

Acceptable Usage Policy



THIS ACCEPTABLE USAGE POLICY COVERS THE SECURITY AND USE OF ALL RIAFOX, INC'S. INFORMATION AND TECHNOLOGY EQUIPMENT. IT ALSO INCLUDES THE USE OF EMAIL, INTERNET, VOICE AND MOBILE EQUIPMENT. THIS POLICY APPLIES TO ALL RIAFOX, INC'S. EMPLOYEES, CONTRACTORS AND AGENTS (HEREAFTER REFERRED TO AS 'INDIVIDUALS').

THIS POLICY APPLIES TO ALL INFORMATION, IN WHATEVER FORM, RELATING TO RIAFOX, INC'S. BUSINESS ACTIVITIES WORLDWIDE, AND TO ALL INFORMATION HANDLED BY RIAFOX RELATING TO OTHER ORGANIZATIONS WITH WHOM IT DEALS. IT ALSO COVERS ALL INFORMATION TECHNOLOGY AND INFORMATION COMMUNICATIONS FACILITIES OPERATED BY RIAFOX OR ON ITS BEHALF.

Information System Access Control – Individual’s Responsibility

Access to Riafox IT systems are controlled by User IDs, passwords and/or tokens. All User IDs and passwords are uniquely assigned to named individuals and consequently, individuals are accountable for all actions on Riafox, Inc’s. IT systems.

There may be Software test environments where user ID’s are distributed across users temporarily for the purpose of testing. Due to the temporary nature of testing environments which do not capture live user data, an individual's responsibility regarding Access Controls do not apply.

During periods of System Maintenance, Riafox Partner's may issue a single ID to the company for purposes of technical support access. Due to the nature of these shared ID authentication tokens we must all be diligent in protecting, updating, or terminating them as required.

Incident Response, Handling, and Reporting

Riafox is committed to providing a safe and productive workplace for its employees, contractors, partners, and its data. In keeping with this commitment, There are four key steps to consider when responding to a breach or suspected breach:

Step 1: Contain the breach and do a preliminary assessment

For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security.

Step 2: Evaluate the risks associated with the breach

Consider the following factors in assessing the risks:

1. The type of information involved (Personal, Medical, Proprietary).
2. The context of the affected information and the breach.
3. The cause and extent of the breach.
4. The risk of serious harm to the affected individuals.
5. The risk of other harms.

Step 3: Notification of breach to supervisor or Management

Notification can be an important mitigation strategy that has the potential to benefit both the agency or organization and the individuals affected by a data breach. The challenge is to determine when notification is appropriate. While notification is an important mitigation

strategy, it will not always be an appropriate response to a breach. Providing notification about low risk breaches can cause undue anxiety and de-sensitize individuals to notice.

Each incident needs to be considered on a case-by-case basis by Management to determine whether breach notification is required.

Step 4: Prevent future breaches

Once the immediate steps are taken to mitigate the risks associated with a breach, the Company needs to take the time to investigate the cause and consider whether to review the existing prevention plan or, if there is no plan in place, develop one.

A prevention plan should suggest actions that are proportionate to the significance of the breach, and whether it was a systemic breach or an isolated event.

Such a plan may include:

- a security audit of both physical and technical security.
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation, and regular reviews after that (for example, security, record retention and collection policies).
- a review of employee/contractor selection and training practices, and.
- a review of service delivery partners (for example, offsite data storage providers).

When responding to Data issues or unprofessional communication time is of the essence.

- Be sure to take each situation seriously and move immediately to contain and assess the suspected breach.
- Breaches that may initially seem immaterial may be significant when their full implications are assessed.
- The Company should undertake steps 1, 2 and 3 either simultaneously or in quick succession. In some cases it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs.
- The decision on how to respond should be made on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined.
- In some cases, malicious code (honeypots) could engage when attempting to extinguish the initial threat.
- Riafox may choose to take additional steps that are specific to the nature of the breach.

Responses to Social Media and Unprofessional Communications

Increased Exposure to Malware

Visiting social networking sites at work can expose company networks to malware, including adware and spyware. Malware, or malicious software, is designed to take control of and damage a computer. It can help hackers steal identities and data. If you suspect you have encountered malware while at work or while logged in remotely be sure to inform your supervisor or Management of the situation immediately.

Ransomware Protocol

Ransomware is the most opportunistic type of malware, infecting from a single user to an entire organization. A tough question for any victim is whether they should pay the money or not. Law enforcement agencies, as well as Riafox, Inc, advises against paying a ransom. It is widely known criminals often do not provide the key even after receiving the ransom.

The most efficient and effective way to get back the data is to restore data files from a backup. In most corporate environments files are backed up regularly so recovery should not be a problem. Normally a backup is made for shared and mapped drives. User desktop data is rarely saved. Users should backup the files to a Riafox network drive. If using an external drive or USB drive you must disconnect it after the backup. Almost all ransomware will encrypt network drives.

