INFORMATION TECHNOLOGY POLICY

Section 1: Introduction – Purpose, Scope, and Applicability

This Information Technology Policy ("IT Policy") establishes governance and the acceptable use of the Information Technology ("IT") systems of McWane, Inc. ("McWane").

The following terms are hereby defined, and have the following meaning(s), as used throughout this document:

- "Company" shall mean McWane, Inc., its divisions, subsidiaries, and affiliates.
- "Corporate IT" shall mean the IT department operating from the Company headquarters and includes designated teams or team members working under the supervision of Corporate IT personnel.
- "Division" or "Divisions" shall mean all companies operating as part of McWane, Inc., including all divisions, subsidiaries, and affiliates.
- "Division IT" shall include all personnel, employed by Divisions, who are involved with supporting IT systems.
- "Company IT System(s)" shall include all Corporate IT Systems and all IT systems operated by a Division of the Company; and
- "Corporate IT System(s)" shall be further defined as follows:

    - "Network" – all equipment, technologies, applications, or other items used to interconnect systems and personnel at the Company, including that which is used to connect the internal McWane Network to the internet, along with any other technology used for communication between Divisions.

    - "Endpoints" – any desktop or laptop computer, tablet, telephone, mobile device, video display, or the like.

    - "IT Service Delivery Equipment" – includes infrastructure equipment such as servers, routers, switches, controllers, and the like, which are used to provide delivery of technology services to Users across the McWane Network, or any segment of the same; and,

    - "Internet Connectivity" – the world-wide network of technological connectivity that provides communication capabilities and access to outside agencies, business partners, and other organizations, via the McWane Network.

The guidelines and procedures contained herein are intended to provide controls around the access to and the security and ownership of the information and data that may exist in or be transmitted across Company IT Systems.

This IT Policy applies to, and its guidelines and procedures must be followed by all Company employees (or "team members"); it also applies to those agents and 3rd parties who have been afforded credentialed access to Company IT System(s).

Failure to follow this IT Policy may result in termination of any access afforded and/or disciplinary action, leading up to and including termination of employment with the Company. This may also include civil and/or criminal prosecution under applicable federal or state laws.

Corporate IT personnel, along with Division IT personnel, share responsibility for assuring adherence to this overall IT Policy. Corporate IT personnel are responsible for acquiring, developing, implementing, and otherwise setting up and managing common-use IT infrastructure resources across the Company. Senior managers and/or executives in each Division are responsible for the performance of IT resources that are within sole control of that Division. Division IT or other personnel may request the Corporate IT department's help with issues pertaining to stand-alone IT systems and operations, at any time, but such Divisions bear responsibility for the performance and costs of such systems.

This IT Policy may be supplemented by guidelines and procedures in place in Divisions, but such supplements may not contravene or weaken the principles contained in this IT Policy. Each Division must provide the Corporate IT department with a copy of any local supplements promptly, and such supplements may be reviewed for consistency with this policy. Periodic audits of compliance with this policy, as well as audits or reviews of any local supplements to this policy, may be conducted by Corporate IT personnel or their designated representatives from time to time, as may be considered necessary and appropriate. Updated versions of this IT Policy will be distributed and posted, as necessary.

All McWane team members, contractors, consultants, temporary or other workers with access to Company IT Systems (collectively "Users") are expected to follow this IT Policy. It is the responsibility of the Company team member requesting access to communicate this requirement to any 3rd Party Users that may be granted access. Questions about the McWane IT Policy, its application, and how it functions in practice can be addressed to the McWane Corporate Legal Department, or to the McWane Corporate Vice President and Chief Information Officer.

While this policy addresses IT matters, it does not stand alone; this document is developed in conjunction with and considered a part of the Company's overall Code of Conduct Policies, as may be published from time to time by McWane Corporate Legal, Human Resources, or other departments. References to such other policies may be included throughout this document, and users are advised that they must follow the overall McWane Code of Conduct Policies, in addition to the specific guidelines set forth in this IT Policy.

Section 2: Authorized Use and Restrictions on Use

This section provides disclosures and User guidelines and procedures related to authorized use and restrictions on use of Company IT Systems. These items are designed to inform and protect all team members, vendors, and customers, when accessing Company IT Systems.

Preamble:

Access to Company IT Systems is provided primarily for business purposes. Occasional, incidental personal use is allowed, provided that such use is consistent with this IT Policy and does not interfere with an employee's performance of his or her job duties. No user should ever deliberately perform an act that will negatively affect the operation of Company IT Systems.

2.1 No Expectation of Privacy

Users should have no expectation of privacy when using the McWane Network through connected devices. Users should be aware that the data they create on the Company's Network remains the property of Company; as such, users should avoid, where possible, storing or transmitting any of their confidential or sensitive personal information, on or across Company IT Systems.

2.2 Internet and E-mail in the Workplace

The Company supplies Internet access and e-mail capability, as a means of increasing productivity, enabling electronic communications, and transacting business. Internet and e-mail services are provided as required for authorized Users, to aid in performance and fulfillment of job responsibilities.

All Users should be aware that because of becoming an authorized User of Corporate IT Systems, internet and E-mail use may be monitored. The Company reserves it's right to monitor, inspect, and or suspend such use by authorized Users, with or without their knowledge or presence. Users inherently consent, by any such use of the internet and/or E-mail in the workplace, to the Company's monitoring of such use.

Evidence of violations of the Company's Internet and E-mail usage guidelines, which may be discovered during monitoring by the Company, will be reported to the management and/or to the proper Corporate or Division Human Resources Department. The Company reserves the right to take proper action in connection with any violations that may be found.

- Divisions shall use only the E-mail systems, Internet connections and Internet service providers approved of by Corporate IT.

- Corporate IT will implement security protocols and technical controls around E-mail systems and Internet access, to maintain Network security.

- No Division may set up a separate connection to the Internet without the explicit approval of Corporate IT; further, Corporate IT may isolate, disconnect, or take other proper action, related to any such connection(s) which may be or may have been set up by Divisions.

- Users shall not conduct Company business using E-mail accounts other than those issued and authorized by McWane Corporate IT or its Divisions.

