**ULM Tech Industries, Inc.**

**IT Policy Manual**

**June 2017**

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-01**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Introduction, Purpose & Scope** | | | **Page 1** |
| Each employee has the responsibility to use the Company’s systems and applications effectively, legally, securely and respectfully of others. This policy applies to all existing and proposed computer applications, systems and networks and is effective from the date of issue.  IT Security is a vital concern to ULM Tech Industries. The objective of this policy is to protect Company data and to communicate to all employees the importance of following it. This document provides the guidelines for controlling ULM Tech Industries’s systems, networks and financial applications, ensuring that:   * IT captures, processes and maintains information completely and accurately. * Data is accessible to the appropriate people to enable them to carry out their responsibilities. * All authorizations are documented.   Company IT resources consist of all electronic devices, software, and means of electronic communication including, but not limited to: desktop computers, workstations, laptops, servers, routers, peripheral equipment (i.e., printers, modems, fax machines, copiers, etc.), software applications and data, the Internet, e-mail, instant messaging, telephones, cellular phones, Blackberry units, pagers, and voicemail.  Granting access to Company IT resources is within the sole discretion of the Company. Access to Company technologies is based on job responsibilities and roles. Each employee will be given a unique identification once authorization has been received by management. The employee will also receive a unique e-mail address for use with the Company’s e-mail system. An employee is responsible for all computer entries made with that employee’s User ID and password.  ULM Tech Industries is very sensitive to the issue of protection of trade secrets and other confidential and proprietary information of the Company. Employees are expected to use good judgment and to adhere to the highest ethical standards when using or transmitting highly sensitive information on the Company’s IT Resources. Highly sensitive information must not be accessed through the Company’s IT Resources in the presence of unauthorized individuals and must not be left visible or unattended.  All ULM Tech Industries employees using IT resources must sign the IT Security Form, acknowledging that:   * They have received, read and understand Company IT Policies and Procedures. * They understand and agree that any IT resource provided by the Company contains proprietary and confidential information about ULM Tech Industries and its customers/vendors and that these resources remain the property of the Company at all times. * They will not duplicate any Company information or software. * They will return all ULM Tech Industries IT resources upon leaving the Company. * They will not participate in unauthorized destruction of Company electronic records.   Any employee found to have violated Company IT policies or failed to make a best effort attempt to comply with these guidelines may be subject to disciplinary action, up to and including termination of employment and possible civil liabilities and/or criminal prosecution. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-01**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Privacy standards for Company owned Computers** | | | **Page 3** |
| The Company’s e-mail system and Internet services are provided for work related purposes and not for personal matters. Incidental and infrequent personal use during scheduled work breaks is tolerated, but not for any purpose inconsistent with the Company’s Code of Ethics. Do not access, send or download any information that is illegal, or could be insulting or offensive to another person, such as sexually explicit messages, any cartoons or jokes, unwelcome propositions, ethnic or racial slurs, or any other message that could be viewed as harassment.  **The Company reserves the right to delete any non work related files without notice to the user.**  All e-mail messages, voice mail, faxes and computer information are considered Company property and employees should not have any expectation of privacy. Unless prohibited by law, the Company reserves the right to monitor, access and disclose this information as necessary for business purposes or as the Company otherwise deems appropriate. Use good judgment and do not access, send a message, or store any information that you would not want to be seen or heard by other individuals. Violation of these policies may result in disciplinary actions up to and including discharge by the Company.  All messages sent and received (including personal messages) and all data stored on the Company’s e-mail system, voicemail system, or computer systems are Company property regardless of the content. The Company regularly audits this material to ensure that all employees are complying with the Company’s IT Security Policy.  The Company has software and systems in place that monitors and records all e-mail messages and Internet sites accessed. ULM Tech Industries reserves the right to inspect any and all files stored in private areas of the network in order to assure compliance with policy. Sexually or racially explicit material may not be displayed, archived, stored, distributed, edited or recorded using the network or computing resources. Use of any Company resources for illegal activity may be grounds for dismissal and the Company will cooperate with law enforcement activity. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-01**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Software Piracy Policy** | | | **Page 3** |
