William Adams

IS-4473-001

10/12/2023

Roadrunner Credit union Acceptable Use Policy (AUP)

At the Roadrunner Credit union, we understand at a high standard that the crucial importance of maintain the confidentiality, integrity, and avaibility our information technology assets is paramount to our success. With how much our world is on the internet in today's internet and workforce, it is pivotal that we can adhere to these policy's. The use of our acceptable use policy (AUP) is designed so that everyone in the organization knows the expectations with using organization systems and to ensure compliance with the Gramm-Leach-Bliley Act (GLBA) security requirements. I do believe that it is very crucial and important as an organization that we follow these set of guidelines and adhere to this policy.

Our acceptable use policy has a lot of goals and objectives that it aims to achieve so that our organization can secure use of our information technology assets. One of our main objectives is to protect member data, it is crucial to be able to secure the financial and personal data of our members. With imposing guidelines that will have for more safer ways of handling, storing, and transmitting of sensitive data. The primary objective is to prevent data breaches, unauthorized access, and data leaks, keeping the confidentiality of our members privacy is crucial to achieving this objective. Another major objective for our acceptable use policy is follow the legal requirements of The Gramm-Leach-Bliley Act (GLBA), the GLBA is a set of requirements for protection of the customers financial information and records. Our AUP is very strictly designed to follow these legal requirements, but also to make sure our beloved client's sensitive information is secured and not at risk. By following these strict guidelines, we are putting on display our commitment to protecting our members and keeping their data secure with the best procedures. Our next objective for our AUP is to minimize security risks, it is a major concern nowadays with how sophisticated hacking has become to prioritize security of digital assets. Best way to achieve this objective is to watch internet usage, eliminating personal use of IT assets, and checking email communications. All these procedures can play a major role in limiting the risk of malware, phishing attacks, and other network threats. The next objective for our AUP is to ensure data integrity, the importance of maintaining the integrity of our systems. This means our systems are functioning as expected and the information that is presented remains reliable and not changed.

The Roadrunner Credit Union use policy (AUP) has a broad and inclusive scope to ensure the responsible and secure use of our information technology assets. It encompasses various elements, IT assets, and organization-owned resources. It encompasses various elements, IT assets, and organization-owned resources. I believe that any individual that is associated with the Roadrunner Credit Union must comply with this AUP, including employees, venders, or any users of the organization. Our AUP applies to all information technology assets that the Roadrunner Credit Union owns, this would include all the hardware such as desktop computers or mobile devices.

For procedures of our AUP policy, a more structured approach is essential to ensure that all employees within the organization and people associated with the organization. Following these procedures are very crucial to make sure the AUP policy is followed as it is made to. All employees, contractors, and third parties who have fallen within the scope, ensuring they have access to the AUP. In the application process upon joining the organization, all future employees will be required to acknowledge their understanding of the acceptable use policy and agree to follow the guidelines by signing the form. For an annual security training and awareness, I believe that is crucial to implement so that all employees, remote workers, and mobile employees

are well trained and are understanding of policies. The topics that the training will cover are email security and internet usage to name a couple. I believe that every organization needs some type of training for new employees so they can get a grasp on procedures and what is expected out of them. The training will be like a hybrid system, where there will be some remote online modules, in-person sessions, and some real time practice. User permissions and restrictions can be a sticky topic to cover, what is allowed and not allowed can be hard for an employee to understand. Employees will only use organization owned technology and assets for business related activities. These technologies are for the use for business only, they are designed to make things easier for employees, not for any other use. Employees are prohibited to use these devices for personal use, this includes any web browsing or social media platforms for personal use. These actives all violate the AUP and forbidden to do so.

For the Do's for what is acceptable:

- Do use organization-owned IT assets and systems responsibly, use them for business actives that are appropriate for work measures.
- Do make sure you are using some caution when you are accessing your email and avoid sending out sensitive information without following security policies.
- Do make sure that you are completing your annual security training so that you are understanding on what is expected.

For the Don'ts on what is not acceptable:

- Don't use the internet for personal use when on the organization's technology devices provided.
- Do not send any sensitive information via email without proper security measures in place and do not share your login credentials with anyone outside of the organization.

As we go more towards the right direction with the Roadrunner Credit Union Acceptable Use Policy (AUP), it is essential to address the roadblocks that could be there in the future and provide guidelines to ensure that the policy is well put. An easy but very important guideline to make stronger passwords by using unique characters. This might seem obvious to do but it is not done by many, it is also very important to update passwords as frequently as possible. Having common passwords that can be easily guessed, like birthdays, or "password", can be a vulnerability. Email etiquette can also be very important for effective email communication. Following email etiquette includes using respectful language and using proper formatting. This is very important, communicating with team members through email is very common so it is crucial to comply with this. As social media is becoming more and more widespread after each year, it is very critical to use caution what you are sharing about yourself on the internet. Using social media on our devices is prohibited but when you are using your social media applications out of the organization, it is important to use caution. The last guideline that has come to us is to avoid suspicious links that you are not familiar with. These links can be very dangerous and malicious if you aren't careful, especially from unknown senders or unexcepted sources.