    - Use of personal E-mail accounts by team members for purposes of transmitting or receiving Company and/or business-related information is prohibited.

    - Users are prohibited from creating any E-mail forwarding or other automated actions, using their Company-issued E-mail account, which would otherwise send business-related information to any personally controlled E-mail account(s).

    - Corporate or Local IT personnel, and in the Company's sole discretion and without prior notice to users, may inspect E-mail records in McWane's systems for indications of use of personal E-mail accounts by users to conduct Company-related business; in such instances where violations are found, the Company may take actions necessary to block such activity and retrieve, delete, or wipe Company-related business information from those personal accounts and/or devices.

- In addition to guidelines, procedures and applicable restrictions that are, or may be contained in other Sections of this IT Policy, the following explicit guidelines apply to authorized Users, when using Company-provided Internet and E-mail services:

    - Excessive personal use of Company-provided Internet and E-mail services may be restricted or blocked, as considered necessary and appropriate by IT administrators.
    - Users should not use Company-provided internet or E-mail services to conduct gaming or gambling activities.
    - Users should not knowingly send E-mail or access Internet content which may contain illegal or otherwise offensive materials of a graphic nature, such as pornographic, violent, or racist content.
    - Confidential information, related to the Company, should be transmitted to outside parties, via email or the internet, only as necessary, and in all circumstances, should be appropriately protected by Users. All emails containing sensitive, confidential, or proprietary information should be marked sufficiently secure, in a manner that satisfies the confidentiality concerns associated with any such information transmission. The Company may provide secure E-mail messaging tools, and any User should contact an IT administrator for help in protecting confidential information, prior to sending any such information via E-mail or over the Internet.
    - When corresponding with the Company's attorneys on any legal matter, Users should always mark messages to attorneys as "Confidential — Attorney-Client Privilege."

- Users should never try to deliberately circumvent or disable the Internet or E-mail filtering and tracking software used by the Company.

2.3 Telecommunication and Wireless Mobile Devices in the Workplace

All telephones and telephone equipment installed for use at McWane facilities, including voicemail boxes, are the property of the Company. Corporate IT and Division IT personnel are responsible for the installation and maintenance of all telephones and appurtenant equipment, including assignment of telephone number and voicemail accounts. Users are recommended to protect such equipment from damage to the extent possible and must set up proper secure access to their voicemail boxes.

In some instances, McWane may issue Company-owned wireless mobile devices to team members. Under any circumstance, wireless mobile devices that are used to connect to and access data, information, and applications situated in the Corporate IT Systems, must be authenticated, and enrolled as approved devices under the Company's device management platform.

In general, personal use of Company-owned telephone, wireless mobile device, and voicemail services is allowable, but must not interfere with performance of official business or individual job performance. Users are advised that, to protect McWane data, prevent misuse, and follow existing legal obligations, the Company reserves the right to monitor its messaging systems and data created on, received, or transmitted by any telephone or wireless mobile device used to connect to the Company's IT infrastructure. The Company may also modify, or remotely wipe or reset to factory default, any system-authenticated or enrolled mobile device. The Company will provide advance notice, where possible, if a connected device must be wiped. However, it is the User's responsibility to regularly back up content from any such device, so that they do not lose information if a device is wiped.

- In addition to guidelines, procedures and applicable restrictions that are, or may be contained in other Sections of this IT Policy, the following explicit guidelines apply to telecommunication and wireless mobile devices:

    - Users should coordinate with IT personnel, to establish appropriate telephone and/or wireless mobile device service, consistent with the Company's purchasing strategies – including but not limited to, obtaining any roaming or international communication services or such features, which may be required for the individual User's telephone or wireless mobile device to operate appropriately for McWane business purposes.
    - Team members should immediately report any telecommunication or wireless mobile device used for conducting McWane business that is lost, stolen, accessed by unauthorized persons, or otherwise compromised. As such, the Company can assess the risk and, if necessary, remotely wipe all McWane content or the entire contents of the device, which may include User personal content.
    - When asked, users must promptly provide the Company with access to any telephone or wireless mobile device, including in case of any security incident or investigation.

- Users should avoid, where possible, connecting wireless mobile devices to un-secured Wi-Fi networks, particularly when conducting McWane business or transmitting Company information.
- Users should keep wireless mobile device settings (security, content restrictions, passwords, or passphrases, etc.) which are consistent with this overall IT Policy.
- Users should not seek unauthorized access to the telephones, voicemail boxes, or wireless mobile devices of work counterparts, under any circumstances.
- Users are advised to follow all applicable federal, state, or local laws or regulations on the use of wireless mobile devices, particularly when traveling, driving, or using machinery or equipment.

2.4 Social Media in the Workplace

"Social Media" refers to a variety of online resources such as blogs, social networks, chat rooms, messaging services, and/or other internet forums. Examples include Facebook, LinkedIn, X, Instagram, Pinterest, and/or one of the many other internet-based platforms which may be accessed by Users. It is not the intent of the Company to control what Users may post on personal Social Media sites, but all team members are responsible for complying with the Company's ***Code of Ethical Behavior in the Workplace,*** when connected to, or working from Company IT Systems, and/or at its physical facilities, and using Social Media.

In addition, The Company has established a specific policy applicable to all team members, under its overall Code of Conduct policies published by the McWane Legal Department, entitled ***"Social Media Policy."*** Such policy and its pronouncements are incorporated herein, by reference, and none of the provisions of this IT Policy are intended to be contrary.

2.5 General Guidelines on Use of Company IT Systems

The following activities are prohibited:

- Use of Company IT Systems for any purpose which would violate applicable federal, state, or local laws.
- Gaining or trying to gain unauthorized access to any kind of network, service, information, communications or computing facility or resource, by any means.
- Damaging or destroying the integrity of a computer system, or the data or programs stored on a computer system.
- Downloading or installing unauthorized or illegally obtained software.
- Interfering with another User's job responsibilities; and/or,
- Using Company IT Systems to conduct unauthorized commercial, personal, or political activities.

Users should not take actions that reflect negatively on the Company, its personnel, or its operations, or expose the Company to potential legal liability or reputational damage.