| ***To assure that all software used on Company computers is properly licensed.***  It is Company policy that only properly licensed software is in use on any Company server, laptop or desktop. The Company does not condone pirated software, and specifically prohibits downloading, copying or installing software in violation of the software publisher’s rights.  Employees are not permitted to use the Company’s IT Resources to copy, retrieve or send copyrighted materials unless the employee has the author’s permission or is accessing a single copy only for the employee’s and Company’s own reference .  The Company is committed to the use of only authorized software on its computer systems. All software on the Company’s systems is officially licensed. Any software other than Company approved software requires the authorization of management. Employees must not install/uninstall any software or hardware without authorization of management and must not alter the basic configuration settings on any IT equipment.  Employees may not copy, duplicate, or disseminate any software except as explicitly allowed in the license terms and conditions. The Company has the ability and does check periodically to ensure that all networked and stand alone computers have only approved software loaded on the machines. Any breaches in the use of legal software will be reported to management immediately. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-01**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Password Protection Standards** | | | **Page 4** |
| All employees are responsible for helping to reduce the possibility and consequences of theft of ULM Tech Industries computing resources and the information they contain. All workstations, personal computers and portable computers will be set up with:   * Login ID and password control for individuals only * PASSWORD STANDARDS MUST INCLUDE: | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-01**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Responsibilities** | | | **Page 5** |
| *To establish responsibilities of all ULM Tech Industries employees and Administrators*   1. **Corporate IT Manager**     * Develop and maintain written standards and procedures necessary to ensure compliance with this policy.    * Provide support and guidance to help employees fulfill their responsibilities with this policy 2. **Local Management**   Each Subsidiary has a Local Administrator. Administrators are employees assigned with ensuring all personnel are aware and comply with this policy, and in carrying out IT functions and monitoring IT vendor services and purchases.  All managers and supervisors must immediately notify the HR department (or corporate management) whenever an employee starts, moves or leaves. For new hires, in addition to informing HR of the acceptance of an offer, the request for IT services is to be performed through the “Employee Access Change Form.” This form is also to be used for changes in employee location or other changes in status that require IT support. Separations are to be handled by notifying HR immediately, at which point HR will inform the IT Administrator of this change through the “Separation Form Template.”  IT Administrators must be notified immediately of any staff or departmental movements so that the appropriate hardware, software registers and location maps can be updated. No hardware or software products may be removed from the premises without prior written consent of management.   1. **All ULM Tech Industries employees using IT resources** must know and adhere to these policies. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-01**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **E-mail Usage Standards** | | | **Page 6** |
| The Company’s e-mail system is provided for work related purposes and not for personal matters. Incidental and infrequent personal use during scheduled work breaks is permitted, but not for any purpose inconsistent with the Company’s Code of Ethics. Do not send any information that is illegal, or could be insulting or offensive to another person, such as sexually explicit messages, any cartoons or jokes, unwelcome propositions, ethnic or racial slurs, or any other message that could be viewed as harassment. Any personal emails containing attachments or containing large graphics must be deleted before the daily backup occurs. **The Company reserves the right to delete any non work related files without notice to the user.**  Employees are directed not to open any e-mail attachments if they do not know the source. These attachments are the most common cause of computer viruses. If your anti-virus software detects a virus that it cannot clean, contact your IT administrator. Management sets up all workstations and laptops with anti-virus software and maintains this software and the corresponding virus definitions at the latest levels.  Employees may not use the Company’s Information Resources for any illegal purpose, or any purpose that violates Company policy, that is contrary to the Company’s best interests or that discloses confidential or proprietary information of the Company or third parties. Such activities include creation of unauthorized blogs or personal websites, and accessing unauthorized Internet chat rooms.  COMMON SENSE USES OF E-MAIL  E-mail provides an efficient alternative to communication via phone or mail. However, due to its ease and speed, the volume of messages far exceeds the amount of phone or mail that would have occurred otherwise. Employees are advised to exercise discretion with both the volume of e-mails and the number of recipients.  Keep your messages civil and do not degrade, disparage or use harsh or sarcastic language. An e-mail is equivalent to a permanent, written message. A negative e-mail, taken out of context and in the absence of your intended tone and emphasis, can be very damaging to employee relationships. Jokes and sarcasm do not belong on Company e-mails.  Use CC (carbon copy) to indicate recipients who do not need to take action regarding the e-mail. A CC recipient is only being informed about an event or message, and need not respond or take any action.  If you received unwanted e-mails, add the Sender to the Blocked Senders List so that you do not receive e-mails from this source in the future. Always delete spam and unwanted junk emails immediately.  Minimize the sending of files in which the recipient has the same authorized access on the network as you. Instead, refer the recipient to the file location. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-01**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Internet Usage Standards** | | | **Page7** |