No Tolerance towards Harrassment

Riafox is committed to providing a work environment that is free of discrimination and unlawful harassment. Actions, words, jokes, or comments based on an individual's sex, race, ethnicity, age, religion, or any other legally protected characteristic will not be tolerated.

If you believe you have been the victim of harassment, or know of another individual who has, report it immediately. Individuals can raise concerns and make reports without fear of reprisal.

Social Media

Social media has changed the way we communicate. Social applications and email present great opportunities for businesses in the areas of public relations, internal and external communications, recruiting, organizational learning and collaboration, and more. Equally so nefarious activity can quickly destroy the public image of Riafox and its Partners. We share in the responsibility to protect each other's social identities.

Also presented are the potential issues created when individuals use their personal social media accounts while at the office, possibly affecting productivity, data security and network security. We value our public image when interacting with the public both in person and online.

Individuals who are aware of negative social or unprofessional communications directed to or emanating from Riafox, or its Partners should raise their concerns to their Supervisor, HR, or Management. Reporting any such communications can be made without fear of reprisal.

Monitoring and Filtering

The need for a policy arises in part from the need to provide you with a consistent, stable, secure working environment. In order to do that, we have adopted these rules of conduct with regards to computer, software, and network use so as to more efficiently use the limited resources available.

All data that is created and stored on Riafox computers, servers, SAAS or cloud service environments is the property of Riafox and there is no official provision for individual data privacy. Wherever possible Riafox will avoid opening personal emails, however, Riafox reserves the right to step in and enforce guidelines that haven't been followed and admonish repeat offenders.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Riafox has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

INDIVIDUALS MUST NOT:

- Allow anyone else to use their user ID/token and password on any Riafox IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Riafox, Inc's. IT systems. (testing environments excluded)
- Leave their password unprotected (for example writing it down).
- Perform any unauthorized changes to Riafox, Inc's. IT systems or information.
- Attempt to access data that they are not authorized to use or access.
- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Connect any non-Riafox authorized device to Riafox network or IT systems.
- Store Riafox data on any non-authorized Riafox equipment.
- Give or transfer Riafox data or software to any person or organization. outside Riafox

without the authority of Riafox.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Internet and email Conditions of Use

Use of Riafox internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Riafox in any way, not in breach of any term and condition of employment or contract and does not place the individual or Riafox in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

INDIVIDUALS MUST NOT:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Riafox considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Riafox, alter any information about it, or express any opinion about Riafox, unless they are specifically authorized to do this.
- Send unprotected sensitive or confidential information externally.
- Make official commitments through the internet or email on behalf of Riafox unless authorized to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Connect Riafox devices to the internet using non-standard connections.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorized access or loss of information, Riafox enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example limited and secured access to scan folders.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Remote / Off-site Access

It is accepted that laptops and mobile devices will be taken off-site, or access to Riafox systems be acquired from personal computers and/or devices. The following controls must be applied:

- Working away from the office must be in line with Riafox remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Company laptops must be handled as a carry-on during air travel.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places).
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

Mobile Storage Devices

Mobile devices such as flash drives, SD Cards, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Riafox authorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software

Individuals must use only software that is authorized by Riafox on Riafox, Inc's. computers, servers or cloud environments. Authorized software must be used in accordance with the software supplier's licensing agreements. All software on Riafox computers must be approved by Riafox Management.

INDIVIDUALS MUST NOT:

- Store personal files such as music, video, photographs or games on Riafox IT equipment.

Viruses

Riafox has implemented centralized, automated virus detection and virus software updates within Riafox networks. All PCs have antivirus software installed to detect and remove any virus automatically.

INDIVIDUALS MUST NOT:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Riafox anti-virus software and procedures.

Telephone/Voice Equipment Conditions of Use

Use of Riafox voice equipment is intended for business use. Individuals must not use Riafox, Inc's. voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

INDIVIDUALS MUST NOT:

- Use Riafox, Inc's. voice equipment for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use.

Actions upon Termination of Contract

All Riafox equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Riafox at termination of contract.

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

Signature

A handwritten signature in black ink that reads "Bai Feng". The letters are written in a casual, slightly cursive style.



Bai Feng

Date: 11 / 02 / 2021

Signature Certificate

Document Ref.: I2N9V-U4MLS-6RKVW-ZM2OS

Document signed by:

	<p>Bai Feng Verified E-mail: baifeng1991321@gmail.com</p>	<p><i>Bai Feng</i></p> 
<p>IP: 209.95.60.92 Date: 02 Nov 2021 08:57:41 UTC</p>		

Document completed by all parties on:
02 Nov 2021 08:57:41 UTC

Page 1 of 1



Signed with PandaDoc.com

PandaDoc is a document workflow and certified eSignature solution trusted by 25,000+ companies worldwide.