Users should be aware that the electronic transfer of certain kinds of materials is illegal and punishable by fine or jail sentence in the United States and elsewhere. The Company will immediately turn over any evidence of illegal conduct on its systems to the proper authorities.

Users who become aware that another User is violating this Policy are expected to notify their supervisor or the proper Corporate or Division Human Resources Department.

This Policy is not intended to restrict communications or actions protected or required by state or federal law.

2.6 End-User Devices

Users may only access Corporate IT Systems using approved end-user devices that support the Company's minimum information security standards. McWane-owned end-use devices should be configured to automatically receive prompt updates and patches, where possible. Users may be denied remote access if they try using non-Company-owned devices to connect to Corporate IT Systems.

All USB-port-connected storage end-user device use (thumb drives, portable hard drives, connected drives, etc.) will be controlled or limited through security software, as configured on all Company servers and workstations, by Corporate IT personnel. In all circumstances, only approved USB-port connected devices shall be acceptable for use.

- All USB-port-connected device use shall be monitored and may be blocked, as considered necessary, to prevent inappropriate or unapproved data transfer or data sharing by users, through the use of such devices; and,
- Any USB-port-connected storage device which has been connected or used by any team member shall be subject to inspection and/or confiscation, at any time and as considered necessary, by an IT administrator.

All USB devices identified as containing Company information, shall be retrieved by, or returned to, a local IT administrator or supervisor, upon termination of any user's affiliation with or employment by the Company; failure to identify and/or return such devices to the Company may result in the Company seeking appropriate remedy, legal or otherwise, as may be necessary, to protect its property and/or its proprietary information from misuse.

2.7 Access Credentials

Each User is assigned a unique User ID and must set up a password or passphrase, as may be needed, to access Corporate IT Systems ("Authorized User(s)"). Passwords and passphrases are considered confidential and should not be shared. Users must immediately inform Corporate IT if they know or suspect that any username/password-passphrase combination has been improperly shared, compromised, or used; and/or, if information security associated with a User ID has been violated in any way.

2.8 Security Associated with End-User Devices and Access Credentials

To the extent not otherwise specifically stated throughout this IT Policy, Company IT administrators (Corporate, local and help desk) should engage in proper security measures when setting up new and/or updating existing Endpoints or Access Credentials on the Company's Network, including but not limited to the following:

- Assure that each Endpoint deployed for use in the Company's Network environment is protected with Corporate-authorized, properly functioning, and configured security software (currently Microsoft Defender, CrowdStrike and/or Airlock).
- Assure that each Endpoint is properly enrolled in the proper Company Device Management System, as such may be specified by Corporate IT from time to time.
- Assure, to the extent practical, that each User ID (team member, consultant, contractor, vendor or otherwise) is added to and kept in the proper Fine-Grain Passphrase or Password Policy security group, as may be existent and applicable for each Division.
- Assure that each User ID is set up and maintained using the principle of least privilege; and,
- Assure, to the extent practical, that each User ID is appropriately enrolled in and has enforced any applicable Multi-Factor Authentication (or "MFA") policy, as may be specified by Corporate IT from time to time.

Users should refrain from downloading, opening, executing, or running unsolicited or unauthorized applications and programs on the Company's IT Networks, Systems or Endpoints.

- Remote desktop, remote access, or remote support software tools (a.k.a. "RAT's"), provide a way for computer users and administrative support staff to share screens, and/or to access the Company's computer Networks or Endpoints from remote locations, and vice versa. These tools also can provide a back door into the McWane and/or Division Network and systems, which could be used for theft of unauthorized access to, and/or destruction of assets. As a result, only Corporate-approved remote desktop, or remote support software, which is monitored and properly configured and controlled by IT administrators, may be used to access the McWane and/or Division Network and associated systems or Endpoints.

Users should exercise caution when opening e-mail attachments contained in communications from unknown senders, as these attachments may contain malware, malicious code, or other information security threats which may cause User compromise. Users should not respond to e-mail or other messages that constitute requests for confidential information, request changes to employees' personally identifiable or banking/direct deposit information, or that request transfers of Company or team member funds, unless they have separately verified the identity of the sender and are certain of the validity of the message's origin and purpose.

Further, Users should take the initiative to be aware of and to strictly follow procedures established by Corporate or Division Accounting, Finance, Human Resources, or other departments, when handling any

information that could be considered the Personally Identifiable Information (or "PII") of a team member, customer, vendor, or other business counterpart.

2.9 Generative Artificial Intelligence ("GenAI") Policy

To the extent that a particular Generative Artificial Intelligence ("GenAI" or "AI") tool has been approved for use, all McWane team members must use such tools in an ethical and responsible manner consistent with the Company's stated information security practices. Team members should prioritize the evaluation of any security risks associated with using GenAI tools and practice strict protection of any Company or personal confidential information when such approved tools are used.

2.9.1 General Principles for GenAI Tool Approval and Use

a. **Use ONLY approved GenAI tools:** McWane team members are allowed to use GenAI tools for Company business that have been vetted and approved by the McWane AI Governance Committee ("AIGC"). Microsoft CoPilot is the default GenAI tool approved for use in the McWane environment and should be the only GenAI tool used by team members unless others are specifically approved under the process described herein. A list of any other GenAI tools approved for use by team members on McWane endpoints or on the Network will be kept, published, and updated by Corporate SharePoint administrators in an appropriate location on the Company intranet.

b. **Use ONLY GenAI tools that are subscribed through Company-controlled accounts:** Subscriptions to GenAI tools intended for work purposes through personally controlled accounts are strictly prohibited. As such, AI-assisted work should be conducted by team members through company-provided, enterprise-grade AI subscriptions that include contractual data privacy protections and 'no-training' clauses, at minimum, and the *use of free or public-tier artificial intelligence tools for work-related tasks should be avoided by all team members*.

c. **Submit Proposals for use of New GenAI tools to the McWane AI Governance Committee:** Team members may submit proposals for use of new GenAI tools, as they may become available for business use. As part of the vetting process, appropriate personnel will be engaged to evaluate the security of any GenAI tools proposed for use. This includes reviewing the tool's security features, terms of service and privacy policy and checking the reputation of the tool developer and any third-party services used by the tool before it can be submitted to the McWane AIGC for approval.

