BYOD (Bring Your Own Device) Acceptable Use Policy

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who are connecting a personally-owned device to GoTriangle's organization network for business purposes. This device policy applies to the following classifications:

- Mobile phones
- Tablets
- Portable media devices (iPods, MP3 players, etc.)
- Laptop/notebook computers, including home desktops and home laptops
- USB thumb and external hard drives

The policy applies to any hardware and related software that is not organizationally owned or supplied by GoTriangle, but could be used to access GoTriangle resources. To rephrase this, if you have a device used for personal reasons, but you also want to use for any work for GoTriangle, this policy applies to you and the device you plan to use.

The goal of this policy is to inform the GoTriangle employee that we need to keep in mind the safety and security of our network and GoTriangle's data. This policy is written to instruct the employee on how to handle your device while you are connected to the GoTriangle network. Loss of information could damage our reputation as well as cause destruction to GoTriangle resources. If you plan to use any device for work, please read and ask for clarification if you do not fully understand this policy.

Applicability

This policy applies to anyone who uses a device that is connected to GoTriangle resources or GoTriangle network.

This policy addresses a range of threats to GoTriangle's data and the use of its data.

Threat	Description
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive organizational data is deliberately stolen and sold by an employee or unsanctioned third party.
Malware	Viruses, Trojans, worms, spyware, and other threats could be introduced via

	devices.
Non-compliance	Loss or theft of confidential and/or personal data could expose GoTriangle to the risk of non-compliance with identity theft and privacy laws.

All employee owned devices will be set up by IT of GoTriangle. This includes email setup on phones as well as any other device that is connected to GoTriangle resources. Addition of new hardware and/or software will be managed by IT. It is forbidden to backup or store GoTriangle data or any GoTriangle information on personal devices or cloud storage services without the consent of IT.

Responsibilities

All GoTriangle employees are responsible to act in accordance with company policies and procedures.

Affected Technology

IT will not directly manage personal devices. Employees are expected to adhere to the same security protocols when using personal devices for work purposes. Protocols include, but are not limited to, using strong passwords, using antivirus, not sharing passwords, etc. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

Policy and Appropriate Use

It is each employee's responsibility to use their personal device carefully in regards to protecting GoTriangle resources and data. It is extremely important that the device is used for business purposes in a responsible, appropriate, and ethical manner.

Access Control

1. IT can refuse the ability of the device to connect to GoTriangle resources if the device is used in a way that puts GoTriangle at risk.
2. All devices must be approved by IT. Devices must have the latest updates and have some form of antivirus protection installed and up to date. All devices must be on a platform that is receiving frequent updates and security patches.
3. Confidential GoTriangle data (i.e. passwords to GoTriangle's resources, SSNs of employees) shall not be stored on personal devices.

Security

4. Employees using personally-owned devices will use a strong password or PIN. GoTriangle data shall not be stored on personal devices. Employees agree never to disclose their passwords to anyone, including family members, or store passwords on personal- devices if company work is

conducted from home.

5. All users must employ reasonable measures to secure their device with a password. Also secure any portable devices physically while they are in transport. For example, do not leave your laptop in plain view in your car if you are stopping at the store on your way home.

6. Any personal devices used for work purposes need to have up-to-date and working antivirus. In addition, any device that is connected to a home computer and then plugged into a work computer, such as a USB stick. Malware can easily spread thru a USB and can result in data loss on a pc and network resources.

7. Passwords and other confidential data as defined by GoTriangle's IT department are **not to be stored** on mobile devices.

8. Any device being used to store GoTriangle data must **be pre-approved by** the IT department.

9. IT will manage security policies, network, application, and data access. **Any attempt to bypass that security implementation will be deemed an intrusion attempt** and will be dealt with in accordance with GoTriangle's overarching security policy.

10. IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of employees to transfer data on GoTriangle's network.

11. Employees will notify the IT Department in order to follow all data removal procedures to remove data off of devices, when devices are no longer needed. An example of this is when an employee upgrades their phone, the IT Department will need to remove their email account off the phone first before they turn the phone in or sale the phone.

12. In the event of a lost or stolen device used for work purposes, it is important that the employee report the incident to IT Department immediately. The IT department will give further advice and take more actions to ensure GoTriangle resources are protected if necessary.

13. When connected to a Public Wi-Fi, Hot Spot or Wired connection. Under No circumstances are Employees to leave the device unattended while connected to GoTriangle's network, through VPN or Remote Desktop for any amount of time.

Help and Support

14. The GoTriangle IT Department is not responsible for repairing, advising or fixing issues with your personal device. A member of the IT department may assist you only on his or her own time (lunch or after hours), but it is not considered a part of GoTriangle's day to day operations.

15. GoTriangle IT Department will troubleshoot any issues relating to GoTriangle equipment or software if it prevents the employee from using their device for work purposes.

16. Employees will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing, overriding the operating system, or "jail-breaking").

Organizational Protocol

17. If your device is connected to our network we can and will use audit trails when investigating possible breaches or misuse of privileges. You agree that your connection to our network will be monitored.

18. The Employee agrees to **immediately report** to his/her manager and GoTriangle's IT department **any incident, suspected incidents, unauthorized data access, data loss, and disclosure of company resources.**

19. **By signing this policy you agree that you fully understand it and all the risks and responsibilities of Bring Your Own Device. Any questions may be directed to a member of the IT team.**

Policy Non-Compliance

Failure to comply with the *BYOD Acceptable Use Policy* may, at the full discretion of GoTriangle, result in the **suspension of any or all technology use and connectivity privileges, disciplinary action, possible termination of employment, [as well as possible criminal charges]**.

The Employee's Manager or Director and the IT Manager will be advised of breaches of this policy and will be responsible for appropriate remedial action.

BYOD Employee Declaration

I have read and understand the above *BYOD Acceptable Use Policy*, and consent to adhere to the rules outlined therein.

_____ _____

Employee Signature Date

_____

Employee Print Name

_____ _____

IT Department Staff Date