Progress Industries

Standard Policies and Procedures

Subject: Cyber Security Policy

Approved by: President & CEO

Effective date: 9-18

Review date:

Modified date: 9-19, 11-19

**POLICY**

**PURPOSE OF THE CYBER SECURITY POLICY**

Progress Industries cyber security policy forms the foundation of the corporate Information Security Program. Information security policies are the principles that direct managerial decision-making and facilitate secure business operations. A concise set of security policies enables the IT team to manage security of information assets and maintain accountability. These policies provide the security framework upon which all subsequent security efforts will be based. They define the appropriate and authorized behavior for personnel approved to use Progress Industries information assets.

This policy includes four distinct components:

• General Email/Internet Security and Use

• Bring Your Own Device (BYOD) and Acceptable Use

• Online Social Networking

• Internet/Intranet Publishing

**APPLICABILITY**

The Progress Industries Cyber Security Policy applies to all employees, interns, contractors, vendors and anyone using Progress Industries assets. Policies are the organizational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks, and components owned or leased by Progress Industries or its designated representatives.

**GENERAL EMAIL/INTERNET SECURITY AND USE**

**General Security Policy**

All employees, contractors, vendors, and any other person using or accessing Progress Industries information or information systems must adhere to the following policies:

* Progress Industries owns and has full access to all information residing on the company network, individual computers/devices, storage media and company internet sites. All information systems within Progress Industries are the property of Progress Industries information or information with Progress Industries policy statements
* Any personal information placed on Progress Industries information system resources become the property of Progress Industries.
* Any attempt to circumvent Progress Industries security policy statements and procedures (e.g., disconnecting or tunneling a protocol through a firewall) is strictly prohibited.
* Unauthorized use, removal, destruction, modification and/or distribution of Progress Industries information or information system is prohibited.
* All users will acknowledge understanding and acceptance by signing the appropriate Progress Industries policy statement (see last page of policy) prior to use of Progress Industries information assets and information systems. Copies will be maintained by Human Resources.
* Users realize that by clicking save, submit, approve, etc., they are electronically signing that record. This electronic signature is legally binding and carries the same legal weight and responsibility as a traditional hand-written signature.
* At minimum, all users will be responsible for understanding and complying with the following policy statements:
1. General Security Policy
2. System Security Policy
3. Password Security Policy
4. Desktop Service Security Policy
5. Internet Acceptable Use Policy
6. Email Security Policy
7. Virus, Hostile and Malicious Code Policy
8. Personal Equipment Policy
9. On-Line Social Networking Policy
10. Internet/Intranet Publishing Policy
* All users will report any irregularities found in information or information systems to the IT team immediately upon detection. Any known breach of electronic security must be reported immediately to the IT department and a member of Leadership. A written report of security breaches, their containment, and potential confidentiality affects will be made within three business days by the IT department to the HIPAA Privacy Officer. The HIPAA Privacy Officer will be responsible for making any necessary reports of the breach to persons served, guardians and the Department of Health and Human Services.
* Progress Industries information systems and information will be subject to monitoring at all times. Use of Progress Industries information systems constitutes acceptance of this monitoring policy.
* Confidential information on the network must remain confidential. Information is to be accessed only on a need to know basis. If employees discover that they have access to another person’s data it is their responsibility to log off and immediately contact the IT department. Any act to access, read, print, edit or delete system, departmental, or another person’s data may result in disciplinary action.
* Use of any Progress Industries information system or dissemination of information in a manner bringing disrepute, damage or ill will against Progress Industries is not authorized.
* Release of Progress Industries information will be in accordance with Progress Industries policy statements.
* Users may attach their own computer or device to Progress Industries guest WIFI network using a password established by the IT department. Anyone trying to connect to the PI guest WIFI network must agree to the usage policy before they connect.

**System Security Policy**

Progress Industries’ System Security Policy addresses control, use of hardware, operating systems, software, servers and backup requirements for ally systems maintained and operated by Progress Industries.

The System Security Policy applies to all Progress Industries employees, contractors, vendors, and any other person using or accessing Progress Industries information systems. Exceptions to this policy must be approved by the CEO or their designated representative.