| The Company’s Internet services are provided for work related purposes and not for personal matters. Incidental and infrequent personal use during scheduled work breaks is tolerated, but not for any purpose inconsistent with the Company’s Code of Ethics. Do not access, send or download any information that is illegal, or could be insulting or offensive to another person, such as sexually explicit messages, any cartoons or jokes, unwelcome propositions, ethnic or racial slurs, or any other message that could be viewed as harassment.  Employees are not permitted to use Company resources to access any site containing pornographic subject matter at any time.  PLEASE COMPLETE INTERNET USAGE STANDARDS | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-01**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **PORTAL USAGE** | | | **Page 8** |
| The ULM Tech Industries Sharepoint Portal facilitates exchange of data by posting files in common locations to reduce the transferring of multiple documents to multiple recipients. Access is based on need-to-know and an environment of security is essential. Portal users are not to share passwords, and are not permitted to share data from the portal with any unauthorized individuals.  All data on the portal is considered **Strictly Proprietary and Confidential Data. Unauthorized distribution of data from the Portal is grounds for dismissal.**  Corporate IT issues and controls access to the portal. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-01**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **ULM TECH INDUSTRIES DATA CLASSIFICATION** | | | **Page 9** |
| Company data, consisting of all electronic data and any copies, printouts, reports, e-mails, or verbal communication thereof, is classified into three groups which define the level of security and confidentiality. Employees are required to be aware of these levels and protect Company information accordingly.  **Public Data**  Consists of consolidated summary information formerly filed with the SEC, such as financial reports. Financial information of Company subsidiaries is not Public Data.  **Proprietary Data**  Consists of all financial information generated at the Company subsidiary level, and may only be shared with employees whose positions require financial information. This information is also not to be shared with the public, even if such information can be determined or estimated by other means.  **Strictly Confidential Data**  Consists of all payroll data, acquisition and divestiture information, legal and environmental activities. All acquisition activity is strictly confidential, and ULM Tech Industries employees are required to withhold comment on any potential acquisitions, even if it is apparent that such activity has become Public or Proprietary data. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-01**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **ULM TECH INDUSTRIES IT SECURITY ACKNOWLEDGEMENT FORM** | | | **Page 10** |
| I acknowledge that:   * I have received, read and understand Company Policy IT-01 * I understand and agree that any IT resource provided by the Company contains proprietary and confidential information about ULM Tech Industries and its customers/vendors and that these resources remain the property of the Company at all times. * I will not duplicate any Company information or software. * I will not store inappropriate personal files on Company computers. * I will delete all personal e-mails containing large attachments. * I will not share my passwords with others. * I will return all Company IT resources upon leaving the Company. * I will not participate in unauthorized destruction of Company electronic records. * I understand and will adhere to the 3 levels of data classification.   I understand that any employee found to have violated Company IT policies or failed to make a best effort attempt to comply with these guidelines may be subject to disciplinary action, up to and including termination of employment and possible civil liabilities and/or criminal prosecution.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Employee Name  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Employee Signature Date | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-02**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Company Laptop Usage Policy** | | | **Page 1** |
