mCloud

Code of Conduct

Table of Contents

Page

Table of Contents
(continued)

Page

Table of Contents
(continued)

Page

1. mCLOUD'S PHILOSOPHY

1.1. Preface

mCloud conducts its business honestly, ethically, and in full compliance with applicable laws and regulations everywhere mCloud operates.

mCloud's Code of Conduct sets forth standards of conduct for all of mCloud. It covers a range of subjects and applies to all directors, officers, presidents and vice presidents ("Leadership Team"), employees, and independent contractors, (all collectively referred to as "Team Members") setting a clear expectation that the standards be followed in all job-related activities, regardless of business pressures. Adherence to the Code is required of all Team Members and representatives of mCloud. Managers have an added responsibility to lead by example and ensure that the Code is followed in areas under their supervision.

mCloud's Code of Conduct establishes standards for:

- Equal opportunity employment.
- Honest and ethical conduct, including the disclosure and ethical handling of actual or apparent conflicts of interest.
- Compliance with applicable government laws, rules, and regulations.
- Procedures for reporting suspected violations of mCloud policies and applicable government laws, rules, and regulations.
- Procedures for the prompt, effective, and impartial investigation of violations of mCloud's standards.
- Accountability for adhering to this Code of Conduct and other company policies and standards.

The Code is not a substitute for good judgment, nor does it cover every situation a Team Member may encounter. Rather, it is intended to provide guidance on responsibilities and to assist in making the correct business decisions. mCloud requires its Team Members to act in mCloud's best interests within the confines of the law at all times.

Action by a Team Member's immediate family members, significant others or other persons living in such Team Member's household also may potentially result in ethical issues to the extent that they involve mCloud business. For example, acceptance of inappropriate gifts by a Team Member's family member from one of mCloud's suppliers could create a conflict of interest and result in a Code violation attributable to the Team Member. Consequently, in complying with the Code, a Team Member should consider not only his or her own conduct, but also that of his or her immediate family members, significant others and other persons who live in his or her household.

When in doubt, a Team Member should ask his or her manager or a member of the Board of Directors for guidance. Individuals who make good faith reports under this Code or applicable

law(s) will not be subject to retaliation.

Any Team Member or representative of mCloud who violates this Code, including stated legal or ethical responsibilities, will be subject to appropriate discipline, up to and including termination. Non-compliance with certain aspects of the Code may also subject the individual and mCloud to civil and/or criminal liability.

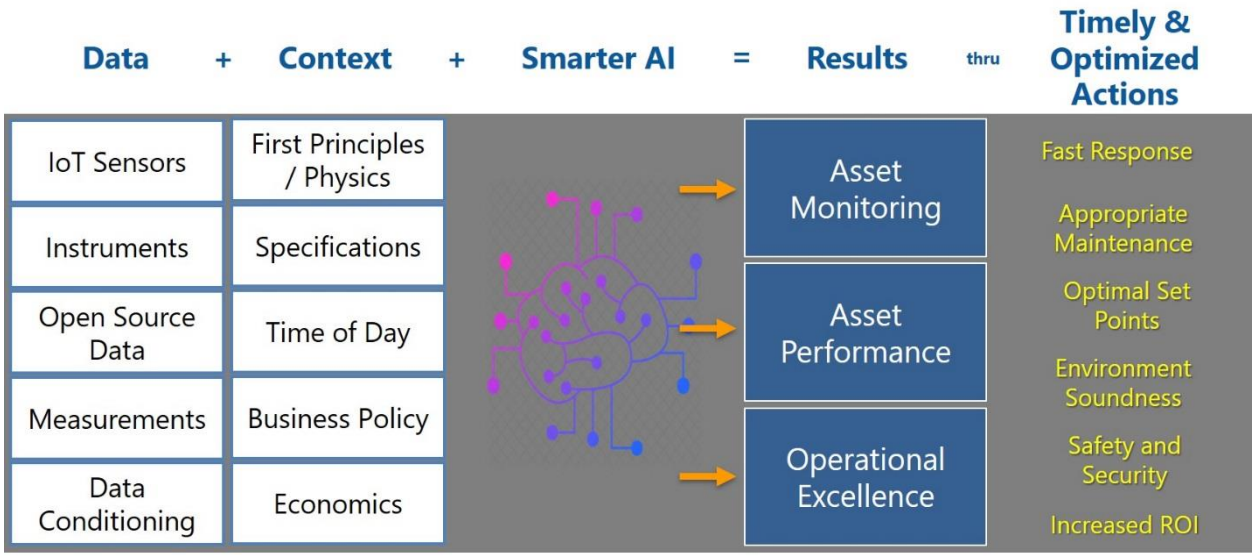
Nothing in this Code of Conduct creates a contract, confers any right to remain in mCloud's employ, or guarantees any fixed terms or conditions of employment. Unless subject to a separate employment contract, a Team Member's employment is at-will, meaning employment is not for a specific time and may be terminated with or without cause and with or without prior notice.

1.2. mCloud's Mission & Vision

Mission: mCloud is an asset management company combining IoT, cloud computing, artificial intelligence ("AI") and analytics to bring together people, data and knowledge to improve the health and performance of equipment.

Vision: mCloud envisions an Asset-Circle-of-Care that includes:

- Machines, devices and sensors that are connected to the cloud
- Real-time and historical data stored in the cloud
- Complex assets that are in need of care and attention
- Context about the assets and real-time data
- Mobile technology that connects people and assets
- AI and analytics that provide guidance for maintenance actions and optimal performance
- Complete engineering and equipment health records including 3D available for each asset
- Real-time collaboration amongst care practitioners and experts



1.3. mCloud's Corporate Values

mCloud's values are to:

- Provide a safe, fun and rewarding work environment
- Enable the best use of valuable asset and natural resources
- Create worthwhile local jobs supported by a global network
- Minimize carbon footprint and contribute to GHG reduction through mCloud's direct actions
- Encourage responsible social behavior from all stakeholders
- Maintain competitive compensation for all stakeholders

1.4. mCloud's Leaders are Responsible for Implementing mCloud's Philosophy

Managers at all levels and the Leadership Team have a special responsibility to engage in ethical behavior and ensure that Team Members under their supervision understand and comply with mCloud's Code of Conduct.

mCloud managers must:

- Understand the Code of Conduct;
- Regularly reinforce and discuss principles set forth in the Code and be available to Team Members to discuss questions and concerns;
- Ensure that Team Members take required trainings on a timely basis;

- Report any complaint of a violation of mCloud's anti-discrimination, anti-harassment, and anti-retaliation policies immediately to the ethics@mcloudcorp.com; and

- Seek guidance from a member of the Board of Directors whenever they have a question about the Code of Conduct.

1.5. mCloud Upholds Honest and Ethical Conduct

mCloud expects its Team Members to conduct themselves ethically, professionally, and with the utmost integrity and transparency in all dealings related to mCloud. The integrity and reputation of mCloud depends on the honesty, fairness and integrity brought to the job by each person associated with mCloud. Unyielding personal integrity is the foundation of corporate integrity. mCloud also expects its business partners, suppliers, and agents to abide by similar values and standards.

1.6. mCloud Complies with Guidelines, Laws and Regulations

Obeying the law, both in letter and in spirit, is the foundation of this Code. mCloud's success depends upon each Team Member's operating within legal guidelines and cooperating with local, national and international authorities. mCloud expects Team Members to understand the legal and regulatory requirements applicable to their business units and areas of responsibility. [mCloud holds periodic training sessions to ensure that all Team Members comply with the relevant laws, rules and regulations associated with their employment, including laws prohibiting insider trading (which are discussed in further detail in Section 3.10 below).][1] While mCloud does not expect Team Members to memorize every detail of these laws, rules and regulations, mCloud wants Team Members to be able to determine when to seek advice from others. If Team Members do have a question in the area of legal compliance, it is important that they not hesitate to seek answers from their supervisor or a member of the Board of Directors.

Disregard of the law will not be tolerated. Violation of domestic or foreign laws, rules and regulations may subject an individual, as well as mCloud, to civil and/or criminal penalties. Team Members should be aware that conduct and records, including emails, are subject to internal and external audits and to discovery by third parties in the event of a government investigation or civil litigation. It is in everyone's best interests to know and comply with mCloud's legal obligations.