Access to the computer network, email and Therap shall be given to employees according to their job duties. Human Resources will notify a Therap Provider Administrator and the IT department when employees are on a leave of absence, hired, transfer or change positions, or end employment.

When employees are on a leave of absence their access to the network, email and/or Therap data will be terminated or suspended. On call employees Therap access will be locked when they return to school or not taking hours for 30 consecutive days. Managers will be required to notify a Therap Provider Administrator when on call employees have accepted hours to reset their account.

**Password System Security Policy**

In today’s information age, poorly selected, reusable passwords represent the most vulnerable aspects of information security. Progress Industries has adopted this policy to ensure that the private information of persons served and our proprietary corporate data are kept secure at all times. Progress Industries authorized users must comply with creation, usage and storage policies to minimize risk to corporate information assets:

* Network Passwords will conform to the following criteria

-Passwords will be a minimum of seven characters

-Passwords must consist of at least one uppercase letter, one lowercase letter, one special character, and one number.

* The sharing of passwords is prohibited.
* Any suspicious queries regarding passwords will be reported to the IT team
* Passwords will be protected as Progress Industries proprietary information. Writing passwords down is prohibited. Passwords can be stored on personal devices as long as the device itself is password protected.
* Users are forbidden from having computers automatically remember passwords. This includes company, personal and public computers/devices that access the PI network or third-party vendors used by PI.
* Network passwords are required to change every 90 days and may reuse passwords only after 10 different passwords have been used.
* Accounts will be locked out after five failed password attempts in a 30-minute time period. Accounts can be reset by contacting the IT team.
* Users will be forced to unlock their computers using their network password after 15 minutes of inactivity on their desktops.
* All system passwords will be changed within 24 hours after a possible compromise.
* When users leave the organization, their accounts will be immediately disabled or deleted.
* If the user leaving the organization was a privileged user or network administrator, all system passwords will be changed immediately.

**Desktop Services Security Policy- Remote Sites**

The Progress Industries Desktop Services Security Policy addresses the authorized and legitimate use of hardware, operating systems, software, local area network (LAN), file servers and all other peripherals used to access any Progress Industries information system:

* No software or hardware of any kind will be installed onto a laptop or desktop computer without written approval of the IT team.
* Only system administrators will have the ability to install software.
* Unauthorized copying or distributing of copyrighted software is a violation of federal copyright law and will not be permitted.
* Personal software will not be installed on any Progress Industries machine.
* Use of temporary storage devices such as disks, CDs/DVDs, USB drives, etc. must be approved by the immediate supervisor and the IT department.
* All files that contain confidential information, including PHI of persons served, MUST be saved to the network or approved third party vendor, not the local hard drive or removable storage devices.
* Users will not allow non-employees to use any Progress Industries machine or device without authorization of the IT team.
* Computers and mobile devices should not be left unattended when the user is logged onto the network or Therap. Users should lock the work station when leaving their computers or mobile devices unattended for more than 15 minutes. Computers in public areas should be logged off before the user leaves.
* The following items are corporate policy for security monitoring:
1. All Progress Industries systems and network activities will be subject to monitoring. Use of Progress Industries systems and networks constitutes consent to this monitoring. Monitoring user internet, email, and network activity will be done only in coordinated effort with the HR Department and for a time limited period during a suspected abuse situation. Monitoring efforts and results will be documented and shared with Human Resources.
2. IT staff will assure that antivirus software is installed on each server and run on each work station. Disabling or interfering with virus protection software is prohibited
3. Disabling or interfering with logging, auditing or monitoring software is prohibited.
4. All Progress Industries computer services will be subject to inventory and inspection.
5. Security irregularities, incidents, emergencies and disasters related to Progress Industries information or systems will be reported to the IT team immediately.
* The following items are corporate policy for system usage:
1. Sabotage, destruction, misuse or unauthorized repairs are prohibited on Progress Industries information systems.
* All repairs will be authorized and performed by the IT team:
1. Computer resources will not be used to compromise, harm, destroy or modify any other service or resources on the Progress Industries information system.
2. All data on information systems at Progress Industries is classified as company proprietary information.
3. Users will secure all printed material and other electronic media associated with their use of Progress Industries information and information systems.
4. Storage, development or the unauthorized use of tools that compromise security (such as password crackers or network sniffers) are prohibited.
* All violations will be reported to the appropriate Director.