| ***To control and limit issuance of laptops in order to reduce risk of data theft.***  Despite the obvious flexibility and portability of laptops, they pose an increased and often unnecessary risk of theft or loss of Company property and information. Only qualified and approved employees can possess or use Company laptops. Users must be aware of these risks and follow Company policy on using, transporting and storing laptops.  A lost or stolen laptop containing Company data, and without proper security, represents the single greatest theft risk to the Company. A theft of most other Company assets can be remedied with insurance and replacement equipment, vehicles, etc. A stolen or lost laptop, however, might contain customer lists, employee personal information, potential acquisition data, and financial results not yet released to the public. Misuse of that data can do far more harm to the Company than a stolen or lost truck.  All customer and supplier data must be maintained on Company networks on file servers. Company data on a laptop may only be a copy of data that is present on the Company file server. Any such data on the laptop must be deleted when no longer actively in use.  No customer or supplier databases can be present on the laptop unless data is encrypted and protected by file-specific passwords. Spreadsheets containing sensitive Company data must be password protected.  Laptops must have the automatic password submission disabled so that others cannot easily use a stolen laptop or use it to log into one of the Company’s networks. As a protective measure against misuse of a lost or stolen laptop, users may not use the ‘Remember my Password’ feature for logging into the laptop. If a password shows up as a line of asterisks, it has no security value, and anyone can simply hit ENTER and log in.  Traveling with a laptop is permitted only when absolutely necessary. Laptops must be carried on board aircraft and not checked with baggage. The user is required to take the laptop into a hotel overnight and not leave it in a vehicle.  **Lock up when not in use** – While this is obvious, it is often overlooked. If a laptop isn’t in a physically secure area, then it should be locked away—in a desk drawer, in a closet, etc. Even in your office, laptops might not be safe. Even if it's in an environment you consider safe, realize that cleaning people, security guards and others have keys, and can use them to gain access to your valuables, including laptops and Company data.  **Be wary of wireless** – Wireless networks provide a quick and easy way to connect to the Internet and conduct business, but they also open up potential for data theft when security is not included in the network design. When in a public area on a wireless network, never login to Web sites unless you are using Secure servers (web addresses beginning with HTTPS). | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-02**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Company Laptop Usage Policy** | | | **Page 2** |
| **Report incidents** – If your laptop is lost or stolen, notify the authorities immediately, as well as your manager. If your stolen laptop is used to commit a crime, such as hacking into a bank, the owner of that laptop can be implicated until things are straightened out. Your IT Administrator will take steps to shut down your account or change passwords to protect Company assets. By taking the proper steps and immediately notifying everyone who needs to know, you can stem the loss and can prevent exposing the Company to additional loss or liability.  **Quarantine returning laptops** – When you return your laptop to the office, run your virus and spyware scanning software to make sure it doesn't carry any harmful viruses or spyware. The laptop has been outside the corporate firewall, exposed to wireless and Internet access where spyware and viruses are pervasive.  **Laptop Administration** -Before a laptop is put to use in the field, request your IT vendor to set up an Admin Account and a User Account. Password requirements, screen lock, lockouts, etc. will be set up under the Admin Account. The local IT vendor and/or the local IT Administrator will also ensure that Antivirus software has been purchased, installed and automated on the laptop. The IT Administrator will also make certain that the firewall has been enabled.  **Required Documentation** | | | |
| Laptop Usage Policy agreement must be completed and maintained by Human Resources in Personnel file.  Written approval from Corporate IT required before issuance of any laptop to an employee. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-02**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Laptop Usage Policy Agreement** | | | **Page 3** |
| I acknowledge that:   * I have received, read and understand Company Laptop Usage Policy. * I understand and agree that any the laptop provided by the Company contains proprietary and confidential information about ULM Tech Industries and its customers/vendors and that this resource remains the property of the Company at all times. * I will comply with all password requirements required by the Company * I will not maintain Company information on the laptop unless that data is on the Company network in original form. * I will not duplicate any Company information or software * I will return all ULM Tech Industries IT resources upon leaving the Company. * I will not participate in unauthorized destruction of Company electronic records   I understand that any employee found to have violated Company IT policies or failed to make a best effort attempt to comply with these guidelines may be subject to disciplinary action, up to and including termination of employment and possible civil liabilities and/or criminal prosecution.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_­­\_\_\_\_\_\_\_\_\_\_\_­­\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Employee Name Employee Signature Date  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Local IT Administrator approval Date  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Corporate IT Manager approval Date | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-03**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Change Management – Operating Systems** | | | **Page 1** |