2. mCLOUD's EQUAL EMPLOYMENT POLICIES

2.1. Team Members are At-Will Employees

mCloud Team Members are at-will employees, unless the Team Member and mCloud have previously entered into a written employment agreement. That means a Team Member's employment is for an indefinite period of time and it is subject to termination by mCloud or the Team Member, with or without cause, with or without notice, and at any time. Nothing contained in this Code of Conduct should be construed as creating a contract guaranteeing employment for

[1] **Note to mCloud**: To the extent mCloud is not doing so already, we recommend instituting periodic training sessions and distributing the Code annually along with a reminder that mCloud employees need to read, understand and comply with the Code.

any specific duration or any other term or condition of employment. However, to the extent possible, two weeks' notice prior to resignation is requested as a matter of general business practice.

2.2. mCloud is an Equal Opportunity Employer

mCloud treats each individual fairly and makes employment-related decisions based on merit, experience and work-related criteria. mCloud also complies with all applicable laws governing fair employment and labor practices.

As such, mCloud is an Equal Opportunity Employer that does not discriminate on the basis of race, color, religion, sex (including pregnancy, childbirth or related conditions, sexual orientation, gender expression, or gender identity), national origin, ancestry, disability, age, genetic information (including family medical history), military and veteran status, marital status or any other protected categories as defined by federal, state, or local laws.

mCloud makes all of its employment decisions based on legitimate business reasons without any consideration to an individual's race, color, religion, sex (including pregnancy, childbirth or related conditions, sexual orientation, or gender identity), national origin, ancestry, disability, age, or genetic information (including family medical history), military and veteran status, marital status, or any other protected categories as defined by federal, state, or local laws. This policy applies to recruitment and hiring, compensation, benefits, discipline, including termination, and all other terms and conditions of employment.

mCloud also does not discriminate based on an individual's participation in protected activity, such as opposing conduct that the individual believes violates the law or retaliate against individuals in any way.

* If you are located outside of the U.S. or with an affiliate or subsidiary that has its own handbook, contact your Human Resources department for a copy. Regardless of location, mCloud conducts business ethically and in full compliance with the law. We will treat each other with respect and dignity, and foster an atmosphere of open communication, trust and mutual respect.

2.3. Discrimination and Harassment are Strictly Prohibited

Discrimination and harassment based on race, color, religion, sex (including pregnancy, sexual orientation, gender expression, or gender identity), national origin, ancestry, disability, age, or genetic information (including family medical history), veteran status, marital status or any other protected categories as defined by federal, state, or local laws, is illegal, prohibited under this Code, and will not be tolerated. At all times, mCloud Team Members are required to behave in a professional manner and in a way that furthers mCloud's best interests. This policy applies to all mCloud Team Members, contractors, public visitors, customers, and other third-parties whom Team Members come into contact with at work.

2.4. What is Harassment?

Examples of harassment include, but are not limited to: offensive jokes; slurs; epithets or name calling; physical assaults or threats; intimidation; ridicule or mockery; insults or put-downs; offensive objects or pictures; and interference with work performance.

Harassment can occur in a variety of circumstances, including, but not limited to the following:

- The harasser can be the victim's supervisor, or a supervisor in another area, an agent of the employer, a co-worker, or a non-Team Member.
- The victim does not have to be the person harassed, but can be anyone affected by the offensive conduct.
- Unlawful harassment may occur without economic injury to, or discharge of, the victim.

Harassment is unacceptable in the workplace or in any work-related setting outside the workplace, such as business trips, meetings and social events. Team Members are encouraged to inform an individual directly if the individual has acted in an unwelcome way and tell the individual his or her conduct must stop.

2.5. Suspected Discrimination or Harassment Must Be Reported

If a Team Member suspects he or she has been subject to discrimination or harassment, the Team Member is encouraged to report the discrimination or harassment in the following ways:

> If a Team Member suspects that he or she has been subjected to harassment, he or she should immediately report the matter to his or her manager. A Team Member may also contact ethics@mcloudcorp.com to report suspected harassment. If the person toward whom the complaint is directed is one of the individuals indicated above, the Team Member should contact any member of the Leadership Team.

Team Members should report suspected discrimination or harassment at an early stage.

2.6. All Reports of Discrimination or Harassment Will Be Investigated

Every supervisor or manager who learns of any Team Member's concern about conduct in violation of this policy, whether in a formal or informal complaint, must immediately report the issues raised to a member of the Board of Directors.

mCloud will promptly, thoroughly, and impartially investigate any claims of discrimination or harassment. Team Members are required to cooperate with all investigations.

When necessary, based on its investigation, mCloud will provide for prompt, proportional and effective corrective and preventive action to ensure behavior that violates this policy does not continue.

mCloud will protect the confidentiality of Team Members who report discrimination or harassment

or participate in an investigation, to the greatest possible extent. Retaliation against any Team Member who reports discrimination or harassment or participates in an investigation is strictly prohibited. Suspected retaliation should be reported in the same manner a Team Member would report suspected discrimination or harassment. Team Members who violate this policy, including by knowingly allowing discrimination or harassment to continue, may be subject to discipline, up to and including termination.

2.7. Sexual Harassment is Strictly Prohibited

mCloud also prohibits harassment of any Team Member by any member of the Leadership Team, manager, Team Member, customer, or vendor on the basis of sex or gender, including all forms of sexual harassment. Sexual harassment includes unwelcome conduct which is either of a sexual nature or which is directed at an individual because of that individual's sex when: (1) such conduct is made explicitly or implicitly a term or condition of employment; (2) submission to or refection of such conduct by an individual is used as a basis for employment decisions affecting an individual; or (3) the conduct unreasonably interferes with an individual's work performance or creates an intimidating, hostile, or offensive work environment.

2.8. What is Sexual Harassment?

Sexual harassment can occur in a variety of circumstances, including but not limited to the following: unwanted sexual advances or requests for sexual favors; sexual jokes and innuendo; verbal abuse of a sexual nature; commentary about an individual's body, sexual prowess or sexual deficiencies; leering, catcalls or touching; insulting or obscene comments or gestures; display or circulation in the workplace of sexually suggestive objects or pictures (including through email); and other physical, verbal or visual conduct of a sexual nature.

The victim as well as the harasser may be a woman or a man. The victim does not have to be of the opposite sex.

- The harasser can be the victim's supervisor, or an agent or the employer, a supervisor in another area, a co-worker, or a non-Team Member.
- The victim does not have to be the person harassed but could be anyone affected by the offensive conduct.
- Unlawful sexual harassment may occur without economic injury to or discharge of the victim.
- The harasser's conduct must be unwelcome.

2.9. Sexual Harassment is Prohibited No Matter Where it Occurs

Sexual harassment is unacceptable in the workplace or in any work-related setting outside the workplace, such as business trips, meetings and social events. Team Members are encouraged to inform an individual directly if the individual has acted in an unwelcome way and tell the individual his or her conduct must stop.

2.10. Suspected Sexual Harassment Must Be Reported

If a Team Member suspects he or she has been subject to sexual harassment, the Team Member is encouraged to report the harassment in the following ways:

> If a Team Member suspects that he or she has been subjected to harassment, he or she should immediately report the matter to his or her manager. A Team Member may also contact the ethics@mcloudcorp.com to report suspected harassment. If the person toward whom the complaint is directed is one of the individuals indicated above, the Team Member should contact any member of the Leadership Team.

Every supervisor or manager who learns of any Team Member's concern about conduct in violation of this policy, whether in a formal or informal complaint, must immediately report the issues raised to a member of the Board of Directors.

2.11. Suspected Sexual Harassment Should be Reported Early

Team Members should report suspected sexual harassment at an early stage so that mCloud is able to take prompt, proportional and effective corrective and preventative measures to make sure further harassment does not occur.

2.12. All Reports of Sexual Harassment Will Be Investigated

mCloud will promptly, thoroughly, and impartially investigate any claims of sexual harassment. Team Members are required to cooperate with all investigations.

When necessary, based on its investigation, mCloud will provide for prompt, proportional and effective corrective and preventive action to ensure behavior that violates this policy does not continue.

mCloud will protect the confidentiality of Team Members who report sexual harassment or participate in an investigation, to the greatest possible extent. Retaliation against any Team Member who reports sexual harassment or participates in an investigation is strictly prohibited. Suspected retaliation should be reported in the same manner a Team Member would report suspected sexual harassment. Team Members who violate this policy, including by knowingly allowing harassment to continue, may be subject to discipline, up to and including termination.