    1. **Governance Principles that Apply to All GenAI Tools Submitted for Use:** Any GenAI tool proposed for use by team members at McWane must be verified to align with the following principles, before submission for approval – fairness (avoids bias), transparency (produces explainable outcomes), accountability (allows for clear oversight and access controls), privacy (protects confidentiality and complies with

privacy laws), security (protects systems from misuse) and human oversight (supports but does not replace human decision-making).

2. **"Free for Use" GenAI Tools:** GenAI tools which do not have sufficient paid or other formal licensing capabilities *will generally be prohibited from receiving consideration for approval by the McWane AIGC*. McWane's Corporate IT and network teams will take steps to ensure that such tools are identified and blocked from use by McWane team members, computers or other devices that are used for business purposes around the environment.

3. **Checklist for GenAI Tool Proposals**: The following analytics or other information must accompany any proposal for use of a GenAI tool:
   - Tool name and vendor (including any website references)
   - Intended use case and business justification (project description or otherwise)
   - Types and sensitivity of data that will be processed
   - Privacy, compliance, and security documentation associated with the tool
   - Risk identification and mitigation plan, if applicable to the tool
   - Terms of service, third-party dependencies, cost, and licensing information
   - Contact information for the proposer and their department

4. **Process for Submission and Review:** Team members seeking approval for a GenAI tool to be used in the McWane environment must submit their proposal including all items in the Checklist for preliminary review to Corporate IT, by email or through the Service Now (Help Desk) portal. Corporate IT will acknowledge receipt of such proposals within 3 business days, review proposals for completeness, seek clarifications as needed, and next steps will be communicated to the proposer to allow for scheduling of consideration by the McWane AIGC at its next regular meeting (generally held every two weeks). If approved, the team member(s) submitting the proposal will be apprised, and the tool will be added to the approved list of GenAI tools maintained by McWane Corporate SharePoint administrators. If denied, reasons and/or recommendations for alternatives will be provided to the proposer.

2.9.2 Security Best Practices must be applied by team members when using GenAI tools:

a. **Protect confidential data:** Team members must not upload or share any data that is confidential, proprietary, or protected by regulation without prior approval from the McWane Corporate Legal Department. This includes data related to customers, team members, and/or any other business partners. Team members must never include sensitive content in queries that use GenAI tools, such as:
   - Personally identifiable information (PII);
   - Personal health information (PHI);
   - Company or Customer Pricing information.
   - McWane-issued user ID's, passwords, or passphrases.

- The Company's intellectual property or trade secrets.
- Other confidential team members, customer, or 3rd Party information.
- Information from documents marked Confidential, Sensitive or Proprietary.
- Strategic information, including questions that might not appear especially problematic but could inadvertently give away strategic organizational plans (Example: Asking the GenAI tool to summarize notes from a meeting during which financial updates and upcoming changes that are confidential are discussed).
- Other non-public Company information that might be of use to competitors or harmful to the Company if disclosed.

b. **Confirm the accuracy of information received:** GenAI tools do not have the ability to recall or cite the specific sources from which their responses are generated. Instead of quoting specific phrases, their responses are constructed based on patterns they have learned from a vast array of sources. This means the responses a team member could receive may not be 100% accurate. Therefore, team members should confirm the accuracy of the information by cross-referencing the reliable sources they would typically use to complete assigned tasks or make decisions, review content for errors and correct any mistakes, and should verify that any response from a GenAI tool that the team member intends to use is appropriate, ethical, not biased, not a violation of any other individual or entity's intellectual property or privacy, and is consistent with Company policies and applicable laws.

c. **Use GenAI tools to enhance, not replace, team members' work: Team** members must not use these tools as a substitute for the unique skills, insights, and decision-making abilities each team member brings to their role. GenAI tools are not a substitute for human judgment and creativity. Team members must evaluate the quality and relevance of the information provided by the GenAI tool and use their own ability and judgment to make informed decisions about what they should include in their work. They must also inform their supervisor if they use generative GenAI tools as part of the drafting or creation of any content that will be published for consumption outside of the Company.

d. **Follow legal and ethical standards: Team** members are expected to follow legal and ethical standards while using GenAI tools. Team members must avoid engaging in activities that may infringe upon privacy or intellectual property rights or violate any regulations or laws. When creating content of any kind, team members must clearly distinguish between their own input and GenAI-generated responses and attribute appropriately when sharing information.

e. **Control access: Team** members should always use a Company-provided user ID for logging into a GenAI tool for business use. Team members must not give

access to GenAI tools outside the Company without prior approval from the proper department or manager and subsequent processes as needed to meet security compliance requirements. This includes sharing login credentials or other sensitive information with 3rd parties. Team members must also apply the same security best practices used for all Company and customer data. This includes using strong passwords, keeping software up-to-date and following the Company's record retention policy.

f. **When in doubt, error on the side of caution: Team** members must always be deliberate and diligent in efforts to protect the Company and the people we serve when using generative GenAI technology.

TEAM MEMBERS MUST NOT:

- Use GenAI tools to make or help make employment decisions about applicants or other team members, including recruitment, hiring, retention, promotions, transfers, performance monitoring, discipline, demotion, or terminations.
- Represent work generated by a GenAI tool as being their own original work; and/or
- Integrate any GenAI tool with internal Company software or programs without first receiving specific written permission from their supervisor and the Corporate IT Department.

2.10 3rd Party Information Security Requirements and Standards

These Information Security standards and requirements shall apply to all 3rd Parties engaged by McWane and/or any of its divisions and/or subsidiaries (collectively, the "Company"). "3rd Parties", as referenced herein, shall include any vendor, consultant, contractor, or other non-employee that seeks to obtain, require, or to be afforded access to any of the Company's networks, systems, and appurtenant Company-owned information and operational technology ("IT" or "OT") equipment.