**Internet Acceptable Use Policy**

Internet access is provided to Progress Industries employees to conduct Progress Industries business. While these resources are to be used primarily for Progress Industries business, the company realizes that employees may occasionally use them for personal matters and therefore provides access to non-offensive personal sites during non-business hours.

* Employee internet activity, during paid, time will be for PI business purposes only.
* The definition of non-business sites is the sole discretion of the IT team. The definition can, and will, change without notice as the internet continues to evolve.
* Internet activity will be monitored for use.
* Internet activities that can be attributed to a Progress Industries domain address (such as posting to a newsgroup, use of chat facilities and participation in mail lists) must not bring disrepute to Progress Industries with controversial issues (e.g., sexually explicit materials).
* Internet use must not have a negative effect on Progress Industries operations.
* Users will not make unauthorized purchases or business commitments through the internet.
* Internet services will not be used for personal gain.
* Internet users will make full attribution of sources for materials collected from the internet. Plagiarism or violation of copyright is prohibited.
* Release of Progress Industries proprietary information to the internet (e.g., posting information to a newsgroup) is prohibited.
* All internet users will immediately notify the IT team of any suspicious activity.
* All remote access to the Progress Industries internal network through the internet will be encrypted and authenticated in a manner authorized by the IT team.
* Accessing personal social networking accounts (including but not limited to Facebook, Twitter, Google+, LinkedIn, Foursquare, and Tumblr) or using Progress Industries email for social networking purposes is prohibited during working hours. The use of social networking sites for specific business purposes must be pre-approved or assigned by a manager or supervisor.

**Email Security Policy**

The Progress Industries Email Security Policy specifies mechanisms for the protection of information sent or retrieved through email. In addition, the policy guides representatives of Progress Industries in the acceptable use of email. For this policy, email is described as any computer-based messaging including notes, memos, letters and data files that may be sent as attachments.

Authorized users are required to adhere to the following policies. Violators of any policy are subject to disciplinary actions, up to and including termination.

**The following items are the corporate policy statements for Access Controls**:

* All email on the Progress Industries information systems, including personal email, is the property of Progress Industries. As such, all email can and will be periodically monitored for compliance with this policy.
* Individual email accounts are intended to be used only by the person to whom they are assigned. Special arrangements can be made to share information between team members. In all other cases, no user is authorized to open or read the email of another without the express consent of senior management (CEO, Controller, or Human Resources Director).
* Email is provided to the users of Progress Industries primarily to enhance their ability to conduct Progress Industries business.
* Email will be stored on the system up to a maximum of 50GB per mailbox. Mailbox is defined as the combined total of deleted items, inbox, sent items and any user-created email folders. Users will receive a warning message stating that they need to clear out space when their mailbox size reaches 49GB. However, once the mailbox storage space exceeds 50GB, users will not be able to send new mail messages until the mailbox size falls below the 50GB limit. In all cases, however, users will continue to receive incoming messages.
* The maximum size of any individual incoming email message will be 25MB.
* Terminated employees will have all email access immediately blocked.
* Users who leave the company will have all new emails automatically forwarded to their supervisor, or designated representative, for 30 days.
* The former employee’s supervisor is responsible for disseminating stored emails to the appropriate person. Thirty days after the date of termination, the former employee’s mailbox will be permanently removed from the system.

**The following items are the corporate policy statements for Content:**

* Use of profane, inappropriate, pornographic, slanderous or misleading content in email is prohibited.
* Use of email to spam (e.g., global send or mail barrage) is prohibited. This includes the forwarding of chain emails.
* Use of email to communicate sexual or other harassment is prohibited. Users may not include any words or phrases that may be construed as derogatory based on race, color, sex, age, disability, national origin or any other category.
* Use of email to send unprofessional or derogatory messages is prohibited.
* Forging of email content (e.g., identification or addresses) is prohibited.

