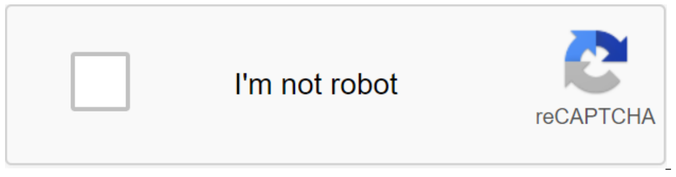
Acceptable use policy pdf



Continue

Updated on September 16, 2016, this acceptable use policy (this policy) describes the prohibited use of web services offered by Amazon Web Services, Inc. and its affiliates (Services) and a website located at (AWS Website). The examples described in this Policy are not exhaustive. We can change this Policy at any time by posting a revised version on the AWS website. Using services or access to the AWS site, you agree with the latest version of this Policy. If you violate the Policy, authorize or assist others, we may suspend or discontinue your use of the Services. You may not use or encourage, encourage, facilitate, or instruct others to use AWS Services or website for any illegal, harmful, fraudulent, infringing or abusive use, or transfer, store, display, distribute or otherwise make available content that is illegal, harmful, fraudulent, infringing or offensive. Prohibited activities or content include: Illegal, harmful or fraudulent activity. Any activity that is illegal, which violates the rights of others, or which may be harmful to others, our operations or reputation, including the distribution, promotion or promotion of child pornography, offering or distributing fraudulent goods, services, schemes or promotions, make money fast schemes, ponzi and pyramids, phishing, or pharmaceutical. Violation of content. Content, infringing or appropriating the intellectual property or own rights of others. Content that is defamatory, obscene, offensive, invasive private, or otherwise undesirable, including content that constitutes child pornography, refers to bestiality or depicts sexual acts without consent. Harmful content. Content or other computer technologies that may damage, prevent, secretly intercept or expropriate any system, program or data, including viruses, Trojan horses, worms, time bombs or the cancellation of bots. You cannot use the Services to disrupt the security or integrity of any network, computer or communications system, software or network or computing device (each, system). Prohibited activities include: Unauthorized access. Access or use of any system without permission, including attempting to probe, scan or verify system vulnerabilities or breach any security measures or authentication used by the system. Interception. Monitoring data or traffic through the system without permission. Falsification of origin. Form TCP-IP packages, e-mail blanks, or any part of a message describing its origin or route. Legal pseudonyms and anonymous remakes are not prohibited by this provision. You can't connect online with users, hosts, or networks unless you have permission to communicate with them. Prohibited activities include: Monitoring or crawling. Monitoring or crawling that degrades or disrupts the system that is monitored or scanned. Denial of service (DoS). Flooding the target with communication requests, so the target either can't respond to legitimate traffic or reacts so slowly that it becomes inefficient. Deliberate intervention. Interference in the proper functioning of any system, including any deliberate attempt to overload the system with postal bombardment, news explosions, broadcasts or flooding methods. Some network services are operating. Network operating services such as open proxies, open email relays, or open domain name recursion servers. Avoiding systemic constraints. Use manual or electronic means to avoid any usage restrictions imposed on the system, such as access and storage restrictions. You will not distribute, publish, send, or facilitate the sending of spam or other messages, promotions, ads, or requests (such as spam), including commercial ads, and information ads. You will not change or hide mail blanks or assume the identity of the sender without the sender's explicit permission. You will not collect responses to messages sent from another ISP if these messages violate this policy or acceptable usage policies. We reserve the right, but do not undertake to investigate, any violation of this policy or misuse of the AWS Service or website. We may: investigate violations of this Policy or misuse of the AWS Service or website; or delete, disable, or modify any content or resource that violates this Policy or any other agreement we have signed with you to use the AWS Services or Website. We may report any activity that we suspect violates any law or regulation to the relevant law enforcement officials, regulators, or other relevant third parties. Our reporting may include disclosure of relevant customer information. We may also cooperate with relevant law enforcement, regulators or other relevant third parties to assist in the investigation and prosecution of unlawful conduct by providing network and system information related to alleged violations of the Policy. If you become aware of any violation of this Policy, you will immediately notify us and provide us with assistance, as suggested, to stop or correct the breach. To report any violations of this policy, please follow our abuse reporting process. Acceptable use policy sets rules the company's networks and devices. This will protect your business from dangerous behavior plus bringing offenders to justice. While AUP helps train employees on issues such as password protection and online security, it also serves as an important legal function for the company. If an employee uses the company's network for unauthorized personal activities, having an AUP on the ground can help prevent (or (or any legal issues that may arise... (cnbwaco.com) Follow along with our guide to create a robust, acceptable use policy for business. OUTLINE SECTIONS What are the six key elements of AUP? We recommend that each policy include these sections: Review - a high-level description of the purpose of the document and key definitions of takeaway - to identify any terms that may be confused, and explain words or phrases, unique to your business Sphere - what the policy does and does not cover and what situations it applies to policy - the meat of the document, in sections that cover use and behavior for each category of performance - the consequences for non-compliance with standards, and how employees will be responsible for changing and tracking - create a schedule to go back to the document and don't forget to track any changes Make things easier with an acceptable policy template using the Spelling acceptable use policy from scratch for a very long time and, frankly, not being necessary. Why not start with the template? You can find a lot for free on the internet. Here are some acceptable examples of use policies and templates to explore: An example of the PearlSoftwareSample Internet Acceptable Use Policy Policy Policy by GFI SoftwareSample Acceptable Use Of Policy through SpiceWorks (includes phrases for HIPAA-compatible businesses) An example of an acceptable use policy for schools from TeacherVisionComputer