Per the Company IT Policy, contracts (or service agreements) executed with 3rd Parties for IT or OT-related services should specify any hardware requirements and/or information security standards that are to be met during the performance of any such work for the Company. As such, all 3rd Parties shall, at minimum:

- agree to follow the McWane Information Technology Policy, or any other applicable Company policy, as published and/or revised from time-to-time, and as may be annexed to or made part of any 3rd Party service agreement.
- provide written acknowledgement of receipt of the policies annexed to or made part of any 3rd Party service agreement (including verification of the delivery of same to its employees), along with an appropriately signed non-disclosure agreement.

- agree to any required background checks (conducted on the 3rd Party entity or its employees), as the Company may consider appropriate.
- accommodate, promptly, the inspection or audit of all computing hardware or software that is proposed to be used by the 3rd Party, prior to and/or during the performance of work for the Company.
- agree to maintain and routinely patch and/or update any computing hardware or software to be used by the 3rd Party in connection with the performance of work for the Company.
- agree to follow all information security standards for network and/or systems access, as may be specifically prescribed by the Company, including but not limited to:
    - network and/or system authentication specifications.
    - 3rd Party or employee identity specifications.
    - user credential use and protection specifications.
    - information and/or data protection and privacy requirements; and/or,
    - information security training or awareness requirements.
- Upon request, complete a written security questionnaire signed by an authorized employee of the 3rd Party, and agree to keep and provide evidence of compliance with all information security standards which may be specifically prescribed by the Company for the 3rd Party.
- agree to promptly notify the Company of any security incident or breach caused by the 3rd Party, and which may affect the Company.
- agree to work in cooperation with the Company to mitigate any adverse impacts (including financial) resulting from a security incident or breach caused by the 3rd Party; and,
- agree to follow any document preservation and /or litigation hold notice(s) which may be issued by the Company, if needed.

Section 3: Information Security and Data Management

3.1 Information Security Operations

Corporate IT will manage information security ("InfoSec") operations across Company IT Systems. As such, Corporate IT will provide guidance on information security practices, manage InfoSec and other cyber-security training and education initiatives, assign system security roles, review InfoSec operations systems logs, review systems hardware, and/or software implementations with Division personnel, and continuously monitor the overall InfoSec operations of the organization. Corporate IT may also perform other periodic analyses of the security posture of the Company's IT Systems as may be found appropriate.

Senior managers and executives in each Division are responsible for ensuring that their division follows the Company's overall InfoSec practices, as may be defined from time to time, by Corporate IT.

All McWane team members are responsible for being aware of and following InfoSec policy, standards, and procedures to help protect information from unauthorized access, use and dissemination, both

inside and outside the Company. McWane team members who suspect or see any violation of the Company's InfoSec standards, notice anything which could be a possible breach of information security, or become aware of unauthorized parties seeking access to Company IT Systems, data or information, should notify their supervisor(s) and/or local or Corporate IT personnel immediately.

Under no circumstance is an established corporate InfoSec standard or practice to be circumvented by any User or 3rd Party acting on their behalf.

3.1.1 IT System, Network, and/or Cloud Information Security Practices

All IT or other designated personnel of the Company, whether Corporate or Division, shall work in accordance with the following basic practices and guidelines, when and where feasible, in conjunction with the ongoing management of information security operations related to the Endpoints, Networks, Internet Connectivity and cloud computing environs that make up Corporate IT Systems:

- IT administrative privileges, whether global, regional, local or otherwise, will be routinely monitored, reviewed and adjusted accordingly, to provide Users with appropriate and secure access to Corporate IT Systems; specific IT administrative privileges may be added to, changed or revoked for any User, as determined necessary, and at any time, by Corporate IT.
- Unnecessary services, applications, and/or network protocols should be identified and removed promptly by proper IT personnel.
- IT administrators shall always exercise their job responsibilities and keep proper separation of duties, where practical and workable.
- Company IT System access controls shall be implemented and monitored, and where possible, appropriate firewall rules and network segmentation shall be set up to provide layers of information security throughout.
- Use of cloud computing services, obtained on behalf of or used by the Company, shall be closely monitored, secured, and controlled by authorized IT personnel, to the extent possible.
- Only Company-approved anti-virus, malware, scanning, data loss prevention or other advanced information security and threat protection tools and/or software, shall be installed on devices connecting to or used throughout the Corporate IT System; and,
- Wireless, remote, Virtual Private Network or other connectivity tools (“Wi-Fi,” “VPN,” and/or similar system elements) shall be monitored and secured, when used to provide access into the Corporate IT System.

3.1.2 Operational Technology (“OT”) Security Principles

Operational technology (“OT”) refers to software and hardware that controls physical devices, machinery, events, and/or other processes conducted by Divisions which manufacture products around the McWane environment. Since OT assets may be directly connected to, or rely upon the McWane

Network and associated Endpoints, safeguarding the technology central to operations is an important facet of OT security best practices.

As such, designated personnel of the Company, whether Corporate or Division, shall operate by the following basic practices and guidelines, when and where possible, in conjunction with the ongoing management of McWane and its Divisions' OT assets:

- Physical and digital locations of all OT devices should be mapped, and connectivity capabilities verified as legitimate and controlled by authorized personnel.
- Every person, device, application, and/or network should be confirmed as legitimate before being allowed to connect to any of McWane's or its Divisions' OT assets. Appropriate security software settings should be deployed for purposes of managing such connections, whether one-time or on an ongoing basis, and an acceptable form of Multi-Factor Authentication ("MFA") should be used in conjunction with setting up such connections.
- Ensure that default connection settings and/or passwords that are embedded in OT assets, when deployed at a McWane Division location, are changed to be unique to that asset, as may be possible.
- Ensure that any team member or other person requiring access to any OT asset are granted access on a least-privilege basis and that identities, credentials, and passwords/passphrases used, along with multi-factor authentication enforcement, are reviewed routinely for prompt adjustment or termination, as may be necessary; and,
- Ensure that all OT asset software or firmware is maintained, updated, and/or patched to address any known security vulnerabilities, as may be necessary and appropriate.