2.13. Retaliation is Prohibited and Will Not Be Tolerated

mCloud's policy is clear: no one should be discouraged from using any available channel within mCloud to report a concern.

mCloud does not retaliate against individuals and does not tolerate retaliation against any individual for filing a good faith complaint with mCloud or for participating in the investigation of a complaint.

Retaliation prohibited by this policy includes any adverse action taken because an individual reported an actual or perceived violation of mCloud's policies or the law, including, but not limited

to, express or implied threats, denying employment benefits, and other actions that are intended to prevent an individual from reporting harassment, discrimination, or retaliation.

2.14. Suspected Retaliation Must Be Reported

If a Team Member suspects he or she has been subject to retaliation, the Team Member is encouraged to report the retaliation in the following ways:

> If a Team Member suspects that he or she has been subjected to retaliation, he or she should immediately report the matter to his or her manager. A Team Member may also contact the ethics@mcloudcorp.com to report suspected retaliation. If the person toward whom the complaint is directed is one of the individuals indicated above, the Team Member should contact any member of the Leadership Team.

Every supervisor or manager who learns of any Team Member's concern about conduct in violation of this policy, whether in a formal or informal complaint, must immediately report the issues raised to the a member of the Board of Directors.

mCloud will protect the confidentiality of Team Members who report retaliation or participate in an investigation, to the greatest possible extent. Retaliation against any Team Member who reports retaliation or participates in an investigation is strictly prohibited. Team Members who violate this policy, including by knowingly allowing retaliation to continue, may be subject to discipline, up to and including termination.

2.15. mCloud Will Promptly, Thoroughly, and Impartially Investigate All Reports of Suspected Discrimination, Harassment, and/or Retaliation

mCloud will promptly, thoroughly, and impartially investigate any claims of discrimination, harassment, including sexual harassment, and/or retaliation. Team Members are required to cooperate with all investigations.

When necessary, based on its investigation, mCloud will provide for prompt, proportional, and effective corrective and preventive action to ensure behavior that violates the Code does not continue. These actions may include, but are not limited to, counseling, suspension or termination. Anyone, regardless of position or title, whom mCloud determines has engaged in conduct that violates this policy will be subject to discipline under this policy.

mCloud will protect the confidentiality of Team Members who report discrimination, harassment, and/or retaliation or participate in an investigation, to the greatest possible extent. Team Members must cooperate fully in any mCloud investigation and keep their knowledge and participation confidential to help safeguard the integrity of the investigation.

2.16. Reasonable Accommodations Will Be Provided in Accordance with Applicable Laws

mCloud provides reasonable accommodations to applicants and Team Members who may need them for medical (including breastfeeding) or religious reasons, as required by law. If a Team Member believes he or she needs a reasonable accommodation to be able to perform his or her job, the Team Member should contact his or her manager and/or the VP of Talent Development.

mCloud managers are required to respond promptly and effectively to reasonable accommodations requests. In certain circumstances, mCloud may need to request additional medical or religious information or documentation to establish whether an individual's medical condition or religious beliefs are protected by law, or to determine whether and what type(s) of accommodations would be effective. mCloud will keep any medical information received as part of an accommodation request confidential. mCloud will communicate with the Team Member as it determines whether a requested reasonable accommodation can be provided or if another accommodation can be provided.

Retaliation against any Team Member who requests a reasonable accommodation is strictly prohibited.

If a Team Member suspects he or she has been subject to retaliation, the Team Member is encouraged to report the retaliation in the following ways:

> If a Team Member suspects that he or she has been subjected to retaliation, he or she should immediately report the matter to his or her manager. A Team Member may also contact the ethics@mcloudcorp.com to report suspected retaliation. If the person toward whom the complaint is directed is one of the individuals indicated above, the Team Member should contact any member of the Leadership Team.

Every supervisor or manager who learns of any Team Member's concern about conduct in violation of this policy, whether in a formal or informal complaint, must immediately report the issues raised to a member of the Board of Directors.

mCloud will protect the confidentiality of Team Members who report retaliation or participate in an investigation, to the greatest possible extent. Retaliation against any Team Member who reports retaliation or participates in an investigation is strictly prohibited. Team Members who violate this policy, including by knowingly allowing retaliation to continue, may be subject to discipline, up to and including termination.

Team Members who violate this policy may be subject to discipline, up to and including termination.

2.17. Workplace Violence is Prohibited

mCloud has a substantial interest in preventing violence. mCloud prohibits its Team Members from engaging in acts of violence, physical assault, the threat of assault, stalking, or intimidating, aggressive, or threatening behavior while working, representing mCloud, or on mCloud property. mCloud also prohibits the unauthorized possession and/or use of weapons by any Team Member while at work, on mCloud property, or while on mCloud business.

2.18. Workplace Violence Must Be Reported

If a Team Member suspects he or she has been subject to workplace violence, the Team Member is encouraged to report this in the following ways:

If a Team Member suspects that he or she has been subjected to workplace violence, he or she should immediately report the matter to his or her manager. A Team Member may also contact the ethics@mcloudcorp.com to report a suspected violation of the workplace violence policy. If the person toward whom the complaint is directed is one of the individuals indicated above, the Team Member should contact any member of the Leadership Team.

Every supervisor or manager who learns of any Team Member's concern about conduct in violation of this policy, whether in a formal or informal complaint, must immediately report the issues raised to the VP of Talent Development.

2.19. All Reports of Workplace Violence Will Be Investigated

mCloud will promptly, thoroughly, and impartially investigate any claims of workplace violence. Team Members are required to cooperate with all investigations.

When necessary, based on its investigation, mCloud will provide for prompt, proportional, and effective corrective and preventive action to ensure behavior that violates this policy does not continue.

mCloud will protect the confidentiality of Team Members who report workplace violence or participate in an investigation, to the greatest possible extent. Team Members are required to report a suspected violation of the workplace violence policy as soon as possible. Retaliation against any Team Member who reports an incident of workplace violence is strictly prohibited. Suspected retaliation should be reported in the same manner a Team Member would report suspected workplace violence. Team Members who violate this policy may be subject to discipline, up to and including termination.

2.20. mCloud is a Drug-Free, Alcohol-Free, and Smoke-Free Workplace

Drug and alcohol use is highly detrimental to the safety and productivity of Team Members. The unlawful or unauthorized use, abuse, solicitation, possession, transfer, purchase, sale or distribution of controlled substances, drug paraphernalia or alcohol by an individual while conducting mCloud business, representing mCloud, or while on mCloud premises is strictly prohibited. Team Members also are prohibited from reporting to work or working while they are using or under the influence of alcohol or any controlled substances, including substances illegal under federal law, except when the use is pursuant to a licensed medical practitioner's instructions and the licensed medical practitioner authorized the Team Member to report to work.

Smoking, including the use of e-cigarettes, is prohibited on mCloud's premises and while conducting mCloud business.

Violation of this policy may lead to disciplinary action, up to and including termination.

3. TEAM MEMBERS' ETHICAL OBLIGATIONS

3.1. Confidential Information, Trade Secrets, and Intellectual Property Must Be Protected

Team Members must responsibly collect, use, and protect the data and personal information they learn during employment with mCloud.

It is important that mCloud's Confidential Information, Trade Secrets, and Intellectual Property be protected. Team Members may not share mCloud's Confidential Information, Trade Secrets, or Intellectual Property with any third-party during or after employment.

3.2. What is Confidential Information?

Confidential Information includes, but is not limited to information regarding mCloud's finances, pricing, products and new product development, software and computer programs, marketing strategies, suppliers and customers, and potential customers.[2] A Team Member also may become aware of similar confidential information belonging to mCloud's clients.

3.3. What are Trade Secrets?

Trade Secrets are a type of Confidential Information that gives mCloud a competitive advantage. Trade Secrets include, but are not limited to source code, pricing information, strategies, processes, employee compensation, offering plans, and customer lists.

3.4. What is Intellectual Property?

Intellectual Property is information, processes, and technology that gives mCloud a competitive advantage and includes, but is not limited to, computer software and systems, patented inventions, and trademarks.