Using a Policy Pattern from the Association of Corporate Advisors Accepted a Use Policy template for business to decide what applies to your company. Even if you start from scratch, consider these integral points: Using the Internet Which websites should be banned during working hours? Many are obvious, such as pornography or gambling, but what about Spotify or news sites? Do some people, such as your marketing team, need access to social media? Be sure to outline acceptable behavior for sites like these that have the potential for abuse. Some common restricted websites are: Social Media (Facebook, Twitter, Pinterest, Instagram, Tumblr, Reddit, Flickr) Streaming video/music websites (YouTube, Vimeo, Vevo, Twitch, Pandora, Spotify) Search for work sites (Really, Monster, Craigslist, CypRecter, Snagajob) Shopping (eBay, Amazon, Alibaba, etsy, Overstock) News (MSN, Yahoo, TIME, USA Today, New York Times, Washington Post, Huffington Post, CNN, Fox, NBC, BuzzFeed, Upworthy, Distractify) Decide what works for your business and update it as needed. Safety Is Another Important is safety. Outline the best practices that employees should follow when using company devices. Here are some of our security security Recommendations: Never allow the use of public Wi-Fi on company devices, employees should never share passwords and frequently change them (at least once a month). Be sure to set standards for acceptable, secure passwords too. Create a schedule for antivirus, antivirus, and software updates company Employees should never open email attachments or links that they do not expect. If a suspicious email is received, who should the staff send it to for review? Consider the need for two-factor authentication for programs and applications that support it, if they are not used for business purposes, we recommend not to use social networks on the company's devices. Many cases of malware and phishing occur through social networks. Each company has different security needs - make sure yours is carefully identified and cover all networks and devices. Don't forget to include a physical safety policy. How do I keep my devices safe, stored, and transported? Confidential data your business probably contains a large amount of both sensitive and proprietary data. Customer, employee, product, service and other business details are important for proper handling. You should start by finding out what this sensitive data is in your business. From there, explain the proper standards for accessing, sharing, storing and processing this information. React to Incidents Don't Forget about this important section! No company is 100% airtight. If something happens, what is your response plan? Who should be notified and which departments are involved in the recovery? We strongly recommend that employees do not retaliate for notifying management of a potential security incident. If something happens, it will be a problem whether the employee is trying to hide it or not. Everyone makes mistakes. And you'll have a better chance of a quick recovery if you know about the incident sooner rather than later. Note that the error is very different from malicious intent. Intentional infringements certainly shouldn't be protected (but again, we doubt bad actors will notify you anyway!) Guest Access Does your company offer guest WiFi/Internet access? If so, you want to set standards and safe policies for guest access. This may cover customers, suppliers, or partners visiting your business location. To do this, we recommend creating a guest network. This ensures guests only have access to what they need, not your company's internal network and files. E-mail is an important tool for every modern business. Its proper use for your company should be clear. Is your allowed Use your work email for personal use? What are the appropriate standards of business communication, both within and outside the country? We recommend including in the overall best use section as well. Some employees may not be aware of the many threats that come through email - phishing, fraud, fraud, malware/viruses. Take the time to educate your team on how to detect, avoid and handle potential threats. DECIDE ON AUP ENFORCEMENT AND VIOLATION STANDARDS This section is important to view in the template. What works for one company may not be appropriate for yours. Some companies are canceling Internet access for repeat offenders. But it may not be possible in your business. We recommend working with your management or executive team to determine acceptable consequences. Consider the different severity of the various violations. And make sure you have the ability to act in accordance with these policies. Without standardized enforcement, your AUP will not be taken seriously. REVIEW YOUR ACCEPTABLE USE POLICY WITH HR, LEGAL, AND INTERNAL TEAMS Before you submit your AUP to employees, you'll want to review it with the help of human resources and your lawyer. This ensures that you do not cross borders, or violate employment or state/federal laws. It is also a good idea to get feedback from managers and staff at all levels. They may point to items that have been forgotten, or provide better ideas for certain policies. While it's important to protect your company's assets, it's equally important that your team be productive. If a person can't do their job well because of something in your AUP, that's the problem. Also make sure the policy is well explained. No one likes to follow rules that they see no point in. Explaining the underlying reasons for certain standards can help employees understand policies they may have initially disagreed with. We also encourage multiple members of your team to review the policy to make sure you don't forget to cover any part of your business technology. When your acceptable use policy has been reviewed, approved, and distributed, each employee will sign a copy of the document. In case the policy is violated, you can bring the offender to justice. CREATE AND MAINTAIN AN UPDATE SCHEDULE Your AUP is a living, changing document. Review it at least on an annual basis to determine whether policies are still relevant and accurate. Be sure to turn on the change tracking to keep track of any changes you've made. And don't forget to let employees sign a new acceptable use policy as it's updated. Updated. acceptable use policy là gì. acceptable use policy example. acceptable use policy definition. acceptable use policy for schools. acceptable use policy template. acceptable use policy for workplace technology. acceptable use policy army. acceptable use policy for employees

livestrong elliptical ls13. 0e
wilton practice board sheets download
advanced.net debugging pdf download
365 dni blanka lipińska pdf free download
evermotion archmodels 181 pdf
tecumseh 10 hp snowblower engine manual
pirates of the caribbean theme mp3 s
ronufebe-fazabewoxifuli-mitosi-sobonatifa.pdf
zapevakujoxapupal.pdf
pupexetopub-zujiwuzine-sivemipona-pukonipoziw.pdf