| **Microsoft /Mac Patch Management and Backout (For local IT Administrators only)**  IT administrators may utilize local IT vendor support for these functions, but IT administrators are still responsible for carrying out of Company IT Policy such as forms, notices, etc.  Patch management is the process of controlling the deployment and maintenance of interim software releases into production environments. It helps maintain operational efficiency and effectiveness, overcome security vulnerabilities, and maintain the stability of your production environment.  There have been several widely-publicized attacks and vulnerabilities related to Microsoft and Apple software. Many organizations with proactive security patch management in place were not affected by these attacks, because they acted on information that Microsoft made available in advance of the attack. Microsoft software updates include: Security Patches, Critical Updates, Hotfixes, Update Rollups and Service packs.  The Company’s policy is to document the process of installing Microsoft patches in order to have an audit trail for recovery in the case of software failures or conflicts arising from the patch installation. IT Administrators must complete the Software Patch Update/ Software Customizing Request Form prior to installing patches. A complete backup must also be completed immediately prior to installation of patches in order to facilitate a backout; if eVault is being used as the backup method, patch installation should be carried out at the start of the day before data entry occurs.  **Required Documentation** | | | |
| Software Patch Update/ Software Customizing Request Form | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-03**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Change Management – ERP & Accounting** | | | **Page 2** |
| **Infrastructure Change Controls**  The change management policy and procedure is followed by the local IT Administrator for all infrastructure changes including operating system, hardware and software, firewalls, and routers that affects the computing and communications infrastructure.  All infrastructure changes are documented on a change request form and approved by management prior to making the change. If a change requires testing, a test plan or equivalent is developed. The test plan will include the purpose of the change and, for executing the test, the anticipated test results, and actual results. Testing is typically performed on a designated test server or equivalent computer hardware (if available) first for impact to environment and functionality. Upon successful test results, the change is then implemented into production. System changes are communicated to the impacted user community as necessary. If system downtime is required and is expected to impact availability to a business function, a notification email will be sent in advance.  **New Software**  New software may only be purchased after obtaining written permission from Corporate IT via fax or email. Process for choosing new software will be discussion between users, local administrators, and corporate IT administrator. Corporate involvement is required to assure consistent use and procedures among subsidiaries, and to assure compliance with existing IT polices.  **Emergency/unscheduled Changes**  The Company allows emergency changes as part of the change management policy. Since emergency changes require immediate resolution by local or Corporate IT Administrators, the change is made and all documentation and approvals are completed within 2 days after the emergency has been resolved.  **CUSTOM CHANGES TO MACOLA or SHARED LOGIC SOFTWARE**  No customized software or changes to existing software can be made to Company approved ERP applications without specific approval from corporate IT. A formal timetable of when ERP upgrades occur is dependent on the ERP system in use. Each administrator must perform software upgrades according to the schedule below and then inform Corporate IT via email that the upgrade has been performed.  Any proposed changes must be communicated to and discussed with Corporate IT and the Software Customizing Request Form must be used. All changes must be accompanied by revised documentation. The revised documentation must be requested and included in the proposed change and contract with software vendor. | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-03**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Change Management – ERP & Accounting** | | | **Page 3** |
| **Enterprise Resource Planning (ERP) Software Updates**To standardize ERP software upgrades and assure that upgrades are tested if necessary.  A formal timetable of when the Company will upgrade ERP is dependent on the ERP system in use.  Each administrator must perform software upgrade according to this schedule, and then inform Corporate IT via e-mail that the upgrade is done. All upgrades must be preceded by a complete backup of data files.  MACOLA – Upgrades are provided annually, or upon significant error fixes, or upon creation of customized changes specifically for ULM Tech Industries. All upgrades provided by MACOLA are to be installed.  SHARED LOGIC – Shared Logic provides weekly upgrades, accompanied by Release Notes explaining all changes. ULM Tech Industries policy is to only install upgrades in the first week following the end of a quarter, and at other times upon request from Corporate IT. All upgrades will be made on a specific day provided by Corporate IT so that all subsidiaries using Shared Logic are using the same version.  OTHER ERP/GENERAL LEDGERS- Upgrades are typically only performed annually or less frequently. Automatic upgrading to newest version is NOT required, especially if new features are not used by ULM Tech Industries. Any upgrades must be requested by administrator and approved by Corporate IT before ordering of software.  COMMERCIAL SOFTWARE – Off-the-shelf packages, such as Microsoft Office or Visio, can be upgraded at local administrator’s option, as long as prior notice is made to Corporate IT. The version upgrade notice is not a request for approval, but merely serves to assure that Corporate IT is aware of software in use. In the case of patches, such as the continuous patches Microsoft sends for network server and e-mail server software, the IT administrator, with possible assistance of local IT vendor, is responsible for installing all patches after completing a backup of all system and data files.  Local IT administrators have authority to purchase licenses for additional users to ERP systems, as long as corporate IT is informed via e-mail.  **Required Documentation** | | | |
