Air Travel

1. Air Fare: Airfare may be deemed necessary due to the traveling distance, and is typically considered if the travel destination is out-of-state.

2. Upgrade Accommodations: Payment shall be authorized for economy class. Travelers desiring to upgrade accommodations on an airline may obtain them by personally paying the difference at the time the reservations are made. If the first class accommodations are necessary due to a medical condition, the fare can be eligible for payment by the City by submitting written documentation to HR in advance of booking and travel.

3. Booking Arrangements: Air travel should be booked directly with the servicing airlines (booking via a third party hosting site like Expedia or Travelocity is not allowable). The airline tickets are the responsibility of the traveler once received and signed for. If tickets are lost by the traveler, it is the responsibility of the traveler to replace them at their own expense (the City will not pay for replacement tickets).

Ground Travel

1. Other Travel Considerations of Personal Benefit to Travelers
   a. In cases where business travel is combined with a vacation trip the meal per diem is limited to the days of work/business travel, which would be incurred. The remainder of the trip is considered annual leave. Additional day(s) parking expenses are the traveler's responsibility and not reimbursable.

   b. Travelers shall, whenever possible, minimize the overall cost to the City when on travel status.

   c. If travel costs are being reimbursed from a third party source the traveler is responsible for invoicing and collection follow-up.

2. Rental Vehicles: All auto rental need to have approval by a traveler's supervisor, unless in emergency situations.

V. LODGING AND MEALS

1. Hotel accommodations will be arranged by the traveler. Daily meal reimbursement rates are identified in Section 2.

2. In most cases where the registration fee provides for meals, a reduction in the daily meal reimbursement rate will be made. In certain circumstances, it may be necessary that a traveler have a meal away from the pre-registered event (i.e. business meeting, networking event off-site, other official business). In these cases, written justification will be needed to prevent a traveler from repayment for the meal. The primary responsibility for adjustments of this nature rests with the traveler's supervisor.

3. No reimbursement shall be made for lodging with friends or family. Additionally, when family or friends accompany traveler, the traveler bears the sole responsibility for expenses incurred on behalf of the family member/friend.

4. Over-night lodging expenses are approved at the discretion of the traveler's immediate supervisor. In most circumstances, when the meeting, training conference, or travel arrangements are scheduled at an early or late hour and the event destination is south of Bend (on Hwy 97), north of Warm Springs (on Hwy 26), or north of Madras (on Hwy 97), overnight accommodations are warranted.

VI. CONDUCT

Travelers who are authorized to travel for, or on behalf of the City are considered to be on official business. While on City business, travelers shall always act in a manner consistent with the highest standards of conduct and in compliance with the City's Personnel Manual (or by the Governance Policies for elected officials).

VII. IMPLEMENTATION AND INTERPRETATION

Intent

Any questions relative to the intent or application of this procedure should be directed to the HR Officer or the Finance Director.

Fraudulent Claims

There are criminal provisions under which severe penalties may be imposed on a traveler who knowingly presents a false, fictitious, or fraudulent claim against the City.

Violations

Any traveler who violates this policy shall be brought to the attention of the Finance Director and/or City Administrator. A violation may result in the traveler being excluded from travel for a period of 90 days unless the severity of the violation warrants additional corrective action with disciplinary measures subject to the City's Personnel Manual and/or Governance Policies.

ACKNOWLEDGEMENT

By signing below, I acknowledge and agree to follow the City of Madras' Travel Policy, revised on 12-6-2017. I agree to be mindful and responsible with use of public dollars when used for my travel accommodations.

_________________________________ ____________________ ____/___/____

Signature Print Date