INTERNET-RELATED SYSTEMS POLICY

McWane, Inc. maintains internet-related systems for the use of employees for the benefit of the Company. The purpose of the Company internet-related systems is to facilitate the exchange of information within the Company for the benefit of the Company. Employees have access to these systems consistent with the requirements of their jobs, are expected to develop the necessary skills to use the systems at the level of proficiency appropriate to their job, and are encouraged to use the systems for business purposes. Different access levels are designated for various job functions and user IDS and passwords are issued to enable each employee to log onto the system and use appropriate functions. Communications and internet access should be conducted in a responsible and professional manner reflecting the Company's commitment to honest, ethical and non-discriminatory business practices. To promote the efficient use and to avoid misuse of internet-related systems, a copy of this policy will be distributed to all new employees. The division will ensure that it has a signed acknowledgement of receipt of the policy from the employee which will be placed in the employee's personnel file.

I. **[Division Name]**

APPROPRIATE USE FOR INTERNET-RELATED SYSTEMS

GUIDELINES OF THE POLICY

All employees, contractors, consultants, temporary or other workers with access to McWane's Internet-Related systems (whether on Company premises or from remote locations) are subject to and must adhere to this policy.

1. INTERNET-RELATED SYSTEMS

Three interrelated systems are presently in use at McWane: (1) intra-net system (available only to employees), (2) Internet World Wide Web system (includes public access to our Web site from outside the Company and Company employee access to the World Wide Web from Company computers), and (3) Electronic Mail ("e-mail").

a) Intranet: Employees have access to Company information via the intranet system. Use of this system enhances employee knowledge of the Company's goals, vision, and performance and reduces the reliance on traditional inter-office mail.

b) Internet and World Wide Web: Employees may have access to the Internet and the Web as a means of obtaining information that will assist them in the performance of their jobs. The public has access to the Company Web site, which enables the Company to project its image and product, develop business, and improve its Company profile. Employees may not use the company equipment or systems for blogging, visiting chat rooms, social media or other similar personal internet activity without specific prior approval from the General Manager.

c) E-mail: The Company maintains an e-mail system, which is fully integrated with both the intranet and Internet systems. The system enables employees to communicate efficiently among themselves and with other parties. Use of this system improves the speed with which information can be disseminated and enables the Company to be responsive to employee needs.

2. OWNERSHIP OF INTERNET-RELATED SYSTEMS

Internet-related systems (including but not limited to: computer equipment; software and operating systems; network accounts providing electronic mail, World Wide Web browsing, file transfer protocol, etc.; networking and intranet systems and software) are

the property of McWane, Inc. They are to be used for business purposes in serving the interests of the Company in the course of normal operations.

3. PRIVACY OF COMMUNICATIONS

Employee communications on these systems are not private. Users of McWane's intranet, Internet and e-mail systems should be aware that the data they create on the Company system remains the property of the Company, and usually can be recovered even though deleted by the user. Despite security precautions, there is no absolutely fail-safe way to prevent an unauthorized user from accessing stored files. The network management cannot guarantee the confidentiality of any information stored on the network. Information that must remain confidential should therefore not be stored on the network. Employees should exercise caution when using these services to ensure that no confidential or sensitive information is transmitted over open systems. In addition, given the accessibility of data transmitted over these systems, employees shall use appropriate discretion to ensure that no inappropriate, inflammatory, or other improper material is sent through the system.

4. MONITORING

Any information, data, files, or other material on the Company's Internet system shall be subject to review or inspection by the Company for any reason and at any time. The Company has the right to monitor all employee usage, appropriate use by employees, the security of Company data, and to retrieve and use the contents of any employee files, data, or communication in these systems. Management may access or use all files, including archived material of present and former employees without the user's consent for any purpose at any time with or without notice. Moreover, by using the Company's computers and Internet-related systems, users consent to allow all information stored on those assets to be divulged to law enforcement at the discretion of the Company.

5. PERSONAL USE

Subject to paragraphs 3 and 4 above, personal use of the system is authorized within reasonable limits as long as it does not interfere with or conflict with business use or the employee's performance of his or her job. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet and e-mail systems; however, in the absence of such policies, employees should be guided by departmental policies on personal telephone use and, in case of doubt, should consult their supervisor or manager. Under no circumstances may the system be used to transmit or material of an inappropriate sexual nature or material which is demeaning to any individual because of that individual's race, color, age, gender, religion, disability, sexual

orientation, marital status, national origin or veteran status. The provisions of this paragraph apply to both electronic communications originating from within the McWane division's facilities and electronic communications coming into the facility from outside.

6. SECURITY

Employees are required to take all necessary steps to prevent unauthorized access to the Internet-related systems in place at McWane. Employees are expected to keep their passwords secure and unknown to all other persons and refrain from sharing accounts. Authorized users are responsible for the security of their passwords and accounts. Passwords should be changed quarterly through contacting the division's IT department. Authorized users should take steps to prevent unauthorized access to their accounts by logging off when their terminal will be unattended.