3.1.3 Information Security Training and Awareness Program

Corporate IT shall coordinate the delivery of information security training and associated newsletters and other awareness materials throughout the organization. All executives, management, team members, contractors, vendors, and/or other personnel, who have been provided with E-mail access to Corporate IT Systems, will be provided with information security training and awareness materials. Information security training will be provided by Corporate IT on at least a quarterly basis, and all Users must engage in and complete any assignments that may be issued through the McWane Information Security Training Platform. Any User who does not complete information security training assignments promptly will be subject to having their external email or system access privileges suspended or terminated.

Divisions may be engaged to help develop and/or provide input and materials for use around the organization, for the purpose of promoting and raising information security awareness throughout the Company. Divisions may also conduct supplemental information security awareness or training exercises, as considered appropriate by local IT or other management personnel.

3.2 Confidential and Proprietary and Personal Information Management

The Company has established a specific policy applicable to all team members, under its overall Code of Conduct policies published by the McWane Legal Department, entitled ***"Confidential and Proprietary Information and Intellectual Property."*** Such policy and its pronouncements are incorporated herein, by reference, and none of the provisions of this IT Policy are intended to conflict with that policy.

All personal data handled by team members shall be subject to the requirements of the ***"Personal Data Protection Policy,"*** established as part of the Company's overall Code of Conduct, and published by the McWane Legal Department. Such policy and its pronouncements are incorporated herein, by reference, and none of the provisions of this IT Policy are intended to conflict with that policy.

Section 4: IT Assets, Protection and Management

4.1 Networks, Centralized Data Center, and Hardware

4.1.1 Networks

Corporate IT will implement, manage, and support any network infrastructure used to connect Corporate IT and Division IT equipment. This includes computer and telephone networks, as well as remote access networks and technologies to be used by McWane team members when travelling or away from their Division office.

Corporate IT will provide guidance for the purchase and procurement of Network-connected infrastructure equipment. Divisions connected to Corporate IT Systems are responsible for ensuring that all equipment connected meets standards that may be published, from time to time, by Corporate IT. Divisions are also responsible for the costs associated with accessibility and interconnections to the Corporate IT System.

4.1.2 Centralized Data Center(s)

Corporate IT will manage and support centralized IT data center(s) that provide hosting of applications, data storage, data backup, disaster recovery, or other IT-related services and equipment. Such facilities are available for use by all Divisions. Such data centers will be kept in one or more physical locations. Corporate IT may charge costs back to Divisions, related to maintenance and usage of centralized IT facilities.

4.1.3 Hardware

Corporate IT provides standards and a published catalogue for all hardware and equipment that is approved to be connected to Corporate IT Systems. Any exceptions in hardware types or standards must be documented, and Corporate IT should be notified of such exceptions, prior to equipment being

purchased, installed, and/or connected. All connected hardware should be documented following Section 4.2 of this policy.

Contracts with 3rd Party vendors and service providers should specify hardware requirements and security standards to be met, as part of any applicable agreement or purchase order.

Unless otherwise provided for in this IT Policy, or as exceptions may otherwise be provided for, privately-owned hardware should not be connected to Company IT Systems. Guest access to Company IT Systems may be supplied for visitors as needed. All guest hardware connections are to be temporary in nature unless an exception has otherwise been provided for by the properly authorized Corporate IT or Division IT personnel.

4.2 Protection and Management of IT Assets

All IT equipment should be protected from unauthorized access and physical harm to the maximum extent possible. IT Service Delivery Equipment (servers, routers, switches, etc.) require a higher level of physical protection, and to the extent possible, access to such Company IT System equipment should be restricted to only those persons with IT responsibilities, 3rd parties needing access to perform work on behalf of Company IT personnel, and/or authorized Corporate IT or Division IT personnel.

To the extent possible and practical, computer rooms, data closets, equipment racks, and other enclosures containing IT equipment should be protected against environmental threats of fire, flood, power failure, excessive temperature, humidity, or other threats, as may be found necessary by Corporate IT or Division IT personnel. The owner of the facility containing said rooms, closets, racks, and enclosures is responsible for providing such protection and notifying the proper IT personnel of deficiencies that need remediation.

Any IT asset (physical or software) which is owned or used to conduct Company business, shall be inventoried and tracked by appropriate and authorized IT personnel, using identification conventions consistent with guidance which has been or may be provided by Corporate IT.

When disposing of any IT asset, all applications, and data including any sensitive material, must be removed prior to disposal, and in a manner that prevents any type of recovery. Any media storing confidential or personally identifiable information (PII) that is not being internally re-purposed should be physically destroyed prior to disposal.

Disclosure of McWane proprietary or collateral-proprietary information to unauthorized parties, either intentional or unintentional, must be reported to Corporate IT, such that action can be taken to review the disclosure and identify if any follow-on remediation efforts or actions are necessary.

All email, documents, data, system logs, and associated information, whether contained on physical devices or associated with cloud computing services, and regardless of whether located on Company IT

Systems or Corporate IT Systems, shall be subject to the requirements set forth in the ***"Records Retention Policy"***, established as part of the Company's overall Code of Conduct, and published by the McWane Legal Department. Such policy and its pronouncements are incorporated herein, by reference, and none of the provisions of this IT Policy are intended to conflict with that Policy.

4.2.1 Patch Management

Corporate IT will coordinate responsibilities with Divisions, ensuring that security or other recommended patches and updates are installed for all hardware, firmware, and software, as needed. Devices not directly connected to the Corporate IT System should be periodically updated and maintained by Division IT personnel, either through automated controls or by employing manual procedures.

When possible, and where practical, all hardware, firmware or software security vulnerability patches should be applied, generally within thirty (30) days of release. Any exceptions should be documented by Divisions, and any remaining unpatched or out-of-date hardware or software should be protected by compensating controls.

Corporate IT, along with Division IT personnel, shall coordinate all patching processes, as practical and as necessary, and work to resolve identified issues and/or implement proper mitigation measures, until any identified issue is fully resolved.

