For Generations

Information Technology Policy

Guidelines and Procedures

The McWane Way

Effective as of May 1, 2021

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 operating 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 maintaining 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" – any and 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 reside 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 third parties who have been afforded credentialed access to Company IT System(s).

Failure to comply with 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 establishing and managing common-use IT infrastructure resources across the Company. Senior managers and/or executives at each Division are responsible for the performance of IT resources that are within the sole control of that Division. Division IT or other personnel may request the Corporate IT department's assistance 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 at 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 in a timely manner, 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 deemed 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 third-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 generally 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 the 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 those overall 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 permitted, 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 impact 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 provides 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 as a result of becoming an authorized User of Corporate IT Systems, internet and E-mail use may be monitored. The Company reserves its 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 appropriate management and/or to the Human Resources Department. The Company reserves the right to take appropriate action in connection with any violations that may be identified.

- Divisions shall use E-mail systems, Internet connections and Internet service providers approved by Corporate IT;

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

- No Division may establish a separate connection to the Internet without the explicit approval of Corporate IT; further, Corporate IT may isolate, disconnect, or take other appropriate action, related to any such connection(s) which may be or may have been established 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, 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 transmit 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 retrieve, delete, or wipe Company-related business information from those personal accounts.

- 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 deemed 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 transmit E-mail or access Internet content which may contain illegal or otherwise offensive materials;
- 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 assistance 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 attempt to deliberately circumvent or disable the Internet or E-mail filtering and tracking software utilized 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 advised to protect such equipment from damage, to the extent possible, and are required to establish appropriate secured 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, in order to protect McWane data, prevent misuse, and comply with 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 requested, users must promptly provide the Company with access to any telephone or wireless mobile device, including in the event 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 maintain wireless mobile device settings (security, content restrictions, passwords, or passphrases, etc.) which are consistent with this overall IT Policy;
    - Users should not seek to gain unauthorized access to the telephones, voicemail boxes, or wireless mobile devices of work counterparts, under any circumstances;

- Users are advised to follow any and all applicable federal, state, or local laws or regulations regarding the use of wireless mobile devices, particularly when traveling, driving, or operating 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, Twitter, 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 attempting 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 Corporate 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 timely updates and patches, where possible. Users may be denied remote access, if they attempt 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 deemed 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 deemed 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 Security

Users should refrain from downloading, opening, executing, or running unsolicited or unapproved applications and programs in the Company's IT Systems and environs.

- 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, access work computer systems from remote locations, and vice versa. They also provide a back door into the McWane and/or Division network and systems, that can be used for theft of, unauthorized access to, 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 systems.

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 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.

2.8 Access Credentials

Each User is assigned a unique User ID and is required to establish a password or passphrase, as may be required, 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 credential has been violated in any way.

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 regarding 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 determined appropriate.

Senior managers and executives at each Division are responsible for ensuring that their Division complies with 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 observe any violation of the Company's InfoSec operations, notice anything which could constitute 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 Corporate IT, immediately.

Under no circumstance is an established corporate InfoSec standard or practice to be circumvented by any User or third-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 operate 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 in a timely manner by appropriate IT personnel;
- IT administrators shall always exercise their job responsibilities and maintain appropriate separation of duties, where practical and feasible;

- Company IT System access controls shall be implemented and monitored, and where possible, appropriate firewall rules and network segmentation shall be established to provide for layers of information security throughout;
- Use of cloud computing services, procured on behalf of or used by the Company, shall be closely monitored, secured, and controlled by authorized IT personnel, to the extent feasible;
- Only Company-approved and appropriate 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 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 E-mail access to Corporate IT Systems, will be afforded information security training and awareness materials. Divisions may be engaged to assist and provide input and materials for use, around the organization, for purposes of promoting information security awareness throughout the Company.

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 handling by team members, shall be subject to the requirements set forth in 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 maintain any network infrastructure operated 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 connecting 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 Corporate IT System.

4.1.2 Centralized Data Center(s)

Corporate IT will manage and maintain 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 maintained 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 in accordance with Section 4.2 of this policy.

Contracts with third 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 may be otherwise excepted, privately-owned hardware should not be connected to Company IT Systems. Guest access to Company IT Systems may be provided for visitors as needed.

All guest hardware connections are to be temporary in nature, unless otherwise excepted by appropriate 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, third 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 determined 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 appropriate 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 data, system logs, and associated information and software, 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 ***"Record 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 appropriate mitigation measures, until any identified issue is fully resolved.

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 third-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 appropriate Corporate IT personnel.

All new IT hardware, software or firmware assets should be scanned, tested, or otherwise confirmed, with appropriate documentation, that no vulnerabilities exist, prior to 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 as may be directed by Corporate IT;
- Never using 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 be applicable 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 are required to be established as part of any User Credential. Such passwords or passphrases are to be established, updated, changed, or reset, in accordance with systematically enforced standards, as they may be published and/or imposed, from time-to-time, across Company and/or Corporate IT Systems;

- Generic or shared User Credentials or accounts should be readily identified as such, limited to only those necessary, and in all instances, established only after approval by appropriate IT personnel has been obtained;

- For any User to gain remote access to Corporate IT Systems, VPN technology and/or multi-factor authentication ("MFA") may be required to access computing equipment, servers, or other Corporate IT environs. In such instances, Users will be provided with specific instructions and appropriate VPN or MFA credentials, as may be determined necessary, to initiate viable 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 maintained 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, generally, 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 deleted by Corporate IT personnel;

- Where feasible, accounts should have a specific expiration date established;

- For all accounts, the "employeetype" field in active directory must be populated, 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 maintained 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 appropriate documentation, by designated employees of that Vendor; or,
- "Admin" – for accounts created and assigned only to authorized personnel, as may be required to perform their job duties and responsibilities.

5.1 3rd Party Account Creation and Access Controls

The following guidelines shall be applicable 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 (or "NDA") from the 3rd Party which specifies, at minimum:
  - the legal name and address of the 3rd Party (company name);
  - the contact name, title, email address, work and mobile telephone numbers of the person who is designated 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 member (sponsor or supervisor) approving the help desk ticket request for any 3rd Parties' access, shall be recorded, and displayed in active directory in an appropriate 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 utilize the VEN.FIRSTNAME.LASTNAME @divisionname.com naming convention;
  - such accounts will only be permitted up to F3 Microsoft Office 365 licensing, unless otherwise justified by the supervisor;
  - such accounts will be forced to comply with McWane's Corporate password, passphrase, 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 anticipated timeframe, the Company authorized team member (sponsor or supervisor) shall notify

appropriate IT personnel to disable and/or delete 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 and IT Disaster Recovery Preparedness

All application, 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 feasible, centralized Corporate IT Systems should be utilized by Divisions for backups, to assure 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.

Corporate IT will work with Divisions to assure consistency in their data backup practices and/or disaster recovery efforts, as needed.

Questions or other inquiries about this policy may be directed to McWane Corporate IT, Birmingham, Alabama, USA.