3.5. Team Members Who Disclose Confidential Information, Trade Secrets, or Intellectual Property May Be Disciplined and/or Subject to Legal Action

It is extremely important that all Confidential Information, Trade Secrets, and Intellectual Property remain confidential, and in particular, not be disclosed to mCloud's competitors. Any Team Member who improperly copies, removes (whether physically or electronically), uses or discloses Confidential Information, Trade Secrets, or Intellectual Property to anyone outside of mCloud may be subject to disciplinary action, up to and including termination. Individuals may also be liable to mCloud for monetary damages for disclosing mCloud's Confidential Information, Trade Secrets, or Intellectual Property.

Team Members also may not use any mCloud logo, trademark, or graphic without prior written approval.

Team Members also may not unethically obtain Confidential Information about competitors, third-

[2]**Note to mCloud:** The definition of Confidential Information used here should be conformed to the definition used in mCloud's standard Proprietary Information and Inventions Agreement (PIIA).

parties, or any other entities, or direct others to obtain Confidential Information. Team Members are required to sign a Confidential Information Agreement before or contemporaneous with beginning employment.

3.6. Conflicts of Interest Must Be Avoided

mCloud respects the rights of its Team Members to manage their personal affairs and investments and does not wish to impinge on their personal lives. At the same time, Team Members should avoid conflicts of interest that occur when their personal interests may interfere in any way with the performance of their duties or the best interests of mCloud. A conflicting personal interest could result from an expectation of personal gain now or in the future or from a need to satisfy a prior or concurrent personal obligation. mCloud expects its Team Members to be free from influences that conflict with the best interests of mCloud or might deprive mCloud of its Team Members' undivided loyalty in business dealings. Even the appearance of a conflict of interest where none actually exists can be damaging and should be avoided. Whether or not a conflict of interest exists or will exist can be unclear. Conflicts of interest are prohibited unless specifically authorized as described below.

If a Team Member has any questions about a potential conflict or becomes aware of an actual or potential conflict, and is not an officer or director of mCloud, such Team Member should discuss the matter with his or her supervisor or a member of the Board of Directors (as further described in Section 7). Supervisors may not authorize conflict of interest matters or make determinations as to whether a problematic conflict of interest exists without first seeking the approval of a member of the Board of Directors and providing a member of the Board of Directors with a written description of the activity. If the supervisor is involved in the potential or actual conflict, the Team Member should discuss the matter directly with a member of the Board of Directors . Officers and directors may seek authorizations and determinations from the [corporate governance and nominating][audit] committee.[3] Factors that may be considered in evaluating a potential conflict of interest are, among others:

- whether it may interfere with the Team Member's job performance, responsibilities or morale;
- whether the Team Member has access to confidential information;
- whether it may interfere with the job performance, responsibilities or morale of others within the organization;
- any potential adverse or beneficial impact on mCloud's business;
- any potential adverse or beneficial impact on mCloud's relationships with its customers or suppliers or other service providers;

[3]**Note to mCloud:** Nasdaq rules require that the Code promote "the ethical handling of actual or apparent conflicts of interest." The changes in this section are recommended best practices, but please confirm you are able to implement these procedures before adopting the Code.

- whether it would enhance or support a competitor's position;
- the extent to which it would result in financial or other benefit (direct or indirect) to the Team Member;
- the extent to which it would result in financial or other benefit (direct or indirect) to one of mCloud's customers, suppliers or other service providers; and
- the extent to which it would appear improper to an outside observer.

Although no list can include every possible situation in which a conflict of interest could arise, the following are examples of situations that may, depending on the facts and circumstances, involve problematic conflicts of interests:

- **Employment by (including consulting for) or service on the board of a competitor, customer or supplier or other service provider.** Activity that enhances or supports the position of a competitor to the detriment of mCloud is prohibited, including employment by or service on the board of a competitor. Employment by or service on the board of a customer or supplier or other service provider is generally discouraged and a Team Member must seek authorization in advance if planning to take such a position.
- **Owning, directly or indirectly, a significant financial interest in any entity that does business, seeks to do business or competes with mCloud.** In addition to the factors described above, persons evaluating ownership in other entities for conflicts of interest will consider the size and nature of the investment; the nature of the relationship between the other entity and mCloud; the Team Member's access to confidential information and the Team Member's ability to influence mCloud decisions. Any Team Member that would like to acquire a financial interest of that kind must seek approval in advance.
- **Soliciting or accepting gifts, favors, loans or preferential treatment from any person or entity that does business or seeks to do business with mCloud.** See Section 3.8 for further discussion of the issues involved in this type of conflict.
- **Soliciting contributions to any charity or for any political candidate from any person or entity that does business or seeks to do business with mCloud**.
- **Taking personal advantage of corporate opportunities.** See Section 3.7 for further discussion of the issues involved in this type of conflict.
- **Moonlighting without permission.**
- **Conducting mCloud business transactions with a family member or a business in which a Team Member has a significant financial interest.** Material related-party transactions approved by the Audit Committee and involving any executive officer or director will be publicly disclosed as required by applicable laws and regulations.

- **Exercising supervisory or other authority on behalf of mCloud over a co-worker who is also a family member**. The Team Member's supervisor will consult with the Human Resources department to assess the advisability of reassignment.

Loans to, or guarantees of obligations of, Team Members or their family members by mCloud could constitute an improper personal benefit to the recipients of these loans or guarantees, depending on the facts and circumstances. All loans and guarantees by mCloud must be approved in advance by mCloud's board of directors or the [corporate governance and nominating][audit] committee.

3.7. Corporate Opportunities Must Be Reported Because They May Create Conflicts of Interest

A Team Member may not take personal advantage of opportunities for mCloud that are presented to or discovered by such Team Member as a result of his or her position with mCloud or through his or her use of corporate property or information, unless authorized by his or her supervisor, the CEO or the [corporate governance and nominating][audit] committee, as described in Section 3.6. Even opportunities that are acquired privately by a Team Member may be questionable if they are related to mCloud's existing or proposed lines of business. Significant participation in an investment or outside business opportunity that is directly related to mCloud's lines of business must be pre-approved. A Team Member may not use his or her position with mCloud or corporate property or information for improper personal gain, nor should Team Members compete with mCloud in any way.

3.8. Care Must Be Given to Avoid Conflicts of Interest in the Exchange of Gifts and Entertainment

Business gifts and entertainment are meant to create goodwill and sound working relationships and not to gain improper advantage with customers or facilitate approvals from government officials. The exchange, as a normal business courtesy, of meals or entertainment (such as tickets to a game or the theatre or a round of golf) is a common and acceptable practice as long as it is not extravagant. Unless express permission is received from a supervisor, the CEO or the [corporate governance and nominating][audit] committee, gifts and entertainment cannot be offered, provided or accepted by any Team Member unless consistent with customary business practices and not:

- excessive in value;
- in cash;
- susceptible of being construed as a bribe or kickback;
- made or received on a regular or frequent basis; or
- in violation of any laws.

This principle applies to mCloud's transactions everywhere in the world, even where the practice is widely considered "a way of doing business." Team Members should not accept gifts or entertainment that may reasonably be deemed to affect their judgment or actions in the

performance of their duties. mCloud's customers, suppliers and the public at large should know that the judgment of mCloud's Team Members is not for sale.

Under some statutes, such as the Foreign Corrupt Practices Act (further described in Section 3.12), giving anything of value to a government official to obtain or retain business or favorable treatment is a criminal act subject to prosecution and conviction. Team Members should discuss with their supervisor or the CEO any proposed entertainment or gifts if Team Members are uncertain about their appropriateness.

3.9. Workplace Relationships Must Be Reported Because They May Create Conflicts of Interest

Personal relationships amongst mCloud Team Members may present an actual or perceived conflict of interest, especially if one individual in the relationship is in a position to make or influence employment decisions regarding the other individual. Team Members are required to report workplace relationships to the VP of Talent Development so that any potential conflicts can be resolved. Team Members should not allow their relationships to disrupt the workplace or interfere with their responsibility to act in mCloud's best interests at all times.

3.10. Insider Trading is Strictly Prohibited

Buying or selling securities while in possession of material nonpublic information ("inside information") violates securities laws.

Inside information is information that is nonpublic, or has been public only a very short time, that a reasonable investor would consider important in making investment decisions. Examples of inside information may include:

- Significant contracts or proposed contracts with customers or suppliers;
- Proposed acquisitions, joint ventures, or divestitures;
- New products or services and regulatory approvals or disapprovals;
- Financial performance; and
- Major product or services announcements.