Local IT administrators or Users may be requested to reboot workstations or servers, as found necessary by Corporate IT, to facilitate receipt of proper updates and/or patches to such machines. Any workstation or server, used for connection to the Corporate Network may be restricted or disabled, temporarily or permanently, through Corporate IT security controls, if such equipment is determined to be lacking appropriate software, security or other updates and/or patches, OR, if a User has not appropriately connected their workstation to the Network in order to receive timely updates.

4.2.2 Vulnerability Scanning and Resulting Management

From time to time, Corporate IT may authorize internal vulnerability testing, scanning or external system penetration testing, on its own, or with the help of a 3rd Party service provider. Any vulnerability scanning, testing tools and/or resources, are not to be used or deployed by any IT personnel, without the prior knowledge and approval of the proper Corporate IT personnel.

All new IT hardware, software or firmware assets should be scanned, evaluated, or otherwise confirmed, with proper documentation, so that no vulnerabilities exist, prior to such assets being placed into service as part of Company IT Systems.

Section 5: Identity and Access Management

Corporate IT, and/or authorized Division IT personnel, shall be responsible for creating, securing, and maintaining User login accounts for access to all systems.

Only Corporate IT personnel may create or grant IT administrator-level access to any User login accounts contained within the active directories of either Corporate IT or Division Systems.

Every Authorized User is responsible for:

- Keeping passwords and/or passphrases private.
- Reporting a general breach of security to their immediate supervisor, the Corporate IT department, and/or to their local IT administrator.
- Changing their password or passphrase immediately if it has been compromised, is suspected of having been compromised, is disclosed to another individual, or may be directed by Corporate IT.
- Never use another individual's logon ID or password/passphrase.
- Avoiding, when possible, writing down passwords and passphrases, and/or storing or posting them in plain sight; and,
- Ensuring that they are logged out of all Systems, or that their workstation and/or other devices used for System access are locked whenever such devices are left unattended.

The following guidelines and/or procedures shall apply to all Company-authorized User accounts:

- Unique login IDs (in whole, may be referenced in this document as "User Credentials" or "Credentials") are required for each authorized User.
- Passwords and/or passphrases are required for all Users and must be set up as part of any User Credential. Such passwords or passphrases are to be set up, updated, changed, or reset, following systematically enforced standards, as they may be published and/or imposed, from time to time, across Company and/or Corporate IT Systems.
- In general, all team members, contractors, shared, administrator, vendor or other account credentials used interactively to login to McWane or its Divisions Network, Endpoints or systems, should be subject to the most restrictive and highest available level of password or passphrase protection prescribed by Corporate IT. In addition, where possible, service accounts used interactively should also be made subject to the same standards.
- Generic or shared User Credentials or accounts should be readily identified as such, limited to only those necessary, and in all instances, set up only after approval by authorized IT personnel has been obtained.
- For any User to gain remote access to Corporate IT Systems, VPN technology and/or multi-factor authentication ("MFA") will be required to access computing equipment, servers, or other Corporate IT environs. In such instances, Users will be provided with specific instructions and proper VPN or MFA credentials, as may be found necessary, to initiate workable local or remote connections.

- All vendor-supplied and any other default passwords must be changed before any computer, device or other communications system is connected and used for business purposes; similarly, passwords or passphrases must be changed when an IT administrator or contractor who has knowledge of such items, leaves or is reassigned.
- User Credentials or accounts should be disabled, as soon as reasonably possible, whenever an authorized User resigns, is terminated, or otherwise leaves employment with the Company or one of its Divisions.
- The active directory (or directories) and details associated with all User Credentials and accounts contained therein, as used to access any Company or Corporate IT Systems, are to be kept in a complete, consistent, orderly, and up-to-date manner, by Division IT personnel.
- From time-to-time, Corporate IT personnel may conduct audits or reviews of active directory (or directories), and require structural adjustments to such, as may be necessary, to facilitate ready identification and reporting of Division-level Users, User groups, and/or other details related to such User Credentials contained therein.
- All credentialed account permissions should be restricted to provide the least privilege functionality necessary.
- All credentialed accounts should be reviewed routinely for continuing validity, and accounts inactive for longer than 90 days should be disabled and set for deletion, unless otherwise determined by an IT administrator.
- Any User Credentials remaining in active directory (or directories), and which are identified as unused for any period longer than 120 days, shall be confirmed by Divisions for continuing need or otherwise may be removed by Corporate IT personnel.
- Where possible, accounts should have a specific expiration date established.
- For all accounts, the "employeetype" field in active directory should be populated, as possible, using one of the following acceptable values:
    - "TeamMember"- for accounts created and assigned to an individual employee.
    - "Shared"- for accounts created only as necessary, and to support multiple users sharing the same identity; all sharing users should be documented, specified, and kept current, for any such account.
    - "Service" – for accounts created when necessary and used for systems or applications to authenticate without any association to a specific individual.
    - "Contractor" – for accounts created and assigned to an individual that is working on behalf of McWane or its' Divisions for a defined period and needs access to systems to perform their assigned duties.
    - "Vendor" – for accounts created and assigned to a Vendor that is working with McWane or its Divisions. These accounts may be shared, with proper documentation, by designated employees of that Vendor; or,
    - "Admin" – for accounts created and assigned only to authorized personnel, as may be needed to perform their job duties and responsibilities.
    -

5.1 3rd Party Account Creation and Access Controls

The following guidelines shall apply to all Company-authorized 3rd Party system access credentials or accounts which are created for use:

GENERAL GUIDELINES RELATED TO 3RD PARTY ACCOUNTS

- 3rd Parties ("Party" or "Parties"), as referenced herein, shall include any vendor, consultant, or other non-employee that seeks to obtain a credential for access to the Companies' networks and/or appurtenant Company-owned technological equipment.
- Prior to making a request for system access to be established for any 3rd Party, a Company authorized team member (sponsor or supervisor) must conduct Visual Compliance screening on the 3rd Party and any of its delegates AND obtain a signed Non-Disclosure Agreement ("NDA") AND/OR a signed Acknowledgement of Receipt and Applicability of this IT Policy, from an authorized agent of the 3rd Party which specifies, at minimum:
    - the legal name and address of the 3rd Party (company name).
    - the contact's name, title, email address, work, and mobile telephone numbers of the person who is named to receive notices on behalf of the 3rd Party; and,
    - the identity of any person or persons associated with that 3rd Party for which specific access to Company systems will be provided; and,
- At least 15 days prior to the commencement of any work to be performed by any 3rd Party through systems access, a Company authorized team member must submit a fully completed help desk ticket specifying the 3rd Party individual or individuals for which user access account(s) will be created. The Company authorized team members (sponsor or supervisor) approving the help desk ticket request for any 3rd Parties' access, shall be recorded and displayed in active directory in a suitable field, as part of that 3rd Party's account details.