**Sending PHI in Email – Technical Safeguards**

**USE of SECURE EMAIL**: This outlines the guidelines for P.I. employees who are assigned a progressindustries.org email.

P.I. is required to have in place reasonable safeguards to (1) limit access to e-PHI to authorized individuals and (2) protect against unauthorized disclosures of e-PHI. These safeguards include, at a minimum, those below. Each employee, however, must put in place additional safeguards, based on the technology used, job responsibilities, and nature or information maintained.

**1. Sending Email Containing PHI within P.I.** Email sent from a progressindustries.org email address to another progressindustries.org email address is permitted and secure within the organization. Always verify the recipient’s name and email address before the message is sent.

**2. Sending Email Containing PHI Outside of P.I.** Any email sent from progressindustries.org to an external email must be sent using P.I.’s encrypted electronic messaging system. Writing “SECURE” in the e-mail subject line activates encryption and requires the recipient to create and use a password to open P.I. encrypted emails. Do NOT include the name of the person served or any PHI in the subject line.

All outgoing emails will automatically include the following statement:

“**CONFIDENTIALITY NOTICE**: This correspondence, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information or Protected Health Information (PHI). Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender and destroy all original copies.”

**The following items are the corporate policy statements for Usage:**

* Any email activity that is in violation of policy statements or that constitutes suspicious or threatening internal or external activity will be reported.
* When sending email, users should verify all recipients to whom they are sending the message(s).
* Be aware that deleting an email messages does not necessarily mean it has been deleted from the system.

**Virus, Hostile and Malicious Code Security Policy**

The intent of this policy is to better protect Progress Industries assets against attack from destructive or malicious programs:

* Any public domain, freeware or shareware software will be evaluated by the IT team prior to installation on any company resource.
* No unauthorized software will be downloaded and installed on end-user machines without express approval from the IT team.
* System users will not execute programs of unknown origin, as they may contain malicious logic.
* Only licensed and approved software will be used on any company computing resource.
* All licensed software will be write-protected and stored by the IT team.
* Progress Industries users will scan all files introduced into the environment for virus, hostile and malicious code before use.
* The IT team will ensure that Progress Industries obtains and deploys the latest in virus protection and detection tools.
* All information systems media, including disks, CDs and USB drives, introduced to the Progress Industries environment will be scanned for virus, hostile and malicious code.
* All email will be scanned for virus, hostile and malicious code. Users should not open any email attachment of suspect nature. Attachments should only be opened if you know the sender and the nature of the attachment.
* All internet file transfers will be scanned for virus, hostile and malicious code.
* The unauthorized development, transfer or execution for virus, hostile and malicious code is strictly prohibited.
* All users will report any suspicious occurrences to his/her supervisor or the IT team immediately.
* All company systems will be protected by a standard virus protection system.
* Virus engines and data files will be updated on at least a monthly basis.
* Viruses that are detected on a user’s workstation will be reported to the IT team immediately for action and resolution.
* Irregular behaviors of any software program will be reported to the IT team immediately.

**BRING YOUR OWN DEVICE (BYOD) AND ACCEPTABLE USE**

The Progress Industries BYOD and Acceptable Use Policy applies to all employees, interns, contractors, vendors and anyone using Progress Industries assets. Policies are the organizational mechanism used to manage the confidentiality, integrity and availability issues associated with information assets. Information assets are defined as any information system (hardware or software), data, networks, and components owned or leased by Progress Industries or its designated representatives.

**BYOD Policy**

This policy provides guidelines for using personally owned devices and related software for corporate use.

The BYOD policy applies to all Progress Industries employees, contractors, vendors, and any other person using or accessing Progress Industries information or information systems. Exceptions to this policy must be approved by the CEO or designated representative.

Furthermore, based on the amount of personally identifiable information employees work with, Progress Industries management reserves the right to determine which employees can use personally owned devices and which cannot.

**Personal Equipment Policy**

This policy provides guidelines for using corporate IT support for personally owned equipment and related software, including, but not limited to, notebook computers, desktop computers, smartphones, and cellphones.

