Acceptable Usage Policy

This Acceptable Usage Policy is written for the Company "MobReach" that builds mobile applications for various organizations and start-ups across bay area. Our headquarters of MobReach INC. is located in Sunnyvale, California. Around 75 employees are employed for this service.

An ISSP (Issue Specific Security Policy) provides employees with guidelines about the appropriate use of company equipment, network and Internet access. ISSP is to protect the company from risk and to secure data. The employee will be aware that browsing certain sites or downloading files is prohibited and that the policy must be adhered to or there could be serious fallouts, thus leading to fewer security risks for the business as a result of employee negligence. The ISSP Policy is an important document that must be signed by all employees upon starting work.

Overview

This Acceptable Use Policy for IT Systems is designed to protect MobReach INC., our employees, customers, vendors and other partners from harm caused by the misuse of our IT systems and our data. "IT Systems" means all IT equipment that connects to the corporate network or access corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices software, cloud services, IoT devices, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

Misuse includes both deliberate and inadvertent actions. The fallout of our systems can be severe. Potential damage includes, virus and malware infection, legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Everyone who works at MobReach INC. is responsible for the security of our IT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to their manager or IT security officer.

Scope

This policy applies to all the employees, contractors, vendors operating on the organization. This policy covers use of information and computing devices owned or leased by MobReach INC.'s IT Systems. Some aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws), in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally.

Employees at MobReach INC. who monitors and enforces compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

Administration

These policies will be managed and implemented in the organization by the Information Security (InfoSec) group. InfoSec group will be conducting periodic training sessions to educate the employees about this security policy.

Enforcement

Violations of the company's security policy will be addressed with proper disciplinary measures. Depending on the severity of the case, this may even lead to termination.

Responsibilities

Data Security:

All necessary steps must be taken by the employees to prevent unauthorized access to confidential information.

1) Users are expected to exercise reasonable judgement on deciding which data or information is confidential.
2) Users may use only the computers, computer accounts and files for which they have been granted authorization by the IT department.
3) Users are individually responsible for the appropriate use of all resources assigned to them, including the computer, the network address or port, software and hardware.
4) Users must not send, upload, remove on portable media or otherwise transfer to a non- MobReach INC. system any information that is designated as confidential, or that they should reasonably regard as being confidential to MobReach INC., except where explicitly authorized to do so in the performance of their regular duties.
5) Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with MobReach INC.'s safe password policy.
6) Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.
7) Users must lock their screens whenever leaving their machines (desktop, laptop) unattended.
8) Employees are instructed to follow the clean-desk policy. The printed classified information documents should not be left at desks, unattended. If it is to be discarded, then the documents must be shredded completely.
9) Encrypt data at rest using native disk encryption functionality to protect data stored on mobile and electronic devices.
10) Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into MobReach INC.'s systems by whatever means and must report any actual or suspected malware infection immediately.

Access Control:

1) Access to all cloud services should have multi-factor authentication enabled with services such as Google Authenticator.
2) Remote access to the corporate network has to be tunneled through Virtual Private Network (VPN) services. User also needs to have enter a unique key generated (RSA ID) logging onto VPN.
3) All access to the corporate network should be logged and all user sessions periodically reviewed and audited to ensure highest security standards.
4) All user systems (Computers/Laptops) should prompt for re-authentication after a period of inactivity.

Employee Owned Assets:

1) Only company- owned and authorized assets should have access to the computing and digital assets of the firm. BOYD devices like phone, laptops must not be used to access the computing and data assets of the firm.
2) Employees are strictly prohibited from photographing any sensitive data or documents in their BOYD devices.
3) Employees are strictly prohibited from downloading any company data into their BOYD devices like pen drives etc.

Company Property:

1) All the documents composed, downloaded on the company's system from internet also becomes the property of the company.
2) Any software created using company's data are also the intellectual property of the company.
3) Employees must not download or install any software on the computing systems like virus, malware etc. that can violate the integrity of the computing system as well as the financial data of the firm.