In alignment with the Roadrunner Credit Union Acceptable Use Policy (AUP), the organization will follow a set of standards that are very crucial for maintain the security and integrity of our organization. These standards empathize hardware, software, or configuration standards and requirements for all users. Users must follow strong unique password standards, which must include the combination of an uppercase letter and a unique symbol.

These passwords should also be updated frequently as possible to ensure strong passwords. Users in the organization should also follow user access control standards, by making sure employees are logging out of there account and not sharing their account information with unauthorized users. This is very important because only users in the organization that are authorized to view certain files should be viewing them, not unauthorized users in the organization. As far as remote access domain standards go, all employees that are working remote will be using virtual private network (VPN) for remote access and strong encryption for data protection so that unauthorized people cannot make out the data. These standards help with security of digital assets while employees are working outside the organization and from remote.

The Roadrunner Credit Union Acceptable Use Policy (AUP) has investigated how there are some unique circumstances that may warrant an exception for breaking policy. As an organization, we do have a waiver process for this type of a situation. If the user feels that there's a legitimate reason for an AUP exception they must complete a request form. This form will explain the situation and why they needed to use to request an exception. Typically, the person who reviews the request is a department head or supervisor so see if the request meets the criteria to grant them that. They make this decision on if the request is granted or not based off if its meats the organizations security measures.

Revision	Originator	Change date	Change description	approver	Approval date
2.0	William Adams	10/11/2023		Prof C	11/20/2023

Author: William Adams
Corresponding documents: this document is much like IT security policy.
Some considerations while writing the policy, this policy was made and put into use to comply with the GLBA and to also to better security for the organization for the future.

There will be an annual review of the policy every single year.

Policy glossary

Acceptable Use Policy (AUP): An acceptable use policy (AUP) is a document stipulating constraints and practices that a user must agree to for access to a corporate network, the internet or other resources.
GLBA: The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.
Phishing: A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.
IT assets: IT assets are the integral components of the organization's IT environment used for storage, management, control, display, data transmission, and more.
Remote access: Remote access is the ability for an authorized person to access a computer or network from a geographical distance through a network connection.

Policy violations clause: violations of the Roadrunner Credit Union AUP aren't takin as a joke. You will be first talked to and be warned if you violate a policy for the first time. The second time you will have access restrictions to your account and be warned one more time. The 3rd time it happens you will be fired after 2 warnings.

I (employee name) have read and have acknowledge the Roadrunner Credit Union AUP.

Employee Name:
Signature:
Date:

References

- Santos, Greene book has a Sample Acceptable Use Policy in Appendix C. (2nd version of book—this appendix is also located in the Course Resources and Links)

5 Questions

1. Why do organizations have acceptable use policies (AUPs)?

I believe that organizations establish AUP's for several reasons, one of the biggest reasons organizations have these in place is to have a set of guidelines for employees and users are expected to interact with the organizations information systems. I believe it is crucial to have these in place to protect the integrity of the organization and to protect the digital assets from future threats.

2. What are two risks of the user domain and the administrative, technical, or physical security control(s) to mitigate the risks?

Risk 1: Phishing and social engineering attacks

Technical control: I would deploy email filters and scanning operations to identify and black phishing emails from coming into the system.

Risk 2: unauthorized access

Administrative control: I would deploy a strong authentication policy; this would include user authentication like MFA to prove who you say you are.

3. Why must an organization have an acceptable use policy (AUP)even for non-employees, such as contractors, consultants, and other third parties.

Organizations must have acceptable use policy's (AUP'S) even for non-employees, having these in place for contractors, consultants, and other third parties are crucial. Having these in place to establish a clear expectation on what is expected behavior when accessing the organizations rescores is significant.

4. What security controls can be deployed to measure, enforce, monitor, and mitigate users from accessing external websites, webmail systems, and social media services that are potentially in violation of an AUP?

Organizations can implement several security controls to enforce users from accessing external websites that can be damaging. Web filtering and proxy servers are used to monitor and control internet traffic, enabling the blocking or restriction of access to specific categories of websites.

5. What would be a huge difference between a Credit Union and Healthcare organization AUP policies?

The difference between the two organizations AUP policies would be about what their organization is mainly about. I believe a credit unions AUP policy would focus on securing financial and personal information of members and securing sensitive data of employees and

members. With a healthcare organization, I belie there AUP policy would revolve around the protection of patient's personal information and health records.