COLORADO
CONVENTION CENTER

END USER COMPUTING POLICY

ASM Global provides Team Members with access to multiple forms of electronic media and services, including but not limited to computers, e-mail, company intranet, Internet, external electronic bulletin boards, online services, wire services, telephones, voicemail, fax machines, and the World Wide Web. The purpose of this policy is to establish acceptable and unacceptable use of such electronic media and network resources at ASM Global and its managed facilities in conjunction with its established culture of ethical and lawful behavior, trust, and integrity.

ASM Global provides computer devices, networks, and other electronic information systems to meet company goals and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires Team Members to comply with company policies and to protect the company against damaging legal issues.

ASM Global encourages the use of these media and associated services because they can improve the efficiency and effectiveness of communications and because they are valuable sources of information about vendors, customers, technology, and new products and services. However, all Team Members and everyone connected with the organization should remember that electronic media and services provided by the company along with the information stored on them are company property and their purpose is to facilitate and support company business. All computer users have the responsibility to use these resources in a professional, ethical, and lawful manner.

To ensure that all Team Members are responsible, the following policies and guidelines have been established for using ASM Global's electronic media, services and resources. No policy can lay down rules to cover every possible situation. Instead, this policy is designed to express ASM Global philosophy and set forth general principles when using electronic media, services, and resources.

Access to Team Member Communications and Equipment

For security, compliance, and maintenance purposes, authorized personnel may, at any time and without notice, monitor and audit equipment, systems, system usage, and network traffic. Team Members have **no expectation of privacy** in any company equipment, systems, system usage, network traffic, or any documents or information created or accessed therefrom.

ASM Global reserves the right, at its discretion, to review any Team Member's electronic files, messages, email and usage history, or any other aspect of the electronic information systems to the extent necessary to ensure electronic media and services are being used in compliance with the law, in compliance with this policy, and in compliance with other company policies. All files, email, voicemails, and other media are ASM Global property and ASM Global reserves the right to access and review Team Member files, email, voicemail, and other media at any time without prior notice.

Team Members should not assume electronic communications are completely private. Accordingly, when transmitting sensitive information, other means should be considered and employed as the individual situation warrants.

Ownership of Equipment and Data

All hardware and software provided to Team Members by ASM Global remains the sole property of ASM Global. All data and information residing on or created with ASM Global equipment is ASM Global property. ASM Global reserves the right to access any personal devices on which company data and information is or has been stored. Each Team Member agrees to grant ASM Global's representatives' access to any such personal devices promptly if requested.

Team Members are responsible for ensuring the protection of assigned ASM Global assets. Any theft or loss of ASM Global assets including but not limited to laptops and business phones must be reported to the IT Department within 24 hours. ASM Global may, at its discretion, hold Team Members personally responsible for the cost of lost equipment.

Team Members must remain vigilant when handling company information and files. Any accidental deletion of files must be reported to the IT department immediately upon discovery or realization of the problem so that recovery efforts can commence.

Prohibited Communications

Electronic media, services and resources may not be used for transmitting, retrieving, or storing any communication that is:

- Discriminatory or harassing;
- Derogatory or offensive to any individual or group;
- Obscene, sexually explicit, or pornographic;
- Defamatory or threatening;
- In violation of any license governing the use of software;
- Engaged in for any purpose that is illegal; or
- Contrary to any ASM Global policy or business interest.

Any Team Member with knowledge of a violation of this policy must immediately report the violation to the Human Resources department.

Appropriate Use of Resources

ASM Global provides its Team Members with computers, electronic media and services to assist them in the performance of their jobs. Use of this equipment must be done in a manner that neither negatively affects the systems' use for its business purpose nor negatively affects or impacts the performance of the Team Member's job responsibilities or the performance of any other Team Member's job responsibilities. Each Team Member's supervisor is responsible for identifying whether job performance is affected by abuse of this policy. Team Members are required to exercise good judgment regarding appropriate use of ASM Global resources in accordance with all ASM Global policies, standards, and guidelines. ASM Global resources may not be used for any unlawful or prohibited purpose.

Blogging and Social Networking

It is the responsibility of the company to protect itself from unauthorized disclosure of information. This policy is intended to provide our Team Members with guidelines established to address company-authorized social networking and personal social networking. While the company respects a Team Member's privacy, conduct that had or has the potential to have a negative effect on the company might be subjected to disciplinary action up to and including termination, even if the conduct occurs off the property or not on company time.