Business Continuity Management:

1) Maintain recoverable copies of sensitive data across multiple availability zones to ensure that business is not impacted in case of a natural disaster.
2) Periodically execute disaster recovery drills for the core data of the firm and confirm its effectiveness.

Encryption:

1) All data must be encrypted with HTTPS/SSL while transmitting over public networks.
2) Sensitive data must be stored in an encrypted format in data systems. Access to this encrypted data must be granted only to authorized and authenticated accounts and systems.

Privacy in Email:

While every effort is to ensure privacy of the organization's email users, thus may not always be possible. In addition, since employees are granted use of computing and network resources to conduct business, there may be instances when the, based on approval from the InfoSec authorities & IT in conjunction with requests and/or approvals from top authorities reserve and retain the right to access and inspect stored information pertaining directly to the business of MobReach without the consent of the user.

Information Security Breaches:

1) Unauthorized attempt to access the data must be reported to the information security team.
2) Multiple failed attempts to access the data should either lead to locking the user account or the originating IP address, if accessed over a public network.

Physical Security:

1) Only authorized personnel must physically enter the organization and access any kind of physical and digital assets that belong to the organization.
2) Access Card needs to be carried by the employees at all times, visitors need to be escorted by employees at all times.

Unacceptable use

Unacceptable use of the Internet by employees includes, but is not limited to:

1) All activities those are detrimental to the success of MobReach INC. These include sharing sensitive information, trade secrets, outside the company, such as research and development information and customer lists, as well as defamation of the company.
2) Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via MobReach INC. email service
3) Using computers to perpetrate any form of fraud, and/or software, film or music piracy
4) Stealing, using, or disclosing someone else's password without authorization
5) Downloading, copying or pirating software and electronic files that are copyrighted or without authorization
6) Sharing confidential material, trade secrets, or proprietary information outside of the organization.
7) Hacking into unauthorized websites
8) Sending or posting information that is defamatory to the company, its products/services, colleagues and/or customers
9) Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications system
10) Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities

11) Passing off personal views as representing those of the organization

Related Standards, Policies and Processes

This policy must be read in conjunction with the following policy references.

1) Digital Millennium Copyright Act (DMCA) and Copyright Infringement
2) Gramm-Leach-Bliley Act
3) Network Security Monitoring Policy
4) Federal Privacy Act Policy
5) Electronic Communications Privacy Act
6) Data Classification Scheme
7) Password Protection Policy

User Compliance:

All data or intellectual property owned by MobReach INC. developed or gained during the period of employment remains the property of MobReach INC. and must not be retained beyond termination or reused for any other purpose.

It is your responsibility to report suspected breaches of security policy without delay to your line management, the IT department, the information security department or the IT helpdesk.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with MobReach INC. disciplinary procedure.

Top five elements of the policy are most important to address risk.

1) Data Security:

   By setting up a system that prompts users to change password every 60 days helps to protect the company's data more efficiently.

   By minimizing the number of accounts which should have access to a critical resource, we can minimize the overall security risk of the system.

2) Access Control:

   Use of VPN services with unique key ID RSA security, multi-factor authentication enabled with cloud services will minimize the risk in securing the organization's sensitive data.

3) Information Security Breaches:

   Creating enough awareness about security breach is primary. Employees unknowingly create a security breach because they were not aware of the security policy of the company. Many of the security issues can be avoided if there is enough training sessions and awareness.

   In an event of a security breach, it is very important to act swiftly. It is necessary to review any minor security breach and take corrective action.

4) Encryption:

   In spite of all the security measures, security breaches occur. The next best option is to make the access to core data as difficult as possible. This can be achieved by encrypting the data

5) Privacy in Email:

   By monitoring any possible security breach by authorized accounts and communicating that to all the stakeholders, firms can ensure that they can prevent any such attempts from happening in the first place.