7. SYSTEM INTEGRITY AND COPYRIGHT

All users should be aware that any information, software, or graphics on the Internet may be protected by federal copyright laws, regardless of whether a copyright notice appears on the work. Licensing agreements may control redistributions of information from the Company's Internet-related systems or from the Internet. Duplication or transmission of such material or downloading shareware may not be undertaken without authorization from the IT department. Employees must never open, execute, or run unsolicited binary code e-mail attachments. Employees must also use extreme caution when opening e-mail attachments contained in communications from unknown senders as these attachments may contain viruses, e-mail bombs or Trojan horse code.

8. ARCHIVING AND BACKUP OF SYSTEMS

Employees who have computers connected to the Internet-related systems and certain other designated employees are responsible for backing up data on a daily basis. This is an important function designed to maintain records of communications and activity which replaces (or supplements) maintaining files containing memoranda, correspondence, etc. The Company provides Network servers to which the employee can copy important data. These servers are backed up nightly. If the employee does not copy his or her data, then any problems (hardware or software) on their computer may jeopardize that data.

9. RESTRICTIONS AND PROHIBITIONS ON USE AND ACCESS

In furtherance of the Company's commitment to honest, ethical and non-discriminatory business practices, the following restrictions and prohibitions apply:

a) Data Security:

1) Personnel must safeguard their logon ID and password from disclosure to any person except the staff of the IT department. Personnel must use their own logon ID and password only, are responsible for all activity on their logon ID, and must report any known or suspected compromise of their ID to the IT department.

2) Unauthorized attempts to circumvent data security schemes; identify or exploit security vulnerabilities are prohibited.

3) Attempting to monitor, read, copy, change, delete or tamper with another employee's electronic communications, files or software without the express authorization of the user (except for authorized IT personnel) is prohibited.

4) Knowingly or recklessly running or installing (or causing another to run or install) a program intended to damage or place an excessive load on a computer system or network is prohibited.

5) Forging the source of electronic communications, altering system data used to identify the source of messages or otherwise obscuring the origination of communications is prohibited.

Employees who engage in any of the activities prohibited above or otherwise take actions that compromise the security of Company information are subject to appropriate disciplinary action, up to and including termination of employment. Alleged violations will be reviewed on a case-by-case basis.

b) Use of Equipment:

1) Any use of McWane's Internet-related systems that violates federal, state, or local law or regulation is expressly prohibited.

2) Knowing or reckless interference with the normal operation of computers or networks is prohibited.

3) Connecting unauthorized equipment (including personally owned computers, PDAs or other electronic devices) to the network for any purpose inconsistent with the business purpose of the Company is prohibited.

4) Deliberately wasting computer resources, including bandwidth, disk space, and printer paper or running or installing games or other unauthorized software on Company computers is prohibited.

5) Using the Company network to gain unauthorized access to any computer system is prohibited.

6) Users of McWane's Internet-related systems must not use them for soliciting business, selling products, or otherwise engaging in commercial activities other than those expressly permitted by the Company.

7) Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type is prohibited.

8) The use of Company Internet-related systems to access, create, transmit, store, utilize, display, or request obscene, pornographic, erotic, profane, racist, sexist, harassing, discriminatory, threatening, illegal, defamatory or other offensive or inappropriate material (including messages, images, video, or sound) is prohibited.

9) Any use that is deemed to adversely affect the Company is prohibited.

10) Users of Internet-related systems are further advised to consider that while they use corporate systems they represent the Company just as they would at a Company function or in a Company vehicle. Visits to Web sites and other Internet use may reflect upon the Company and should be undertaken in a serious, businesslike manner.

11) Web pages and links made available to the public must be approved by and developed in cooperation with the IT department prior to activation.

12) Personal blogs regarding any of the following is strictly prohibited:

a. Company business, financial, pricing, technical, marketing and/or service information

b. Personnel information, job assignments, medical information and/or records and salary/compensation information.

c. Engineering designs/specifications, manufacturing or process information, business or product plans with outside

vendors, business or cooperation arrangements with other companies, internal data bases, patent application and copy righted material.

d. Business operations or projects, whether past, current or proposed.

e. Any other information that is confidential or proprietary to the Company or to any third party that has disclosed the information to the Company.

Employees who violate any of the prohibitions listed above or otherwise use McWane's Internet-related systems in a manner inconsistent with Company policy or applicable law are subject to appropriate disciplinary action, up to and including termination of employment. Alleged violations will be reviewed on a case-by-case basis. Moreover, McWane also reserves the right to report the illegal use of its computers and Internet-related systems to the appropriate law enforcement agencies.

The Company may amend this Acceptable Use Policy from time to time as necessary. All users will receive notice of any amendments. The Company will not be responsible for any misuse or unauthorized use of Company Internet-related systems.

ACKNOWLEDGMENT

I acknowledge that I have read, understood and agree to each of the provisions of McWane's Appropriate Use Policy for Internet-Related Systems. I further understand that I am subject to immediate disciplinary action, up to and including termination, for any actions deemed by McWane to be in violation of this policy. Finally, I understand that if I have any questions regarding this policy or my duties and obligations under this policy, I can direct those questions to the Company's Human Resources Department.

_____ _____

Employee Signature Date

Print Name: _____