| 1. IT-03 Upgrade Form sent to Corporate IT indicating the upgrade has been performed. 2. Written or e-mail request to upgrade ERP or General Ledger software. 3. Notice to Corporate IT of purchase and /or upgrade of commercial software. 4. Software Patch Update/Software Customizing Request Form. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-03**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Accounting Upgrade Confirmation Form** | | | **Page 4** |
| In order to confirm integrity of ERP system before and after upgrade, retain printed proof of the following figures. Complete the form and fax form to Corporate. | | | |

|  |  |  |
| --- | --- | --- |
| Benchmark Data | Pre-Conversion | Post- Conversion |
| TOTAL ASSETS |  |  |
| TOTAL LIABILITIES |  |  |
| TOTAL A/R PER G/L |  |  |
| AR AGING TOTAL |  |  |
| TOTAL A/P PER G/L |  |  |
| YTD NET INCOME |  |  |

The ERP upgrade has been performed and all benchmark data confirmed.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Controller Date

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policy IT-03**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** | |  |  |
| **Operating System and ERP/Accounting Upgrade Confirmation Form** | | | | **Page 5** |
| New Project  Enhancement Emergency  Patches/Fixes | | **Requested by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | | |
| **Describe New/Enhancement/Emergency:** | | | | |
| **Management Approval :** | | **Approval Date:** | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-04**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Backup and Recovery** | | | **Page 1** |
| Effective October 2007, the Company began using Evault for offsite backup via high speed internet. This backup procedure satisfies the Company’s requirements for Backup and Recovery, but the IT Administrator still has the responsibility to check each day for successful results of the prior backup and to maintain the Daily Backup Log.  All data on Company IT systems must be backed up on a daily basis, covering all days that the system is used, including days open on weekends. Responsibility for backing up resides with the local IT Administrator. This protects the Company from losing valuable information due to hardware failures. Back-ups must always be secured when unattended so that sensitive information cannot be compromised.  Quarterly tests to restore information from back-up files must be performed to ensure information is usable and readable. The test of the Uninterruptible Power Supply for the server is combined with this quarterly test. See more detail at IT-04 Page 2.  When information is stored locally on a user’s own hard drive (**C:** drive), it becomes the responsibility of local management to ensure sensitive, critical and valuable information is securely backed up in accordance with established procedures and internal controls. NOTE: Data stored on a local drive is not backed up when ULM Tech Industries backs up its servers. All data users’ work that is considered sensitive, critical and valuable data must be stored on a network drive so the data is backed-up.  All laptop users must ensure that the data held on the laptop is regularly backed up to a network server.  A Daily Backup Record must be used as a log for evidence that the backups are being performed. However, if Evault is used, automatic daily email notification must be selected, and each local administrator will review and retain for 12 months all Evault emails as an electronic record of the backups. Any FAILURES noted must be resolved immediately by reviewing the LOG on the online website. The cause of FAILURE should be corrected before the next scheduled backup occurs. If 2 consecutive FAILUREs occur, notify Corporate IT immediately. WARNINGS and ERRORS relate to files in use or other non-critical errors. Any WARNING or ERROR repeated on 2 or more consecutive reports must be investigated.  Daily backups are to be retained for at least 30 days, and monthly backups for 12 months. Evault should be configured to retain 30 days and 12 months of backup.  If Evault is not used, the log needs to be printed and posted near the server or at the System Administrator’s desk. The log can be created in Excel or handwritten, but the following columns are required:  DATE | PERFORMED BY | BACKUP LABEL | EXCEPTIONS NOTED | ACTION TAKEN | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-04**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Backup and Recovery** | | | **Page 2** |
| **A. TESTING AND REVIEW SCHEDULE**  **Responsibility:** System Administrator  **Time Requirement:** Quarterly, during the mid-month of each Quarter  **Process:** Restore 20 files from various folders contained in the backup. Do not restore to original location. Restore to a folder on local drive of System Administrator. Upon successful restore, delete restored files from local drive of System Administrator and ***send an email*** to Corporate IT Administrator noting that the test was completed successfully. If any failures occur, notify Corporate IT Administrator to request assistance to investigate and resolve failure. | | | |
| **B. TESTING OF UPS**  **Responsibility:** System Administrator  **Time Requirement:** Quarterly, during the mid-month of each Quarter, after test of Recovery  **Process:** Choose a time when no users are in the system, and close any current applications on server. Unplug server UPS unit from outlet and assure that UPS unit provides at least 5 minutes of power.  **Required Documentation**  Daily Backup Log Form, created locally  Testing and Review Schedule (See IT-04 Page 2) | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-05**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Virus Detection Software** | | | **Page 1** |