Progress Industries recognizes that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of corporate resources, human or otherwise, for personal gain must be monitored closely.

As a general rule, employees of Progress Industries will not use or request corporate IT resources in the use, network connectivity or installation of their personally owned equipment or software.

Personally owned notebooks, smart phones, and tablets will not be granted direct access to the network, but access to the guest network for work purposes only. Employees that wish to access the Progress Industries network from a remote location using their personally owned computer may do so using only Progress Industries-authorized software and only with the approval of their supervisor or manager.

Smart phones, which include devices using Blackberry, iPhone, Windows Mobile, Android, and Linux will be supported according to the following rules:

* Employees are responsible for learning, administering, installing and setting up their own personal smartphones.
* Corporate IT resources should not be used for assistance in the basic operation of these devices

**General Policy**

Progress Industries recognizes that personally owned equipment can play a valuable role in convenience, efficiency and productivity of its employees. Nonetheless, the use of these devices must be monitored closely.

The following is a list of personally owned devices permitted by Progress Industries for corporate use:

* Desk top computers
* Laptop computers
* Tablets
* Smartphones

**Reimbursement**

Progress Industries may provide a stipend for employees utilizing personal devices for work-related activities, with the approval of the appropriate Director.

**Registering Devices**

All personally owned devices, that will contain PI sensitive data on them such as email, must be registered with the Progress Industries IT department.

**End-User Support**

As a general rule, users of registered personally owned devices will not use or request corporate IT resources in the use, network connectivity or installation of their equipment or software. Users are responsible for learning, administering, installing and setting up their personally owned devices.

Progress Industries IT will support personally owned devices as follows:

* The user will be required to allow IT to load security software on each device.
* The user will be required to allow IT to install remote wiping software on each device.
* Upon request, the IT team will install the necessary synchronization software to the user’s desktop or notebook computer.

**Device Security**

The user should follow good security practices including the following:

* Password protect all personally owned devices.
* Do not leave personally owned devices unattended.

**Release of Liability and Disclaimer to Users**

Progress Industries hereby acknowledges that the use of personally owned devices in connection with Progress Industries business carries specific risks for which you, as the end user, assume full liability.

In the case of litigation, Progress Industries may take and confiscate a user’s personally owned device at any time.

**Acceptable Use Policy**

This policy provides rules for the acceptable use of personally owned devices on the corporate network.

The Acceptable Use Policy applies to all Progress Industries employees, contractors, vendors, and any other person using or accessing Progress Industries information or information systems. Exceptions to this policy must be approved by the CEO or a designated representative.

**General Policy**

Users that wish to access the Progress Industries network using their personally owned computer may do so using only Progress Industries-authorized software and only with the approval of the user’s supervisor and the IT department.

Users must follow the same rules when accessing the network from both corporate-issued equipment and personally owned devices. When connected to the Progress Industries network, the user will NOT do the following:

* Use the service as part of violating the law
* Attempt to break the security of any computer network or user
* Attempt to send junk email or spam to anyone
* Attempt to send a massive amount of email to a specific person or system in order to flood a server.

**Authorization of Devices**

Progress Industries IT reserves the right to determine the level of network access for each personally owned device. The user could be granted full, partial or guest access.

**Third Party Applications on Devices**

Progress Industries IT reserves the right to block or limit the use of certain third-party applications, such as those that probe the network or share files illegally, that may harm the corporate network.

As the number of approved applications continually evolved, the user must check with the IT department for the current list of approved third-party applications and get IT approval before downloading an application on the device.

**Reporting Security Concerns**

The user agrees to report the following immediately:

* If the device is lost or stolen
* If the device has been attacked with malware, a virus or any other suspicious attack
* Any other security concern with regard to company data

**Release of Liability and Disclaimer to Users**

Progress Industries hereby acknowledges that the use of a personally owned device on the Progress Industries network carries specific risks for which you, as the end user, assume full liability.

