Yeykin Valenzuela

10/06/2019

IT in the Global Ages

Professor Ermicioi

**Policy Brief and Purpose**

At Bank of America, we value privacy. Our records are being stored in devices to be used later and must be handled properly and confidently. The following regulations, policies, and procedures must be implemented in order to keep employee and client information private. Negligence or misuse of these policies and procedures will result in disciplinary action.

**Fundamental rules to be followed**

1. **Updating passwords**

In order to manage account security, passwords must be updated every six months. Passwords related personal information should not be used, and old passwords cannot be used. Do not share account passwords and keep personal passwords separate from passwords used for company accounts.

1. **Sharing Information**

Confidential information should not be shared with third parties, and should be used for professional purposes only. Customer’s information should not be distributed among employees without proper clearance for that data. Personal or customer information should not be shared through email.

1. **Unknown emails**

When receiving emails from unknown senders, avoid opening the emails, as they may introduce viruses into our company software or may be a scam. Before opening an email, make sure you know the sender. Keep your inbox clean. If you’re constantly receiving emails from unknown senders, please contact our IT specialists.

1. **Report scams to our IT specialists**

If you receive unknown emails and/or phone calls, immediately contact our specialists. They will make sure our information is not at risk and can assist with any problems you may experience with the company software. Our IT specialists are here to make sure our data, network and devices are secure and no information can be breached.

1. **Log out after leaving your workplace**

Do not leave company accounts open when leaving the workplace. Make sure you log out from every device before leaving the area. Leaving information unattended puts the privacy of our employees and customers at risk. Our information is very sensitive and must be handled properly. We are entrusted with this information, our job is to maintain it secure.

1. **Company Devices**

Our devices can only be used for work purposes. You should not use our computers and other devices for personal use and vise versa. For example, you should not log into your personal social media accounts using your work device.  Also, do not use you personal device to access information from our company without the proper clearance. Keep personal and work accounts separate.

1. **Update security software**

Be sure to keep up with security software updates. Emails will be sent when new updates are available. To ensure that our security system is the best it can be, all software must be kept up to date.

1. **Encryption**

When saving files/documents, please make sure you name it appropriately so that it can be found by other employees. Do not use personal information to encrypt such information. Such encryptions have to be understood and not forgotten by employees, but hard for other people to guess. Use appropriate encryption for credit cards and other information, if you’re unsure of what is appropriate regarding encryption, please contact your supervisor for further examination.

1. **Schedule backups**

In order for us not to lose valuable information, please schedule backups for your devices. Backups will be conducted once a week to ensure that employee and client information is not lost. If backups are not scheduled, you may lose sensitive information that will not be able to be retrieved.

1. **Remote Access**

Clearances may be given to access customer and employee information from your own devices when you are not in the workplace. The same precautions should be taken when accessing data from other devices. Employees must be hypervigilant when opening sensitive documents to ensure the privacy and safety of the material. Be sure to log out before leaving devices unattended and to always save content before closing documents.

* 1. **What is the Dark Web?**

It’s a web that cannot be accessed by common software. It’s used to find things that cannot be obtained through regular means.

**2. Who uses the Dark Web?**

The deal web is used by the common people, and the government, but its specially used by criminals to buy and sell illegal stuff.

**3.  What type of activities do people perform on Dark Web?**

It can be used as private communication and for investigations, but unfortunately, it’s mainly used to practice illegal doings.

**4. Who controls the Dark Web?**

The Dark Web does not have a specific owner, it is controlled by people- it’s users.

**5. What are the consequences of using the Dark Web?**

Consequences of using the Dark Web can end up in investigations by authorities, incarceration and the worst outcome, which is harm the user’s self-and/or the society.