Insider training is both unethical and illegal. This policy applies both to trading in any stock or other securities based on inside information, including inside information learned about an organization with which mCloud does or might do business and giving inside information to someone else, so the individual can profit from that information by trading in stock or other securities. Both actions by Team Members or Team Members' immediate family or others in the household are strictly prohibited by this policy and applicable laws.

As always, Team Members should use good judgment and should promptly raise any suspected violations of this policy to a manager, the ethics@mcloudcorp.com, or a member of the Leadership Team. Violations of this policy may result in disciplinary action, up to and including termination,

as well as severe civil and criminal penalties.

3.11. mCloud is Committed to Fair Competition

mCloud conducts its business honestly, ethically, and in full compliance with applicable laws and regulations everywhere mCloud operates. As such, Team Members may not have discussions or enter into agreements about competitive matters. Team Members also may not make any promises or agreements that may create an unfair advantage in the market, such as those to fix prices, divide customers, or prevent competitors from entering the market. Pricing, contract terms, and marketing plans should not be discussed with competitors, regardless of how innocent or casual the exchange may be and regardless of the setting, whether business or social.

As always, Team Members should use good judgment and should promptly raise any suspected violations of this policy to a manager, the ethics@mcloudcorp.com, or a member of the Leadership Team. Violations of this policy may result in disciplinary action, up to and including termination, as well as severe civil and criminal penalties.

3.12. Corrupt Practices and Bribery are Strictly Prohibited

Team Members are expected to comply with the applicable laws in all countries to which they travel, in which they operate and where mCloud otherwise does business, including the Foreign Corrupt Practices Act. Therefore, bribery of any kind is not tolerated, regardless of the status of the recipient. Behavior that violates this policy includes directly or indirectly, offering, giving, or promising (or authorizing someone to offer, give or promise) an improper benefit to influence or reward the behavior of someone to obtain or retain a commercial advantage. Payments to secure permits or approvals or to speed up government processes, also known as facilitating payments, are also prohibited. Team Members must ask themselves if an action could be viewed as having an illegitimate purpose before offering, giving, or promising anything of value to any person or receiving something of value. If the action could be viewed as illegitimate, the Team Member must not proceed.

Special consideration must be taken in any activity with public officials. Public officials include:

- Elected or appointed officers or employees or individuals acting in an official capacity for on or behalf of a government or government department, agency, or company that is owned in whole, or in part, by a government;
- Elected or appointed officers or employees of public international organizations; and
- Politicians or candidates for political office

Team Members may not make political contributions on mCloud's behalf or with the expectation of a benefit for mCloud. Team Members must also seek written approval from the CEO before offering or providing anything of value to a public official.

As always, Team Members should use good judgment and should promptly raise any suspected violations of this policy to a manager, the ethics@mcloudcorp.com, or a member of the Leadership Team. Violations of this policy may result in disciplinary action, up to and including termination,

as well as severe civil and criminal penalties.

3.13. Accurate Records and Reports are Important to mCloud

mCloud endeavors to meet its legal, financial, and management obligations in all respects and everywhere mCloud operates.

Accuracy of mCloud's corporate and business records is crucial to meeting these obligations, as well as mCloud's commitment to maintaining investors' trust and meeting its regulatory obligations as a public company. mCloud makes full, accurate and timely financial disclosures as required by securities laws and makes sure all its public statements are honest and accurate.

Team Members must ensure that all communications, records, and reports, are full, fair, accurate, timely, and understandable. Team Members must never misstate facts, omit critical information, or modify records or reports in any way to mislead others, and never assist others in doing so. mCloud also properly maintains and retains the records needed to support its tax, financial, and legal obligations. mCloud requires that:

- no information be disposed of that may be relevant to an investigation or subject to a litigation hold;
- no entry be made in mCloud's books and records that intentionally hides or disguises the nature of any transaction or of any of mCloud's liabilities or misclassifies any transactions as to accounts or accounting periods;
- transactions be supported by appropriate documentation;
- the terms of sales and other commercial transactions be reflected accurately in the documentation for those transactions and all such documentation be reflected accurately in mCloud's books and records;
- Team Members comply with mCloud's system of internal controls; and
- no cash or other assets be maintained for any purpose in any unrecorded or "off-the-books" fund.

mCloud's accounting records are also relied upon to produce reports for mCloud's management, stockholders and creditors, as well as for governmental agencies. In particular, mCloud relies upon its accounting and other business and corporate records in preparing the periodic and current reports that it files with the Canadian regulatory authorities and/or the United States Securities Exchange (the "SEC"). Securities laws require that these reports provide full, fair, accurate, timely and understandable disclosure and fairly present mCloud's financial condition and results of operations. Team Members who collect, provide or analyze information for or otherwise contribute in any way in preparing or verifying these reports should strive to ensure that mCloud's financial disclosure is accurate and transparent and that its reports contain all of the information about mCloud that would be important to enable stockholders and potential investors to assess the soundness and risks of its business and finances and the quality and integrity of its accounting and disclosures. In addition:

- no Team Member may take or authorize any action that would intentionally cause mCloud's financial records or financial disclosure to fail to comply with generally accepted accounting principles, the rules and regulations of the SEC or other applicable laws, rules and regulations;

- all Team Members must cooperate fully with mCloud's [Accounting and Internal Auditing Departments], as well as its independent public accountants and counsel, respond to their questions with candor and provide them with complete and accurate information to help ensure that mCloud's books and records, as well as its reports filed with the SEC, are accurate and complete; and

- no Team Member should knowingly make (or cause or encourage any other person to make) any false or misleading statement in any of mCloud's reports filed with the SEC or knowingly omit (or cause or encourage any other person to omit) any information necessary to make the disclosure in any of mCloud's reports accurate in all material respects.

Team Members are also responsible for keeping the following information accurate and current in SharePoint:

- Mailing address;
- Telephone numbers;
- Name and number of dependents;
- Emergency contact(s);
- Marital status; and
- Citizenship status

As always, Team Members should use good judgment and should promptly raise any suspected violations of this policy to a manager, the ethics@mcloudcorp.com, or a member of the Leadership Team. Violations of this policy may result in disciplinary action, up to and including termination, as well as severe civil and criminal penalties.

4. TEAM MEMBER COMPENSATION AND BENEFITS

4.1. mCloud Fully Compensates Team Members in Accordance with Federal, State, and Local Laws

Team Members are paid semi-monthly for all time worked during the previous pay period. Team Members are responsible for keeping their information up to date. Team Members are required to enroll in direct deposit.

Team Members are paid bi-monthly. Any bonuses awarded to Team Members will be paid within the next pay period. mCloud will make required deductions for Social Security, federal income tax and any other tax and appropriate taxes. These required deductions also may include any court-ordered garnishments.

Any suspected errors in a Team Member's pay or improper deductions must be brought to the

attention of the Chief Financial Officer within two weeks. mCloud will not retaliate against any Team Member who reports suspected issues with compensation.

*If you are located outside of the U.S. or with an affiliate or subsidiary, contact your Human Resources department for a copy of the applicable handbook. Policies and legislation specific to compensation, overtime, expense reimbursement and incentive payments vary between countries and jurisdictions where mCloud conducts business.

4.2. Team Members are Responsible for Recording Their Time Worked

mCloud's policy and practice is to compensate Team Members for their work in compliance with all applicable local, state, and federal laws.

Team Members must record their time worked for compensation and benefit purposes. Altering, falsifying or tampering time records is prohibited and may result in discipline, up to and including termination. Team Members should review their pay stubs for accuracy each pay period and bring any compensation discrepancies to the CFO's attention immediately.

4.3. Team Members May Not Work Overtime Without Permission

mCloud's business needs may require Team Members to work overtime (work in excess of forty hours per week). Team Members may not work overtime without written permission from his or her manager. Working overtime without permission may subject a Team Member to discipline, up to and including termination.

Team Members, who are non-exempt employees as classified by the Fair Labor Standards Act, who work overtime will be paid one and a one-half times his or her normal hourly rate, unless otherwise required by law.

4.4. Insurance

Eligible employees may participate in mCloud's insurance benefits programs, including disability benefits programs. The most up-to-date information on these benefits is found on SharePoint. Questions about benefits should be directed to mCloud's Director of Global Support Services in the USA, and to the VP of Talent Development for team members outside the USA.