GUIDELINES FOR IT ADMINISTRATORS RELATED TO 3RD PARTY ACCOUNTS

- 3rd Party system access credentials or accounts issued by McWane are also subject to the following limitations:
    - such accounts created for use on McWane systems shall not be valid beyond 120 days from the date of creation, and shall by default, expire and become disabled, absent a supervisor request for extension beyond 120 days; supervisor requests for extensions to such accounts shall not be granted for longer than 120 days at a time.
    - such accounts may not be shared by multiple individuals or 3rd Parties.
    - such accounts must use the VEN.FIRSTNAME.LASTNAME @divisionname.com naming convention.

- such accounts will only be allowed up to F3 Microsoft Office 365 licensing, unless otherwise justified by the supervising team member of such 3rd Party.
- such accounts will be forced to follow McWane's Corporate password, passphrase, remote access, VPN, and/or Multi-Factor Authentication (MFA) requirements, upon creation; and,
- such accounts may only be used through secure remote connections, when necessary, using McWane-approved software which has been installed and configured on the 3rd Parties' computer.

- When any 3rd Party with McWane systems access is terminated and/or completes their work earlier than the originally expected timeframe, the Company authorized team member (sponsor or supervisor) shall notify proper IT personnel to disable and/or remove the credential or account assigned to that 3rd Party, in a timely manner.

- All 3rd Party computers, laptops, tablets, or other devices, used to access McWane's systems, may be subject to inspection and approval by McWane's or its Divisions' IT personnel, prior to being allowed to connect to McWane's or its Divisions' systems.

Section 6: Data Backup

All applications, data and information contained within Company IT Systems should be backed up and/or archived to ensure that fundamental data and/or disaster recovery capabilities are in place. Where possible, centralized Corporate IT Systems should be used by Divisions for backups, to ensure consistent and ready access, in the instance of need for recovery. All data backup and IT disaster recovery measures undertaken at the Company, and by its Divisions, should provide for satisfactory support of internal or external needs, including compliance with any applicable federal, state, or local laws and regulations. Divisions should also keep adequate records which document successful routine backups of all locally maintained data, workstations, and servers, and as such, provide such records that may be needed from time to time to meet any internal or external audit or other compliance requirements. Corporate IT will work with Divisions to ensure consistency in their data and/or hardware backup practices, as necessary.

Section 7: Incident Response and Disaster Recovery Preparedness

McWane has developed and maintains a separate **IT Incident Response Plan ("IRP"),** which may be updated from time to time, and which is established to provide management and IT personnel with principles, guidelines, and procedures to properly identify and handle IT incidents that may affect the safety and/or information security of McWane's and/or its Divisions' overall IT resources.

In general, the objectives for handling IT incidents in the McWane environment include:

- Determining what happened.

- Determining how it happened.
- Assessing any impact and/or damage resulting from an IT incident.
- Avoiding escalation, spread, or further impact that could result from an IT incident.
- Recovering from an IT incident.
- Pursuing prudent and permanent remediation of threats to allow opportunity to avoid further IT incidents that could otherwise recur from the same or similar system vulnerabilities.
- Determining the identity of threat actor(s) involved in any IT incident, and pursuing any legal recourse available to the Company, if appropriate and possible; and,
- Determining any actions (consistent with existing federal, state, or local law) necessary for McWane or its Divisions to take, which would appropriately mitigate and resolve any information or data breach, or Privacy Breach, which may have resulted from an IT incident.

McWane's IT Incident Response Plan provides guidance for, and addresses the following principles:

- Established guidelines to help with prioritizing, characterizing, and/or classifying incidents.
- Specific definitions of the roles and responsibilities of incident responders, incident handling procedures, and communication plans.
- Established guidelines which will lead to the proper preservation of any relevant documentation related to reportable incidents, as may be required by applicable law, or as may be directed by the McWane Legal Department.
- Established processes which allow the plan to be reviewed and changed, periodically; and,
- Established processes which provide for the IRP to be assessed, as may be found necessary by McWane management, to assure that McWane and/or its Divisions are positioned to conduct a thorough response to any actual IT Incident.

Section 8: General Items

Issues and Feedback: To inform and improve the Company's practices surrounding Information Technology management, team members are encouraged to supply feedback on the effectiveness, limitations, or any problematic aspects they encounter when applying the principles included in this Policy.

Modern technologies are rapidly evolving. As such, McWane reserves the right to change, amend, supplement, or replace this Policy at any time, with or without prior notice, and all team members should stay informed about the latest version of this Policy.

Disclaimer: Nothing in this policy is designed or intended to interfere with, restrain, or prevent team member communications about wages, hours or other terms and conditions of employment or any other rights protected by applicable labor laws.

Compliance with Related Policies and Agreements: This Policy is intended to add to, not contradict, limit, or replace, any other applicable policies and legal requirements, all of which remain in full force and effect.

Acknowledgement and Compliance: COMPLIANCE *WITH THIS POLICY IS A CONDITION OF EMPLOYMENT WITH THE COMPANY.* All active team members are encouraged to read and sign this policy, either as part of their onboarding process, or through the conduct of routine interaction with Division or Corporate IT or other management personnel. Copies of returned signature pages shall be maintained by the Company, either locally or in a designated storage folder located on the McWane network.

By signing below, I acknowledge that I have read and understand the requirements outlined in this policy. I agree to use McWane networks, systems, and/or computer equipment in a manner consistent with the security best practices outlined above and to report any security incidents or concerns to my supervisor or HR manager.

Team Member Signature: _____

Date: _____