These guidelines are referring to all forms of social media technology, including but not limited to: blogs; wikis; RSS feeds; social networking sites such as Facebook, LinkedIn, or Instagram; video and photo sharing websites such as YouTube; microblogs such as Twitter, chat rooms, personal blogs or other similar forms of online journals, diaries, or personal newsletters affiliated and/or not affiliated with ASM Global.

Authorized Social Networking

The goal of authorized social networking and blogging is to become a part of the industry conversation and promote web-based sharing of ideas and exchange of information. Authorized social networking and blogging is used to convey information about company events and services, promote and raise awareness of the ASM Global brand, search for potential new markets, communicate with the public and issue or respond to breaking news.

When social networking, blogging or using other forms of web-based forums, ASM Global must ensure that use of these communications maintains our brand identity, integrity, and reputation while minimizing any types of risk. Facilities should designate authorized Team Members who can prepare and modify content for ASM Global's blogs and/or company social networking entries.

Each facility is responsible for ensuring all blogging and social networking information complies with ASM Global's policies. ASM Global reserves the right to remove any content that does not meet the rules and guidelines of this policy or that may be illegal or offensive. Removal of such content will be done without permission of the blogger or advance warning. ASM Global also reserves the right to take legal action against persons who engage in prohibited or unlawful conduct.

Non-Authorized Social Networking

Team Members should not use employer-owned equipment, including computers, company business phones, company-licensed software, or other electronic equipment for non-authorized social media technology. Nor should Team Members use our facilities and/or company time to conduct personal blogging or social networking activities.

Team Members should be certain not to post company or client-privileged data, including but not limited to copyrighted information or trade secrets.

ASM Global respects the right of Team Members to write blogs and use social networking sites and does not want to discourage Team Members from self-publishing and self-expression. However, Team Members are expected to follow the guidelines and policies set forth to provide a clear line between you as the individual and you as the Team Member. ASM Global does not discriminate against Team Members who use this type of media for personal interests and affiliations or other lawful purposes.

If you choose to identify yourself as an ASM Global Team Member, please understand that some readers may view you as a spokesperson for ASM Global. Because of this possibility, we ask that you state that your views expressed in your blog or social networking area are your own and not those of the company, nor of any person or organization affiliated or doing business with ASM Global.
Team Members cannot use blogs or social networking sites to harass, threaten, or discriminate against Team Members, vendors, clients and/or anyone associated with or doing business with ASM Global.
Bloggers and commenters are personally responsible for their commentary on blogs and social networking sites. Bloggers and commenters may be held personally liable for commentary that is considered defamatory, obscene, proprietary or libelous by any offended party.

Discipline for Violations

Violations of ASM Global's social networking policy may result in disciplinary action up to and including immediate termination even if the conduct occurs outside of company time, off company property and/or not on employer owned equipment. ASM Global reserves the right to take legal action where necessary against Team Members who engage in prohibited or unlawful conduct.

Employer Monitoring

Team Members are cautioned that they should have no expectation of privacy while using the internet. Your postings can be reviewed by anyone, including ASM Global. ASM Global reserves the right to monitor comments or discussions about the company, its Team Members, clients and the industry, posted on the internet.

If you have any questions relating to this policy, please see your manager and/or your local Human Resources Department

Data Security and Network Integrity

Team Members are responsible for the security of data, accounts, and systems to which they have access. Account information and passwords must be kept secure and should not be shared with anyone. Passwords must be at least six characters in length and must contain at least one number and one letter. It is ASM Global policy for all users to change their passwords at least twice each calendar year. In the rare occasion where a Team Member must reveal their password to another Team Member (ex., IT Support, while out on vacation and supervisor needs access, etc.) it is the responsibility and obligation of the Team Member to request a password change.

Any theft or loss of ASM Global asset(s) including but not limited to laptops and business phones must be reported to the IT Department within twenty-four (24) hours. Equipment falling into the wrong hands presents an opportunity for unauthorized access to ASM Global data, accounts, and systems.

Personally, identifying information such as Social Security Numbers, credit card numbers, addresses, etc. must not be stored on portable devices such as notebooks, portable hard drives, flash drives, etc. If such information must be sent, the file must be properly encrypted. Team Members needing to engage in this type of file transfer should consult with the IT department to ensure compliance.