4.5. Workers' Compensation Insurance

mCloud provides workers' compensation insurance for its Team Members. It is a Team Member's responsibility to report immediately to his or her manager or the Director of Global Support Services in the USA, and to the VP of Talent Development for team members outside the USA any work-related accident or injury so that the necessary paperwork may be completed. Failure to promptly report an accident or injury may make it difficult to prove that the accident or injury was work-related and may jeopardize the Team Member's eligibility to receive these benefits.

mCloud does not retaliate against any individual in regards to workers' compensation insurance.

4.6. Paid Time Off Leave

mCloud provides leave to its full-time Team Members (employees working an average of at least 35 hours per week) in the form of personal time off ("PTO"), or other leave required by state or local law. A full-time Team Member is eligible for PTO as follows:

- First year of employment -120 hours/15 days annually, at the rate of 10 hours per month
- After five years of employment – 160 hours/20 days annually, at the rate 13.333 hours per month
- After ten years of employment -200 hours/25 days annually, at the rate of 16.667 hours per month
- Or designated in the Team Member's offer of employment approved by the CEO or CFO

Leave is intended to be used in the year it is received. However, Team Members may carry over up to five days or 40 hours per year. Any carry-over PTO must be used in the first 90 days of the new calendar year.

Team Members must submit a written request for time off to their reporting manager as early as possible. Requests for time off will be reviewed at the discretion of the manager. Mangers will deliver approved time off request to payroll@mcloudcorp.com for processing. PTO days may be requested in half or full day increments for exempt staff and hourly increments for non-exempt staff, up to a maximum of five consecutive days off at one time, unless otherwise approved in writing by the Leadership Team. Paid PTO will not be considered hours worked for the purposes of calculating overtime.

mCloud will pay Team Members for earned, but unused, PTO at the end of their employment.

*If you are located outside of the U.S. or with an affiliate or subsidiary, contact your Human Resources department for a copy of the applicable handbook. Policies and legislation specific to Paid Time Off vary between countries and jurisdictions where mCloud conducts business.

4.7. Paid Time Off Leave Addendum (California Employees Only)

mCloud provides leave to its full-time Team Members (employees working an average of at least 35 hours per week) in the form of personal time off ("PTO"). PTO is intended to be used for vacation, personal business reasons and all other reasons required by applicable law. A full-time Team Members is eligible for PTO as follows:

- First year of employment – 120 hours/15 days annually, which is accrued at the rate of 10 hours per month
- After five years of employment – 160 hours/20 days annually, which is accrued at the rate 13.333 hours per month
- After ten years of employment – 200 hours/25 days annually, which is accrued at the rate of 16.667 hours per month

- Or designated in the Team Member's offer of employment approved by the CEO or CFO (accrues on a monthly basis)

PTO accrues at the rates specified above, but is subject to a maximum accrual cap which is equal to 1.25 times the amount the Team Member is eligible to earn annually. The caps are:

- For first year of employment to end of fifth year, 150 hours
- For sixth year through end of tenth year, 200 hours
- For after ten years, 250 hours
- For offers of employment, 1.25 times the annual amount that can be accrued

When a Team Member's PTO bank reaches the maximum accrual cap, the Team Member stops accruing PTO until sufficient PTO is used to drop below the cap. For example, a Team Member who is eligible to earn 160 hours of PTO per year will stop accruing PTO when the Team Member's PTO balance reaches 200 hours.

All accrued but unused PTO carries over into subsequent years. However, PTO is intended to be used in the year it is received. If a Team Member is unable to use the annual amount of PTO that is accrued, the Team Member should discuss the situation with his or her supervisor. Team Members who carry large PTO balances may have time off scheduled for them. Team Members must submit a written request for time off to their reporting manager as early as possible. Requests for time off will be reviewed at the discretion of the manager. Mangers will deliver approved time off requests to payroll@mcloudcorp.com for processing. PTO may be requested in increments of two or more hours or full day for exempt staff and hourly increments for non-exempt staff, up to a maximum of five consecutive days off at one time, unless otherwise approved in writing by the Leadership Team. However, more than 5 days of PTO may be used when required by law, for example, in conjunction with a pregnancy disability leave. Paid PTO will not be considered hours worked for the purposes of calculating overtime.

mCloud will pay Team Members for earned, but unused, PTO at the end of their employment.

4.8. Holidays

Full-time Team Members will receive a day off with pay at the regular rate for each of the following holidays observed by mCloud.

Holidays for United States-based Team Members:

- New Year's Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- Day after Thanksgiving
- Christmas Eve
- Christmas Day

Holidays for Canadian-based Team Members:

- New Year's Day
- Family Day (BC)
- Family Day (AB/SK/ON/NB)
- Good Friday (National except QC)
- Easter Monday (QC only)
- Victoria Day (National except NB, NS, NL)
- Canada Day
- Civic Holiday (AB, BC, SK, ON, NB, NU)
- Labour Day
- Thanksgiving (National except NB, NS, NL)
- Remembrance Day (National except MB, ON, QC, NS)
- Christmas Day
- Boxing Day (ON only)

4.9. Additional Leave Will Be Provided in Accordance with Applicable Laws

mCloud will also provide leave to Team Members who need time away from work for medical or religious reasons, and/or other reasons as required by federal, state, or local law. Team Members' eligibility for additional leave depends, in part, on their state of residence. It is not possible to list every scenario in which mCloud would give additional leave to a Team Member or whether the leave would be paid or unpaid.

However, in all cases, mCloud will not discriminate or retaliate against a Team Member who requests leave.

If a Team Member suspects he or she has been subject to discrimination or retaliation, the Team Member is encouraged to report this in the following ways:

> If a Team Member suspects that he or she has been subjected to discrimination or retaliation, he or she should immediately report the matter to his or her manager. A Team Member may also contact the ethics@mcloudcorp.com to report a suspected violation of this policy. If the person toward whom the complaint is directed is one of the individuals indicated above, the Team Member should contact any member of the Leadership Team.

Every supervisor or manager who learns of any Team Member's concern about conduct in violation of this policy, whether in a formal or informal complaint, must immediately report the issues raised to the VP of Talent Development.

mCloud will protect the confidentiality of Team Members who report discrimination or retaliation or participate in an investigation, to the greatest possible extent. Retaliation against any Team Member who reports discrimination or retaliation or participates in an investigation is strictly prohibited. Team Members who violate this policy, including by knowingly allowing discrimination or retaliation to continue, may be subject to discipline, up to and including termination.

Team Members who violate this policy may be subject to discipline, up to and including termination.

Any questions about leave should be directed to the VP of Talent Development, as soon as possible. Genetic information or medical information received as a result of a leave request will be kept confidential to the fullest extent possible.

4.10. Reasonable Approved Business Expenses Will Be Reimbursed

Team Members will be reimbursed for reasonable approved expenses incurred in the course of business, examples of which include business entertainment, travel, transportation, food, lodging, and food. Team Members must use their best judgment in submitting expenses for reimbursement. All expenses must be submitted through Expensify within two weeks and will be reviewed by the Team Member's manager.

F

4.11. Jury Duty and Witness Leave Will Be Provided in Accordance with State Law

Team Members will be allowed time off to perform such civic service as required by law, including jury duty and serving as a witness in a judicial proceeding. Team Members are expected, however, to provide proper notice of a jury duty summons and verification of their service or a subpoena to appear and testify. Team Members also are expected to keep management informed of the expected length of jury duty or service as a witness and to report to work for the major portion of the day if excused by the court. Team Members will be paid their normal rate of pay during the time they are serving on a jury or testifying pursuant to a subpoena.

Additionally, depending on applicable state law, Team Members who have been victims of serious or violent felonies may take time off work to attend judicial proceedings related to the crime.

mCloud will not discriminate or retaliate against any Team Member for requesting or taking time off to serve as a juror, appear in court to comply with a subpoena or other court order, including serving as a witness in any judicial proceeding, or for crime victims to attend court proceedings.

4.12. Voting Leave Will Be Provided in Accordance with State Law

Consistent with applicable state laws, mCloud will provide Team Members with up to two (2) hours off from work to vote if the Team Member does not have sufficient time outside of working hours to vote in a statewide election. This time off should be taken at the beginning or end of the regular work schedule, whichever allows the most free time for voting and the least time off from work. Wherever possible, the Team Member should notify their supervisor of the need for leave at least three (3) working days prior to Election Day.

mCloud will not discriminate or retaliate against any Team Member for taking time off to vote, in accordance with applicable state laws.