**ONLINE SOCIAL NETWORKING POLICY**

Our company is committed to maintaining a good relationship with employees and with the public. If Progress Industries sustains a positive reputation and excellent image in the public eye, it directly benefits the company as a whole, in addition to putting you in an advantageous situation as an employee. The way the public views Progress Industries is vital to promoting business, gaining new business, retaining first-class employees, recruiting new employees, and marketing our products and services.

While Progress Industries has no intentions of controlling employees’ actions outside of work, it is important that employees and volunteers practice caution and use discretion when posting content on the internet, especially on social networking site that could affect Progress Industries’ business operations and reputation. This policy serves as a notice on the practice of social networking for all employees to read and understand.

The following is the purpose of the Online Social Networking Policy:

* To guarantee a constructive relationship between the company and its employees
* To reduce the possibility of risk to Progress Industries or its reputation
* To discourage the use of company time for personal networking.
* To ensure employees are aware of their actions while engaging in social networking, the number of individuals who can access information presented on social networking sites and the consequences associated with these actions.

**Definitions**

**Social Networking:** Any activity that involves interaction in online communities of people. This interaction includes, but is not limited to, browsing other users’ profiles, browsing other users’ photos, reading messages sent through social networking forums and engaging in online communities’ instant messaging services.

**Social Networking Sites:** Specific online communities of users, or any website that links individuals electronically, and provides a forum where users can connect and share information. These websites can be general or tailored to specific interests or certain types of users. Examples of popular social networking sites include Facebook, Twitter, Google+, LinkedIn, Foursquare and Tumblr. The list of domains that constitutes social networking sites is ever-growing and changing because of the nature of the internet.

**Social Networking Profile**: A specific user’s personalized webpage within a certain social networking site, usually containing personal information such as one’s name, birthday, profile photo and internet.

**Microblogging**: The practice of publishing your recent whereabouts, thoughts or activities on a social networking site for other users to see. This is the main focus of social networking sites such as Twitter, but is also includes features like status updates on Facebook.

**Business Purposes**: Using a social networking site for the company’s gain, usually as a task or assignment given by a manager or supervisor. This can be done either through a specific company account on a given social networking site or through a personal account for the purpose of recruiting or marketing for Progress Industries.

**Prohibited Use**

It is important that employees use their time while at work to conduct company business. The following actions are prohibited during working hours:

* Using social networking to conduct personal or non-company business
* Browsing social networking sites for non-company business on company time
* Reading email alerts regarding personal social networking account activity or using Progress Industries email to correspond with personal social networking contacts.
* Updating information, uploading photos or otherwise engaging with one’s own, personal social network profile for non-business purpose
* Micro-blogging for a non-business purpose on a social networking site throughout the day, whether it is on a company-provided computer or a smartphone device.

**Prohibited Conduct**

Having your own individual social networking account and using it on your own time is certainly permissible. However, keep in mind that some actions on your personal site are visible for the entire social networking community and are no longer private matters. While Progress Industries will not be continuously monitoring employees’ personal conduct on social networking sites, it might be a good guideline to assume that anything posted on your personal social networking profile could potentially be seen by anyone at the company. While this section of the policy is a sensitive one, Progress Industries put it in place to protect not only the company, but you and your job. It is for your own security and defense that you follow these guidelines:

* Do not use microblogging features to talk about company business on your personal account, even on your own time. Do not post anything you would not want your manager or supervisor to see or that would put your job in jeopardy.
* Do not use the company name, address email addresses or other information in your personal profile. This is for your physical safety as well as the safety of everyone else at the company and the protection of Progress Industries name.
* Do not post any pictures or comments involving the company or other Progress Industries employees that could be construed as inappropriate. Do not take pictures of persons served without a release and do not post pictures of persons served on social media.
* Do not post information about persons served by Progress Industries, including general address or locations, any information that would be governed by HIPAA regulations or other items that could reasonably be construed by the person served to be personal or an invasion of their privacy.
* You are also responsible for what other users post on your individual social networking profile. Do not allow inappropriate or sensitive information regarding Progress Industries anywhere on your profile, even if it is generated by a different user.
* If your personal profile is visible to other employees at the company, supervisors, manager or peers, practice caution. You have control over yourself but not over these employees, and just one inappropriate picture or comment taken out of context could fall into the wrong hand and cost you your job.