Team Members must respect the confidentiality and privacy of other individuals' electronic communications. Except in cases where explicit authorization has been granted by company management, or in conjunction with the monitoring and enforcement of these policies or other ASM Global policies, Team Members are prohibited from engaging in, or attempting to engage in:

- Disabling or circumventing any programs or filters such as anti-virus programs, firewalls and web-blockers that are part of the ASM Global network;
- Adding devices such as wireless access points or routers to the network without first consulting with the IT department;
- Monitoring or intercepting the files or electronic communications of other Team Members or third parties;
- Hacking or obtaining access to systems or accounts they are not authorized to use;
- Using other people's log-ins or passwords;
- Breaching, testing, or monitoring computer or network security measures;
- Tampering with any software installed by ASM Global;
- Formatting or “wiping” a computer or other electronic device;
- Malicious deleting or deliberate altering of data;
- Reinstalling an Operating System or intentionally restoring a PC to a previous state;
- Unauthorized sharing of data or network resources.

No email or other electronic communication may be sent in a manner that attempts to hide the identity of the sender or represent the sender as someone else.

Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use ASM Global's systems and resources.

Social Engineering and Network Security

ASM Global's data network is the potential target of hackers that may want to infiltrate it for a variety of reasons including but not limited to:

- Performing acts of random or targeted malicious damage;
- Theft of company confidential information;
- Identity theft or theft of personal Team Member information;
- Gaining status among other hackers or to prove how smart they are.

While ASM Global has implemented many safeguards to limit the hacker threat, the most difficult method of hacking to prevent is called social engineering. This refers to an act in which a hacker tricks a user into disclosing a password or other sensitive information. Some examples are:

Phone calls: A hacker will call up and pretend to be someone in a position of authority or relevance and gradually pull information out of the user. Some common roles that may be played in impersonation attacks include: a repairman, IT support, a manager, a fellow Team Member, or a trusted third party (for example, claiming to be the CEO's executive assistant calling to say that certain information is needed by the CEO).

Phishing: An e-mail message arrives that appears to come from a legitimate source such as a service provider or financial institution. The e-mail message may ask the user to reply with sensitive data, or to access a Website to update information such as a bank-account number. These fake Websites look realistic enough to fool many victims into revealing data that can be used for identity theft.

Contests and coupons: A hacker group sets up websites advertising a bogus sweepstakes or offering discount coupons or travel deals. They require anyone registering for the sweepstakes to supply a username and password for future access to the site. Soon a database of thousands of usernames and passwords is compiled. Since many people use the same user name and password for multiple sites, a program then systematically attempts to log on too many popular websites using the supplied usernames and passwords. The hacker group can then use details from these sites to gain more information. For example, if a hacker can get into a person's Hotmail account, they might be able to figure out where the person works and then may try to break into that company's computers using the person's logon name and password.

Remote assistance: Someone calls a user claiming to be from the IT department and asks if they can connect to the computer via remote assistance to load a security patch. After the connection is made, a spyware module is loaded onto the machine. The spyware module then collects username and password information and silently e-mails them to the hacker.

Many of the policies in this document are intended to limit ASM Global exposure to social engineering threats. However, it is critical that users are aware of the types of threats that exist and that they are always suspicious of any inbound requests for data or system access of any kind.

Any suspicious calls or emails, especially those asking for passwords, user names, financial information, payments or wire transfers, network access information or other confidential information must be reported to the IT department immediately. Never provide passwords, usernames, account information or other potentially confidential data to a 3rd party unless you are 100% certain that the request is legitimate and warranted, or act on such information to wire funds or otherwise send payments. When in doubt, ask the IT department for assistance.

Licensing and Copyrights

Downloading or installing any unauthorized or unapproved software and or hardware is strictly prohibited. All software and or hardware must be properly licensed and approved for purchase and use by department management or the IT Department.

Programs or software used to illegally copy, hack, or bypass proper licensing and or software activation are forbidden.

Sharing, copying or duplicating any software or copyrighted material without proper licensing or permission is a violation of ASM Global policy.

Anyone obtaining electronic access to materials owned by other companies or individuals must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

Violations

Any Team Member who abuses the privilege of their access to electronic media and services, computers, e-mail, intranet, Internet, external electronic bulletin boards, online services, wire services, telephones, voicemail, fax machines, the World Wide Web and any other technology provided to them will be in violation of this policy and will be subject to corrective action, including possible termination of employment, legal action, and criminal liability.