4.13. Military Leave Will Be Provided to Eligible Team Members

If Team Members are called into active military service or enlist in the uniformed services, they will be eligible to receive an unpaid military leave of absence. To be eligible for military leave, Team Members must provide management with advance notice of service obligations unless they are prevented from providing such notice by military necessity or it is otherwise impossible or unreasonable to provide such notice. Provided the absence does not exceed applicable statutory limitations, Team Members will retain re-employment rights and accrue seniority and benefits in accordance with applicable federal and state laws. Team Members should contact the VP of Talent Development for further information about eligibility for Military Leave.

If Team Members are required to attend yearly Reserves or National Guard duty, they can apply for an unpaid temporary military leave of absence not to exceed the number of days allowed by law (including travel). Team Members should give their manager as much advance notice of their need for military leave as possible so that mCloud can maintain proper coverage while Team Members are away.

Team Members whose spouse is a qualified member of the United States Armed Forces, the National Guard, or the Reserves may be eligible to take leave when his or her spouse is home during a qualified leave period depending on applicable state law. Team Members should contact the VP of Talent Development for any inquiries under this policy.

5. GENERAL STANDARDS OF CONDUCT

mCloud Team Members are expected to be top performers in their role and act in mCloud's best interests at all times. It is not possible to list every potential type of conduct that would not be in mCloud's best interests.

However, the following are examples of conduct that would be unacceptable: disparaging or offensive language; rude, discourteous or unbusinesslike behavior; obtaining employment on the basis of false or misleading information; recording conversations, phone calls, images or company meetings with any recording device without prior approval; theft; insubordination; unlawful conduct; excessive absenteeism or tardiness; excessive personal activities during work hours; violation of mCloud's policies; conduct that is detrimental mCloud's business; and damage to mCloud property.

Team Members who are not performing to an acceptable level and/or who exhibit unacceptable conduct may be subject to discipline, up to and including termination.

5.1. Team Members Must Use Communication and Computer Systems Responsibly

mCloud's communication and computer systems, including company-provided cell phones, are intended primarily for business purposes. However, limited personal usage is permitted if it does not hinder performance of job duties or violate any other mCloud policy. This includes the voicemail, e-mail and Internet systems. Users have no legitimate expectation of privacy in regard to their use of mCloud's systems, including personal cell phones and laptops used for mCloud business.

Team Members may not use mCloud's communication and computer systems to view or transmit material and statements that are:

- Illegal, fraudulent or part of an unlawful activity
- Slanderous, libelous and/or defamatory
- Offensive, obscene or in bad taste
- Abusive and/or threaten violence
- Discriminatory, harassing or retaliatory towards mCloud Team Members

Team Members may not use their personal cell phones or laptops for business unless they agree to submit the device to the IT department on or before their last day of employment for resetting and removal of mCloud information. This is the only way currently possible to ensure that all mCloud information is removed from the device at the time of termination. The removal of mCloud information is crucial to ensure compliance with the mCloud's confidentiality and proprietary information policies and objectives.

5.2. Team Members May Not Use mCloud's Systems to Harass, Discriminate, or Retaliate

mCloud's policies prohibiting discrimination, harassment, and retaliation, in their entirety, apply to the use of mCloud's communication and computer systems and use of a personal cell phone or computer for mCloud business. No one may use any communication or computer system, including personal devices, in a manner that may be construed by others as discriminatory, harassing, or retaliatory based on race, color, religion, sex (including pregnancy, childbirth or related conditions, sexual orientation, gender expression, or gender identity), national origin, ancestry, ancestry, disability, age, genetic information (including family medical history), military and veteran status, marital status or any other protected categories as defined by federal, state, or local laws.

No Team Member may access, or attempt to obtain access to, another Team Member's computer systems without appropriate authorization. Team Members must return all mCloud-provided devices at the time of their termination of employment.

Team Members who violate this policy may be subject to discipline, up to and including termination.

5.3. Team Members Must Use Facilities, Equipment and Property Consistent with mCloud's Best Interests

Team Members are expected to exercise care, perform required maintenance, and follow all operating instructions, safety standards and guidelines in performing their duties.

Team Members should notify their Supervisor if any equipment, machines, or tools appear to be damaged, defective, or in need of repair.

Improper, careless, negligent, destructive, or unsafe use or operation of equipment can result in discipline, up to and including termination.

5.4. Team Members Have a Limited Expectation of Privacy in the Workplace

It is important that mCloud Team Members understand that, subject to applicable laws and regulations, mCloud may take the following steps when Team Members access mCloud's network or systems or use any device, regardless of ownership, to conduct mCloud business:

- Access, search, monitor, and archive all data and messages sent, accessed, viewed, or stored.
- Conduct surveillance, search workspaces, review phone records, and search property on mCloud premises.
- Disclose to law enforcement information discovered that indicates possible unlawful behavior without prior notice.

5.5. Team Members May Not Make Public Statements for mCloud

All public inquiries, including media inquiries must be referred to the CEO. Team Members are not authorized to make or approve public statements on behalf of mCloud, unless authorized to do so by a member of the Leadership Team. Team Members also may not provide any information to the media about mCloud off the record, for background, confidentially or secretly.

5.6. Team Members Must Use Their Best Judgment When Using Social Media

mCloud's discrimination, harassment, retaliation, workplace violence, Confidential Information, Trade Secrets, and Intellectual Property, conflict of interest and business ethics, and other policies apply to Team Members' use of social media. Team Members must use their best judgment when using social media.

mCloud's social media policy is designed to limit potential embarrassment to mCloud and its Team Members and to protect the Confidential Information of customers, not limit the free flow of ideas. Communications protected by the National Labor Relations Act and/or other federal, state, or local laws are not covered under this policy.

mCloud Team Members may not:

- post any of mCloud's or mCloud customer's Confidential Information, Trade Secrets, or Intellectual Property;
- post any statements, photographs, video or audio that reasonably could be viewed as disparaging to Team Members;
- share information concerning customers or vendors;
- disclose confidential financial data or other non-public proprietary company information;
- misrepresent the company's product or services or its Team Members on social media;
- participate in social media activity that creates an actual or potential conflict of interest with mCloud;
- disparage mCloud's Team Members, customers, or vendors on social media;
- make negative comments about mCloud's customers or vendors on social media;

- use social media on mCloud equipment during working time unless used for legitimate pre-approved mCloud business;
- post information about mCloud Team Members which could lead to morale issues; and
- participate in social media activity that is discriminatory, defamatory, or libelous

5.7. Suspected Discrimination, Harassment, and Retaliation on Social Media Must Be Reported

If a Team Member suspects he or she has been subject to discrimination, harassment, or retaliation by another Team Member through social media use, the Team Member is encouraged to report the discrimination, harassment or retaliation in the following ways:

> If a Team Member suspects that he or she has been subjected to discrimination, harassment, or retaliation, he or she should immediately report the matter to his or her manager. A Team Member may also contact the ethics@mcloudcorp.com to report suspected discrimination, harassment, or retaliation. If the person toward whom the complaint is directed is one of the individuals indicated above, the Team Member should contact any member of the Leadership Team.

Team Members should report suspected harassment, discrimination, or retaliation at an early stage. Every supervisor or manager who learns of any Team Member's concern about conduct in violation of this policy, whether in a formal or informal complaint, must immediately report the issues raised the ethics email noted above and/or a member of the Board of Directors.

mCloud will promptly, thoroughly, and impartially investigate any claims of harassment, discrimination or retaliation. Team Members must cooperate fully in any mCloud investigation and keep their knowledge and participation confidential to help safeguard the integrity of the investigation.

When necessary, based on its investigation, mCloud will provide for prompt, proportional, and effective corrective and preventive action to ensure behavior that violates this policy does not continue.

mCloud will protect the confidentiality of Team Members who report harassment, discrimination, or retaliation or participate in an investigation, to the greatest possible extent. Retaliation against any Team Member who reports discrimination, harassment, or retaliation or participates in an investigation is strictly prohibited. Suspected retaliation should be reported in the same manner a Team Member would report suspected harassment or discrimination. Team Members who violate this policy, including by knowingly allowing harassment to continue, may be subject to discipline, up to and including termination.