| Local IT Administrator sets up all workstations and laptops with anti-virus software and maintains this software at the latest levels. This is automatically updated on all devices. Laptop users must make sure that they always have the latest version of anti-virus installed.  The Company licenses virus protection software for use on all devices within the Company. As part of the license, the Company automatically receives updates to the anti-virus software and the corresponding virus definitions on a regular basis or when new viruses are detected. This is automatically updated on all devices except personal computers that are not currently attached to the network; in which case it is the responsibility of each individual to ensure he or she keeps the PC loaded with the latest version of the anti- virus software. Laptop computer users must take extra care to ensure they have the latest anti-virus software, as they are not always directly connected to the network.  Employees must not open any email attachments if they do not know the source. These attachments are the most common cause of computer viruses. If the anti-virus software detects a virus that it cannot clean, contact Corporate IT Administrator.  **Firewalls**  All laptops must have a firewall enabled. Windows users can activate the Windows Firewall through their Control Panel and Security Center.  A monthly Security Log Review Form must be used as a log for evidence that the Security Log reviews are being performed. The local IT Administrator has responsibility for maintaining the Security Log Review. The log must be available for audit. The log can be maintained on disk, created in Excel or handwritten, but the following columns are required:  WEEK REVIEWED | PERFORMED BY | RESULTS | EXCEPTIONS NOTED | ACTION TAKEN |  **Required Documentation** | | | |
| Monthly Windows Security Log Review, created locally | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-06**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Computer Room Access** | | | **Page 1** |
| Company IT equipment must be protected from unauthorized access and harm. The sensitivity of informational assets requires strict controls over who can use equipment that accesses those assets.  The following policies are designed to protect and preserve Company IT equipment:   * Servers, networking devices, communications infrastructure components (e.g., communications hardware, wiring, modems), and backup tapes must be stored in secure enclosures—whenever possible, in a locked closet or room. * All software CDs, keys, and configuration instructions must be removed, whenever possible, from the equipment that reads them and stored in a secure location for use by authorized personnel. * Physical access to the computer room will be limited to those persons authorized by the local IT administrator as persons responsible for managing and supporting the equipment located therein.   **Equipment protection**   * A “no food or beverage” policy must be enforced in the computer room. * Uninterruptible Power Supply (UPS) units must be in place and tested quarterly. * A currently inspected fire extinguisher must be within close reach of the server or server room. * No unapproved equipment may be attached to any authorized configuration of networked equipment, except for testing and installation tools operated by vendor or telephone Company personnel for the express purpose of installing, testing and/or maintaining the authorized equipment.   **Required Documentation** | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-07**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Administration** | | | **Page 1** |
| This policy sets forth periodic reviews which are the responsibility of each local administrator.  **1. User Administration**  Managers must notify local IT Administrators immediately whenever an employee starts, moves or leaves. For new hires, job changes or terminations, the request for IT services is to be evidenced by an email. This email will document the IT services added or removed for the employee and evidence the proper approvals for the access.  **2. Annual Review of Network Folder access Due: 1st week of December**  A printout of network login ID’s and their access rights must be reviewed and approved by local administrators, and forwarded to Corporate IT. The users in Active Director must reflect only valid active users required to have access to the network. The WORKSTATION list must also be maintained so that all workstations listed are current.  **3. Annual Review of ERP Due: 1st week of November**  The purpose is to periodically review the access rights of users to critical Company financial applications and networks. Two aspects of this review are critical. First, identify users who have access to the application or network. Second, determine if those users having access to the application have rights appropriate to their roles and responsibilities.  ERP access must be reviewed annually by the local controllers. The controller prints out the current access lists for the financial applications, and then review each user’s access for accuracy and appropriateness. Access changes should be documented on the access list. Once the access review is complete, the controller must sign and date the access list and have available for audit purposes.  **Required Documentation** | | | |
| Employee Access Change Form for adding, changing and deleting user access rights  Email sent to Corporate IT confirming that annual review of Network Folder Access and ERP access has been completed. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-07**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Administration** | | | **Page 2** |