**General Rules**

* Respect all copyright and other intellectual property laws when posting on the internet and social media.
* Only authorized employees are permitted to engage in social media forums during regular business hours on P.I. provided equipment for work related purposes only.
* Only authorized employees may prepare or modify content to PI owned or branded sites. Employees who wish to post photos and/or content on a PI site may forward the information to the Communications Director.
* Progress Industries reserves the right to remove any content from any PI branded page. Removal of such information will be done without permission of the author or advance warning. This includes postings by employees and non-employees.
* Progress Industries employees may not post photos or content on the Internet or any social media outlet that represents P.I. name or in a manner that could be attributed to the agency without written authorization from the Communications Director. You should not represent any opinion or statement as the policy or view of Progress Industries unless specifically authorized to do so.
* You are personally responsible and can be held liable for commentary that is considered defamatory, obscene, proprietary or libelous by P.I. or any offended party.
* You should avoid any posts that could be considered harassment, bullying, discrimination or retaliation. If a post would not be permissible in the workplace, it is not permissible between co-workers online, even if it is after hours, from home and on home computers. P.I.’s non-discrimination and harassment policies apply to all conduct by its employees, including posting on the Internet and social media sites. Inappropriate postings that may include discriminatory remarks, harassment and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.
* If you choose to identify yourself as a P.I. employee, please understand that some readers may view you as a spokesperson for the agency. Therefore, it is important that you expressly state that your postings are your own and do not represent the opinions of the agency.

**INTERNET/INTRANET PUBLISHING POLICY**

**Introduction**

These Wide Area Network (WAN) Internet and Intranet Publishing Guidelines are applicable to all employees of Progress Industries and P.I. Foundation, its board and volunteers. They provide specific guidance on implementing P.I. Policy with respect to information posted to and removed from internet and internal network servers. P.I. servers are configured and administered internally by the IT Department.

**Web Publishing Guidelines**

Information published to the internet/intranet servers should follow the same consideration as that published to other media for distribution. Published material should:

* Protect intellectual property rights of ownership (e.g. copyright)
* Protect every individual’s right to privacy
* Protect the welfare of individuals served by Progress Industries.
* Promote the use of resources toward the accomplishment of company goals

**Links and Consents**

Links to personal home pages are not permitted. Likewise personal information (home address, email address, phone numbers) should not appear on Internet/Intranet web pages. An individual’s full name shall not be published without written consent from the individual and, if applicable, the individual’s guardian. Photographs of a person from the back or indistinguishable frontal photographs may appear on the Internet/Intranet without written consent. Group of unidentified persons served and employees may be published on the Intranet without permission.

**Content Responsibility**

**ORIGINATOR'S RESPONSIBILITY**

Progress Industries employees are personally responsible for their use of network services made available to them. Those creating internet/intranet server content are responsible for seeing that it meets these guidelines and implements P.I. Policy.

The web content originators, not the server maintenance personnel, are responsible for the information they submit to be posted. All information must be double-checked for accuracy. Per P.I. Policy, information which could be perceived as threatening, obscene, disruptive, unethical or construed as harassment or disparagement of others based on their race, national origin, gender, sexual orientation, age, disability, religion or political beliefs shall not be posted.

Agreement forms required for the posting of any sensitive, confidential, copyrighted, or private information must be collected and stored by the originator for as long as needed to assure satisfaction of legal requirements. P.I. staff are directed to limit access of web content containing information on, or photographs of, individuals served to the minimum audience needed to accomplish company goals. Information that is only for employees should be kept separate and secure from public information.

**WEBMASTER RESPONSIBILITIES**

Each web site will have one webmaster or designee who is responsible for posting to the Internet. Web server submittals may be made through the site's webmaster or designee. Webmasters and designees will not share passwords or allow anyone else to post to the web server. Webmasters and designees must not knowingly post inappropriate material and should exercise controls necessary to remove and prevent reposting of inappropriate content when any is found. Employee names, pictures, work assignments and e-mail addresses should only be posted to the Internet with the employee's written/e-mail permission.

