



7.1 PhotoBiz Public Network Usage Policy & Device Identification

Revised: 2012-12-17

Policy Purpose and Scope

The purpose of this policy is to outline the guidelines for use of the public and wireless networks by employees.

Roles and Responsibilities

The PhotoBiz public networks are available to all employees of PhotoBiz for use with personal devices, including smart phones and tablets. The use is subject to guidelines and limitations, which are as follows:

1. All policies regarding acceptable use of company resources apply to use of the public networks.
2. You will implement and maintain reasonable security measures on your device. This includes, but is not limited to:
 - a. Using secure passwords and other security measures to prevent unauthorized access;
 - b. Keeping the device up to date and patched with the latest operating system and security patches; and
 - c. Refraining from installing or using questionable applications often used for potential malicious content without authorization of the IT department.
3. Before access to the public networks are granted, information must be obtained about device so that it can be properly identified on the network.
4. Using your personal device on any PhotoBiz network other than the public networks is forbidden unless using an approved VPN solution.
5. Permission must be obtained from the IT department for hosting services on your device, for work related purposes or otherwise, prior to their use.
6. The IT department can opt to throttle, limit, or block access to the public networks at anytime without explanation if your device is using an excessive amount of bandwidth or if it represents a possible security threat.

Operational Procedures

You agree to abide by the above guidelines to the best of your ability and acknowledge that failing to comply with the above can result in disciplinary action. You also assert that you understand the above guidelines and have already discussed any potential concerns with the IT department.

Device
Type: _____

Wireless
MAC: _____ Wired MAC: _____

Your Name: _____ IT Manager: _____

Your
Signature: _____ IT Mgr
Signature: _____

Date: _____ Date: _____