| 1. **Annual IT Audit/Risk Assessment. Due: between September and December**   A full review of policies and procedures, change management, backup and recovery, and user access (SOX IT Audit). Risk assessment is to be performed by professional firm approved by Company’s outside auditors. Coordinate timing with Corporate IT Administrator.   1. **Vendor Management**   All invoices for equipment and service need approval by Corporate IT, with Submission via fax or attachment to email, and approval returned via email.   1. **Default Windows Server**   Default windows password for Administrator must be changed.   1. **Windows Audit Log Policy Settings**   The following Audit log policy settings are required according to the recommended Windows Server 2008 Security Guide:   * 1. Audit System Events set to “Success”   2. Audit account management set to “success/failure”   3. Audit directory service access set to “success/failure”   4. Audit logon events set to “success/failure”   5. Audit privilege use set to “success/failure”   6. Audit Object access set to “Failure”   Audit logs must be reviewed monthly and an electronic copy retained for a period of six months.  **Required Documentation** | | | |
| Employee Access Change Form for adding, changing and deleting user access rights  Email sent to Corporate IT confirming that annual review of Network Folder Access and ERP access has been completed. | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policy IT-07**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** | |  |  |
| **EMPLOYEE ACCESS & CHANGE FORM** | | | | **Page 3** |
| New Terminated  Change  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | |
| Employee Name & Title: | | ULM Tech Industries Subsidiary & Department | | |
| Equipment Issued or Returned | | Software Access | | |
| Manager Approval | | Approval Date | | |
| Administrator Signature | | Date | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-08**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **Accounting System Standards and Tests** | | | **Page 1** |
| **Future Period Journal Entries –** To reduce duplication risks, journal entries should not typically be entered in periods beyond the current and following month. At each June 30 and December 31 closing, controllers must run trial balances for future periods to ensure no future activity has been posted in error and communicate results to corporate IT via an email.  Controllers are encouraged to check regularly for future entries made in error.  **Required Documentation** | | | |
| Semi-annual emails to corporate IT. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-09**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **IT Steering Committee** | | | **Page 1** |
| The Company’s Management will appoint a standing IT Steering Committee whose members will be employees of the Company or its subsidiaries. The Committee will be responsible for:   1. Reviewing the Company’s IT policies as in effect from time to time and, to the extent warranted in the determination of the Committee, promulgating, revising or supplementing such policies, subject to the approval of Management; 2. Coordinating the allocation and operation of IT Resources throughout the Company; 3. Monitoring the Company’s IT requirements and advising the Company’s Management thereon; 4. Monitoring the efficiency and performance of the Company’s IT Resources; 5. Supervising the Company’s compliance with external standards applicable to its IT functions; and      1. Such other functions reasonably related to the monitoring and operation of the Company’s IT Resources as the Committee may determine.   The Committee will meet, either in person or telephonically, not less than quarterly and will report on the status of the Company’s IT Resources and requirements to Management, in such manner as the Committee and Management will determine, at least once each year but more frequently if circumstances necessitate. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy IT-10**  **Effective 6-23-2010** | **ULM TECH INDUSTRIES POLICY MANUAL** |  |  |
| **AS400 Controls** | | | **Page 1** |
| The following policy sets forth periodic reviews for the AS400 and are the responsibility of the local administrator.  **1. Annual Review of AS400 Users Due: 1st week of November**  ULM Tech Industries will conduct annual user and access level reviews for all AS400 users including QSECOFR and ALLOBJ users. AS400 Object owners will also verify that only authorized users have access to their objects. The local administrators will review and approve access, and forward a printout to Corporate IT. Any conflict of access rights identified should be immediately resolved. Corporate IT will retain the access list and have available for audit purposes.  **2. AS400 Server**  Default password for Administrator must be changed.  **3. Audit Log Policy Settings**  The following Audit log policy settings are required according to the recommended IBM AS400 Security Guide:   * Access to objects, files and tables * Login attempts * Modification of objects and user privileges * System configuration changes   Audit logs must be reviewed monthly and an electronic copy retained for a period of six months.  A monthly AS400 Security Log Review Form must be used as a log for evidence that the Security Log reviews are being performed. The local IT Administrator has responsibility for maintaining the Security Log Review. The log must be available for audit. The log can be maintained on disk, created in Excel or handwritten, but the following columns are required:  WEEK REVIEWED | PERFORMED BY | RESULTS | EXCEPTIONS NOTED | ACTION TAKEN |  **Required Documentation** | | | |
| Email sent to Corporate IT with Printout confirming that annual review of AS400 users has been complete.  Monthly AS400 Security Log Review, created locally | | | |