Links to pre-existing sites should be checked regularly to ensure that they are appropriate and active. Only active files that are required for the proper operation of the Internet/Intranet should be stored on the Internet/Intranet server. Inactive files should be deleted.

**APPENDIX A**

**SUGGESTED WEB PUBLISHING GUIDELINES**

**Content Style**

**Access for People With Disabilities:** Websites and pages should be guided by Section 08 of the Rehabilitation Act (29 U.S.C. 794d), designed to make online information and services fully available to citizens with disabilities.

**Plain Language:** Web sites must ensure that home pages, all major entry points, and navigational elements are written in plain language, considering the knowledge and literacy level of their typical visitors.

**Access to Documents in Different File Formats:** Choice of file formats should be based on both the business needs of the company and the needs of the web site visitors. Web sites should provide information in a format that does not require the audience to use a plug-in or additional software, if it imposes a burden on its visitors. When choosing the file format, the agency should consider: (1) the intended use of the material by the target audience; (2) the accessibility of the format to the target audience; and (3) the level of effort required to convert the material to the format. Agency web sites should, when linking to documents that require downloading (for example, PDF, MS Word, or MS Excel documents), provide sufficient contextual information so visitors have a reasonable understanding of what to expect when they view the material.

**Accessing Information via a Search Engine:** Every web page must include (or link to) a search engine that allows visitors to search the content of the web site.

**Agency Web Sites Must Use Standard Metadata:** In order to improve search relevancy and publication dates, web sites should include the following metatags on all home pages and second-tier pages (one level below the home page):

* Page Title,
* Creator (in most cases, the agency name),
* Language,
* Publication Date,
* Subject and Keywords

**Web Pages Must Link Back to the Home Page:** To improve web site usability, every web page must link back to its home page.

**Authenticity:** Each web page should clearly display the company name and logo. Links to other sites require approval of the Communications Director or CEO. Web pages will include a statement prohibiting unauthorized link from other sites to P.I. site and procedure to obtain authorization for written permission for approved links.

**Cyber Security Acknowledgement Agreement**

1. Passwords:
	1. I will take precautions to make sure that computer settings must not be set to remember password for any computer used, personal or public.
	2. I will not share my network or other records password with or make it known to anyone, including friends and family, PI staff, or I.T. support personnel. My password will not be shared, disclosed or written down. I understand that violations of this requirement are against Iowa law, and if convicted, are punishable by monetary fine, imprisonment, or both.
	3. If the password is known or suspected to be compromised, I will immediately change the password to a new one meeting security requirements.
	4. I will use a password that is not easily guessed (favorite color, birth date, favorite pet, etc).
2. I will not leave my computer workstation unattended unless locked or shut off and will not allow others to view the records I access.
3. If I discover that I have access to records I shouldn’t I will close that record and notify I.T. staff immediately.
4. I will not down-load, copy or otherwise transfer information from the PI database or network unless I am specifically authorized to do so by nature of my position. If allowed to transfer this information I will keep it secured and delete it when finished.
5. By clicking save, submit, approve, etc., I understand that I am assigning my legal signature to that record. This electronic signature is legally binding and carries the same legal weight and responsibilities as a traditional handwritten signature.

**Social Media:**

**Progress Industries employees may not post photos or content on the Internet or any social media outlet that represents P.I. name or in a manner that could be attributed to the agency (including the people P.I. support) without written authorization from the Communications Director.  You should not represent any opinion or statement as the policy or view of Progress Industries unless specifically authorized to do so.**

I acknowledge that these requirements have been explained to me, that I understand them, and that I will uphold these in order to protect the security, integrity and confidentiality of electronic records, including EPHI. I am aware that failure to maintain security protocol could result in disciplinary action up to and including termination of employment, fine, and imprisonment.

Printed Name & Title:

Signed Name:

Date:

This form is to be completed once by all users with access to P.I. records, including the P.I. network or any online database. The original of this signed form will be kept in the HR file. For non-staff users (guardians, case managers, etc.) the original will be kept by the Director of Operations.