6. POST-EMPLOYMENT POLICIES

6.1. Exit Interviews

mCloud requests that Team Members complete a Confidential Team Member Exit Interview when their employment with mCloud ends. mCloud also encourages Team Members to bring any issues to mCloud's attention during his or her employment.

6.2. Return of mCloud Property

All mCloud property, including, but not limited to, Confidential Information, Trade Secrets, Intellectual Property, keys, security cards, computers, telephones, and files must be returned to mCloud at the end of employment.

6.3. References and Employment Verification

All reference requests and requests for employment verification must be submitted to the HR Department. References provided will be limited to a Team Member's dates of employment and position(s) held. Team Members may not provide references for current or former mCloud Team Members.

7. COMPLIANCE STANDARDS AND PROCEDURES[4]

7.1. Compliance Resources

To facilitate compliance with this Code, mCloud has implemented a program of Code awareness, training and review. Any questions or concerns with respect to potential violations of this Code, contact the ethics email noted above, the VP of Corporate Amin and/or a member of the Board of Directors who will be responsible for:

- investigating possible violations of the Code;
- training new employees in Code policies;
- conducting annual training sessions to refresh employees' familiarity with the Code;
- distributing copies of the Code annually [via email] to each Team Member with a reminder that each Team Member is responsible for reading, understanding and complying with the Code;
- updating the Code as needed and alerting Team Members to any updates, with appropriate approval of the [corporate governance and nominating][audit] committee of the board of directors, to reflect changes in the law, mCloud operations and in recognized best practices, and to reflect mCloud experience; and
- otherwise promoting an atmosphere of responsible and ethical conduct.

A Team Member's most immediate resource for any matter related to the Code is his or her supervisor. He or she may have the information Team Member needs or may be able to refer the question to another appropriate source. There may, however, be times when a Team Member prefers not to go to his or her supervisor. In these instances, a Team Member should feel free to

[4]**Note to mCloud:** This new section contains two changes intended to bring the Code into compliance with Nasdaq's rules, namely (i) "establishing an enforcement mechanism that ensures prompt and consistent enforcement of the code, protection for persons reporting questionable behavior, clear and objective standards for compliance, and a fair process by which to determine violations" and (ii) a "requirement that any waiver of the code for executive officers or directors may be made only be the board and must be disclosed to the shareholders along with the reasons for the waiver."

discuss his or her concern with the VP of Corporate Admin or a member of the Board of Directors[5] [Of course, if a Team Member's concern involves potential misconduct by another person and relates to questionable accounting or auditing matters under the Company's **[Open Door Policy for Reporting Complaints Regarding Accounting and Auditing Matters]**, the Team Member may report that violation as set forth in such policy.][6]

[The EthicsLine, ethics@mcloudcorp.com, a dedicated email address] [is/are] also available to those who wish to ask questions about mCloud policy, seek guidance on specific situations or report violations of the Code. Whether the Team Member identifies himself or herself or remain anonymous, his or her [telephonic or email] contact with the EthicsLine will be kept strictly confidential to the extent reasonably possible within the objectives of the Code.][7]

7.2. Clarifying Questions and Concerns; Reporting Possible Violations

If a Team Member encounters a situation or is considering a course of action and its appropriateness is unclear, the Team Member should discuss the matter promptly with his or her supervisor or a member of the Board of Directors; even the appearance of impropriety can be very damaging and should be avoided.

If a Team Member is aware of a suspected or actual violation of Code standards by others, the Team Member has a responsibility to report it. Such Team Member is expected to promptly provide a compliance resource with a specific description of the violation that he or she believes has occurred, including any information he or she has about the persons involved and the time of the violation. Whether a Team Member chooses to speak with his or her supervisor or with a member of the Board of Directors, the Team Member should do so without fear of any form of retaliation. mCloud will take prompt disciplinary action against any employee who retaliates against such Team Member, including termination of employment.

Supervisors must promptly report any complaints or observations of Code violations to a member of the Board of Directors. If a Team Member believes his or her supervisor has not taken appropriate action, the Team Member should contact the ethics@mcloudcorp.com directly. The Company will investigate all reported possible Code violations promptly and with the highest degree of confidentiality that is possible under the specific circumstances. Neither the Team Member nor the Team Member's supervisor may conduct any preliminary investigation, unless authorized to do so by the CEO or a member of the Board of Directors. The Team Member's cooperation in the investigation will be expected. It is mCloud's policy to employ a fair process by which to determine violations of the Code.

[With respect to any complaints or observations of violations that may involve accounting, internal accounting controls and auditing concerns, under mCloud's **[Open Door Policy for Reporting Complaints Regarding Accounting and Auditing Matters],** the audit committee shall be responsible for supervising and overseeing the inquiry and any investigation that is undertaken.][8]

---

[5]**Note to mCloud not used**

[7]**Note to mCloud:** Consider whether you would like to implement a hotline service.
[8]**Note to mCloud:** Please confirm whether you have a 'whistleblower' policy.

If any investigation indicates that a violation of the Code has probably occurred, mCloud will take such action as it believes to be appropriate under the circumstances. If mCloud determines that an employee is responsible for a Code violation, he or she will be subject to disciplinary action up to, and including, termination of employment and, in appropriate cases, civil action or referral for criminal prosecution. Appropriate action may also be taken to deter any future Code violations.

7.3. Waivers

Any waiver of this Code for executive officers (including, where required by applicable laws, mCloud's principal executive officer, principal financial officer, principal accounting officer or controller (or persons performing similar functions)) or directors may be authorized only by mCloud's board of directors or, to the extent permitted by the rules of Nasdaq, a committee of the board and will be disclosed to stockholders as required by applicable laws, rules and regulations.

8. CONCLUSION

mCloud expects its Team Members to conduct themselves ethically, professionally, and with the utmost integrity and transparency in all dealings related to mCloud. This obligation includes complying with all applicable laws, rules and regulations. This Code of Conduct is only one resource available to Team Members. Team Members are expected to comply with this Code and take advantage of other resources, including training and the availability of mCloud managers, the VP of Corporate Admin, a member of the Board of Directors, and the Leadership Team to answer any questions.

8.1. mCloud May Modify this Code of Conduct

mCloud's Code of Conduct may be amended, altered, or terminated at any time and for any reason.

mCloud

Acknowledgement of Receipt of mCloud Code of Conduct

I acknowledge that an electronic copy of the mCloud Code of Conduct and supplement (if applicable) outlining the policies and procedures of mCloud have been made available to me. I have read the Table of Contents, and I know what kind of information I can find in the Code. I acknowledge that it is my responsibility to read and understand the information contained in this Code and supplement (if applicable) and to follow the policies and procedures of mCloud at all times. If I have any questions, I understand that I should contact my manager or a member of the Board of Directors.

I am aware that mCloud can revise, add or delete any policies, procedures or benefits in its discretion.

I AGREE TO FOLLOW THE POLICIES AND PROCEDURES OF THE COMPANY. I UNDERSTAND THAT, UNLESS OTHERWISE AGREED IN WRITING SIGNED BY AN OFFICER OF THE COMPANY AND SUBJECT TO ANY APPLICABLE LAW, ALL MCLOUD TEAM MEMBERS ARE EMPLOYED ON AN AT-WILL BASIS. THIS MEANS THAT EMPLOYMENT IS NOT GUARANTEED FOR ANY SPECIFIC DURATION, AND MCLOUD RETAINS THE RIGHT TO TERMINATE MY EMPLOYMENT AT ANY TIME, WITH OR WITHOUT CAUSE. NO ORAL REPRESENTATIONS MADE BY A MCLOUD TEAM MEMBER WITH RESPECT TO CONTINUED EMPLOYMENT CAN ALTER THIS RELATIONSHIP. LIKEWISE, NO STATEMENT MADE IN THIS CODE OF CONDUCT IS INTENDED TO ALTER THE AT-WILL NATURE OF EMPLOYMENT WITH MCLOUD OR TO CREATE ANY CONTRACT WITH RESPECT TO THE TERMS OR CONDITIONS OF MY EMPLOYMENT.

Note to Team Members:
As of its issue date, this Code replaces all previously distributed editions. Any policy contained in any previous Code which does not appear in this edition, or is different from the information provided in this edition, is invalid. This Code is the property of mCloud. All information contained within this Code is for mCloud and its Team Members only.

Please sign and date this receipt and return it to the VP of Talent Development.

Signature	Date
Print Name	Date